UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

IMPLEMENTACION DE UN PLAN DE RECUPERACION EN CASO DE DESASTRE (DRP) PARA BACKOFFICE SAP ERP

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Jorge Venegas Rodríguez
Profesor Guía : Roberto Carú Cisternas
Profesor Integrante : Jorge Tapia Castillo

Santiago – Chile
Agosto, 2013

Declaración Jurada

Por el presente instrumento, **Jorge Segundo Venegas Rodríguez**, cedula de identidad **12.111.533-6** viene a declarar bajo fe de juramento, haciéndolo responsable de la veracidad de lo expuesto, que:

Toda la información contenida en el trabajo de investigación para optar al título de Ingeniero(a) de Ejecución en Informática denominado: "**Implementación de un Plan de Recuperación en caso de Desastre (DRP) para BackOffice SAP ERP**", es original y no referida a otras fuentes, salvo en aquellos casos en que se admite expresamente, que se ha utilizado información proveniente de otros estudios efectuados por terceras personas o instituciones, las cuales fueron debidamente citadas.

Para constancia firma en Santiago, 28 de Octubre del 2013

Jorge Segundo Venegas Rodríguez

Autorización para la publicación de memorias de Pregrado y tesis de Postgrado

Yo, **Jorge Segundo Venegas Rodríguez** cedula de identidad Nº **12.111.533-6** autor de la memoria o tesis que se señala a continuación, autorizo a la Universidad Gabriela Mistral para publicar en forma total o parcial, tanto en formato papel y/o electrónico, copias de mi trabajo.

Esta autorización se otorga en el marco de la ley Nº 17.336 sobre Propiedad Intelectual, con carácter gratuito y no exclusivo para la Universidad

Título de la memoria o tesis:	Implementación de un Plan de Recuperación en caso de Desastre (DRP) para BackOffice SAP ERP
Unidad Académica	Facultad de Ingeniería
Carrera o Programa	Ingeniería de Ejecución en Informática
Titulo y/o grado al que se opta	Ingeniero(a) de Ejecución en Informática

Firma del Alumno(a)

RUT: 12.111.533-6

DEDICATORIA

A mi esposa Pamela Guajardo y a mis hijos Betzabet y Jorge por ser la fuente de mi inspiración y motivación. Ustedes son la energía que me permiten superar cada obstáculo que me presenta la vida.

A mis padres, quienes me dieron la base que hoy me permite afrontar y disfrutar los retos que se presentan en mi camino.

AGRADECIMIENTOS

A Empresas CMPC S.A por la oportunidad de crecimiento profesional y el apoyo incondicional que me brindan a través de mis veintitrés años (1990-2013) trabajando en esta gran empresa.

A la Universidad Gabriela Mistral, a nuestros profesores por compartir con nosotros los estudiantes, sus experiencias y conocimientos, permitiéndonos ser mejores profesionales y mejores personas.

RESUMEN EJECUTIVO

El término desastre, de acuerdo a Jon William Toigo, significa la interrupción del negocio debido a la pérdida o incapacidad de acceso a los elementos que contienen la información necesaria para la operación normal de la organización. El autor se refiere a la pérdida o interrupción de las funciones que procesan los datos de la compañía o a una pérdida en sí de la información. La pérdida de datos puede presentarse debido a borrados accidentales, intencionales o por la destrucción de los medios que almacenan la información de la empresa. Esta pérdida puede ser causada por fenómenos naturales o inducida por el factor humano.

Para mitigar las consecuencias que podría causar un desastre, nacen los planes de recuperación por desastre o DRP por sus siglas en inglés (Disaster Recovery Planning), los cuales consisten básicamente en las acciones para recuperarse en caso de que se presente un desastre. Incluye la planificación de pasos para evitar riesgos, mitigarlos o transferirlos a alguien más por medio de seguros. El DRP es aplicable a todos los aspectos de un negocio, sin embargo se utiliza normalmente en el contexto de operaciones para el procesamiento de datos.

Los procesos críticos que tiene cada uno de los diferentes negocios que posee la Empresa, mueve diariamente una cantidad de dinero tal, que requiere una alta disponibilidad (entre 99% y 100%) de los sistemas SAP ERP que soportan este procesamiento. Dada la competencia que se desarrolla en el mercado, no solo en chile, sino que también en otros países, un fallo en los sistemas de información, puede significar pérdidas importantes, tanto monetarias como en la imagen de la Empresa. Por lo anterior, es de gran valor para la Empresa, contar con un plan de contingencias, que le permita continuar con el negocio, en caso de que se presente un imprevisto que impacte los sistemas SAP ERP que soportan el normal funcionamiento de este negocio.

El objetivo general de este proyecto consistió en diseñar una guía que le permita a la organización crear un procedimiento de recuperación ante desastre, natural o inducido, para el sistema informático de Empresas CMPC ubicado en el Data Center de IBM, tal que pueda ser ejecutado por personal técnico externo al sitio de desastre y en pocas horas se pueda restablecer el servicio normalmente brindado.

Como parte de los objetivos específicos, se diseñó una guía para crear un plan de mantenimiento que garantice que el procedimiento a definir se mantenga vigente y finalmente se dieron los lineamientos para crear un plan de simulacros de desastre que ayude a comprobar la efectividad del plan maestro.

INDICE

1. INTRODUCCIÓN

Un desastre dentro de la organización puede significar muchas cosas, desde una pérdida importante de datos hasta un desastre natural que destruye la infraestructura tecnológica de la organización. Cualquier evento que cause una interrupción en la operación normal del negocio se considera un desastre. Sin un plan efectivo para recuperación de desastres, la mayoría de las organizaciones no sobrevive ante interrupciones importantes de su negocio.

Los planes para darle continuidad a una actividad, realmente no son nuevos, diariamente se convive tanto con estos que se hace imperceptible su utilización. Sea cual sea la medida que se tome para afrontar un riesgo, las acciones buscan siempre alguno de los siguientes objetivos: mitigar, evitar o transferir el riesgo identificado.

Las economías mundiales, hoy en día, viven un proceso de globalización, y las empresa para sobrevivir, deben tener tecnologías eficientes. Es por esta razón que empresas CMPC adquirió e implemento, hace trece años atrás, el software SAP ERP.

SAP AG, es el líder mundial de sistemas de administración para empresas, y ofrece completo software de gestión y servicios que satisfacen las necesidades de empresa CMPC, el principal software adquirido es SAP ERP[1]. Esta solución brinda una funcionalidad de principio a fin para todos los negociones de la empresa CMPC.

El presente trabajo, pretende crear una guía que permita crear un procedimiento o plan de recuperación a seguir en caso de que se presente un desastre (natural o inducido) en el sistema informático SAP ERP de la Compañía Manufacturera De Papeles y Cartones (Empresas CMPC), de manera que los

[1] ERP, Enterprise Resource Planning (Sistemas de planificación de recursos empresariales).

procesos se puedan habilitar en un sitio alterno y la compañía continúe su operación normal desde otro lugar mientras se recupera el sitio original.

Empresas CMPC pertenece a cinco sectores de negocio, Forestal, Celulosa, Papeles, Tissue[2] y Productos de Papel.

Forestal: Esta área de CMPC desarrolla sus negocios en el ámbito de la forestación, el suministro de productos de madera distintos a celulosa y papel, formando y administrando un patrimonio forestal sostenible en Chile y Argentina, que respalda la actividad industrial de la compañía. Cuenta con una amplia red comercial en los 5 continentes y oficinas en Chile, Estados Unidos y Japón. Además, más de 535 mil hectáreas de plantaciones.

Celulosa: Orientada a la fabricación y comercialización de celulosa, esta división exporta el 90% de su producción a los mercados de América, Europa, Asia y Oceanía, contando con una red logística que contempla terminales en todo el mundo.

Papeles: Produce y comercializa papeles y cartulinas a través de sus filiales Papeles Río Vergara (Nacimiento), Cartulinas CMPC (Maule y Valdivia) y Papeles Cordillera (Puente Alto). A través de SOREPA recolecta el papel usado y de EDIPAC comercializa papeles de impresión. Los productos de esta área se exportan principalmente a Latinoamérica, Estados Unidos, el Caribe, Europa y Asia.

Tissue: Esta área de CMPC fabrica y comercializa productos tissue en Chile, Argentina, Perú, Uruguay, Colombia, Ecuador, Brasil y México, a través de marcas que han logrado situarse con un importante liderazgo en cada uno de estos mercados.

[2] TISSUE, Papel higiénico fino absorbente hecho de pulpa de celulosa.

Productos de Papel: Desarrolla su trabajo a través de las siguientes filiales en Chile: Envases Impresos, Envases Roble Alto, Chimolsa y Forsac; Forsac Argentina, Forsac Perú y Forsac México, atendiendo mercados tan diversos como el sector industrial, frutícola, vinícola, de la construcción y salmones.

El Sistema SAP ERP, es elemental para la continuidad de los cinco negocios de esta Empresa, una interrupción del sistema SAP ERP, generaría una gran pérdida en los activos correspondientes a la información y servicios críticos de sus negocios.

Es por esta razón que la alta disponibilidad para el sistema SAP ERP se vuelve un asunto crítico y la mejor forma de asegurar esta disponibilidad es contar con un procedimiento que de forma proactiva permita habilitar el sistema SAP ERP en caso de desastre.

El sitio alterno o lugar escogido para hospedar los sistemas que se van a utilizar como medida de contingencia en caso de desastre también es una parte importante que se debe tomar en cuenta en este tipo de proyectos. Los sitios alternos varían desde una simple área cerca del centro de operaciones hasta el alquiler de un lugar exclusivo. Estos últimos cuenta con todas las facilidades en equipo, infraestructura y seguridad, sin embargo, tiene un alto costo el cual se vuelve relativo cuando se habla de que puede ser la diferencia entre seguir o no en el negocio.

Otros elementos o características importantes que se deben tomar en cuenta en este tipo de planes son el contenido y redacción de los mismos, de manera tal que un equipo de personas con solo conocimientos técnicos en informática, o sea, sin ser expertos en los sistemas a habilitar, pueda ser capaz de tomar el procedimiento y activar los procesos en el sitio alterno escogido para esta función. Por lo tanto, a lo largo de esta investigación se hará énfasis en la calidad de la información contenida en el plan.

Por lo tanto el objetivo general de este proyecto consiste en:

- La implementación de un sitio de contingencia que pueda entregar una alta disponibilidad y contingencia de los servicios críticos, ante la caída del sitio principal, una óptima distribución del hardware, redundancia en enlaces y redes extendidas TCP/IP[3] y SAN[4], mínimos tiempos de recuperación entre sitios y una modalidad activa- activa del servicio en ambos sitios.

También se tienen los siguientes objetivos específicos:

- Diseñar una guía que permita crear un procedimiento de recuperación ante desastre, natural o inducido, para el sistema informático SAP ERP, tal que pueda ser ejecutado por personal técnico externo al sitio de desastre y en un tiempo previamente definido, se pueda restablecer el servicio normalmente brindado.
- Diseñar una guía que permita crear un plan de mantenimiento para garantizar que el procedimiento a definir se mantenga vigente.
- Definir los pasos necesarios para crear un plan de simulación de desastre que ayude a comprobar la efectividad del plan maestro.

[3] TCP/IP, Siglas de Protocolo de Control de Transmisión/Protocolo de Internet.
[4] SAN, Storage Area Network (red de área de almacenamiento).

2. MARCO TEÓRICO

Muchos negocios dependen fuertemente de la tecnología y sistemas automáticos y la interrupción de estos, por inclusive unos cuantos días, podría causar serias pérdidas financieras y poner en peligro su supervivencia. La continuidad de las operaciones de una organización depende de la conciencia administrativa acerca de desastres poderosos, así como su habilidad para desarrollar planes para minimizar las interrupciones de las funciones esenciales.

Un plan de recuperación de desastres es una declaración de acciones consecuentes que se deben realizar antes, durante y después del desastre. Este plan debe ser probado y registrado para asegurar la continuidad de las operaciones y la disponibilidad de los recursos necesarios para ella.

El objetivo principal de la planificación de recuperación de desastres es proteger, a la organización, en caso de que todas o alguna porción de sus operaciones y/o servicios computacionales se bloqueen. La clave consiste en la preparación. El proceso de planificación deberá reducir la interrupción de las operaciones y prometer un nivel de estabilidad organizacional y una recuperación ordenada después del desastre.

Un riesgo se define como un evento o condición inciertos que, si se produce, tiene un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, costo, alcance o calidad (PMI[5]).

Una crisis o desastre puede categorizarse en tres niveles, de acuerdo a su nivel de riesgo:

[5] Siglas en ingles del Instituto de Administración de Proyectos (Project Management Institute).

NIVEL I, BAJO RIESGO

Se presenta sin daños serios, mínimo daño físico, no se presenta interrupción de las operaciones críticas de la compañía y no hay angustia en el personal.

NIVEL II, RIESGO MODERADO

Se presentan daños serios, una cantidad importante de daños menores, daños menores en las instalaciones y servicios, se presenta una interrupción menor en las operaciones críticas y un impacto moderado en las actividades de negocio rutinarias. Se presenta cierto grado de angustia en el personal.

NIVEL III, ALTO RIESGO

Daños humanos mayores, incluyendo muertes, daños físicos mayores, un impacto significativo en las actividades de negocio de mayor importancia, visibilidad media y potencial impacto en los clientes y accionistas.

Para mitigar el efecto o impacto de un riesgo para la organización, las compañías desarrollan planes de contingencia que son en pocas palabras respuestas para superar o mitigar el impacto de situaciones inesperadas.

En 1978, un estudio de la Universidad de Minnesota, investigó la vulnerabilidad relativa ante desastre de algunas industrias específicas y demostró la máxima cantidad de tiempo que sus sistemas pueden estar “caídos” antes de que la recuperación sea imposible. Como se observa en el Figura 1, la industria financiera tiene la menor tolerancia a una caída prolongada mientras que los seguros y manufactura pueden sostenerse por más tiempo ante una caída prolongada sin causar un colapso en su negocio.

INDUSTRIA	DIAS
Financiera	2.0
Distribución	3.3
Misceláneas	4.8
Manufactura	4.9
Aseguradoras	5.6
Promedio	4.8

Figura 1. Máximo tiempo permitido para estar sin sistema por tipo de industria.

Aunque el estudio de la Universidad de Minnesota tiene más de 20 años, muchos expertos consideran que su grado de exactitud aún se mantiene.

Otro estudio, de la Universidad de Texas encontró que el 85% de la industria financiera depende directamente de sus sistemas de información, para subsistir en el negocio.

La figura 2, documenta algunas estadísticas con respecto al impacto que han causado algunos desastres en Chile.

10 principales desastres naturales en Chile para el periodo 1900-2010, ordenados por daño económico

N°	Desastre	Fecha	Daño en miles de dólares (US $)
1	Terremoto y tsunami	27-02-2010	30.000.000
2	Terremoto	03-03-1985	1.500.000
3	Terremoto	24-01-1939	920.000
4	Terremoto y tsunami	22-05-1960	550.000
5	Terremoto	06-05-1953	500.000
6	Incendio forestal	02-01-1999	280.000
7	Terremoto	08-07-1971	236.400
8	Terremoto	28-03-1965	235.000
9	Sequía	enero-1991	200.000
10	Inundación	24-05-2002	200.000

Figura 2. Estadísticas con respecto a desastres (Fuente ONEMI: 2010 - 2012)

Estadísticas recientes sobre los tipos más comunes de desastres que ocurren en nuestro territorio indican que los terremotos y tsunami son la causa más frecuente de desastres, pero también existen otras causas no tan devastadoras, pero con grandes pérdidas para las empresas también, las más comunes son los incendios, Interrupciones del suministro de energía eléctrica e interrupciones de servicio en las redes.

Ante un desastre, las compañías no solo enfrentan el costo económico implicado, hay otros costos indirectos que también deben tomarse en cuenta, tales como:

- Interrupciones en el flujo de caja
- Pérdida de clientes
- Pérdida de competitividad
- Erosión en la imagen del negocio
- Pérdida de incursión en el mercado
- Violaciones legales o regulatorias
- Pérdida de confianza en los inversionistas. (Ianna,1997)

2.1. Beneficios de un plan de recuperación por desastre

Entre los beneficios más destacados de implementar un plan de continuidad de negocio o de recuperación por desastre se tienen los siguientes:

- Le permiten a la organización evitar ciertos riesgos o mitigar el impacto de éstos al:
  - Minimizar potenciales pérdidas económicas
  - Disminuir la exposición a escenarios de desastre
  - Reducir la probabilidad de que ocurran.
  - Mejorar la capacidad de recuperar las operaciones normales del negocio.

- Ayuda a minimizar la probabilidad de interrupción de funciones críticas y a recuperar las operaciones en caso de crisis al:

- Reducir las interrupciones de la operación
- Asegurar la estabilidad organizacional

- Ayuda a identificar sistemas críticos y sensitivos dentro de la organización.
- Provee un procedimiento pre-planificado minimizando el tiempo de toma de decisiones en caso de desastre.
- Elimina la confusión y reduce la probabilidad de error humano debido al estrés que produce una crisis.
- Protege los activos de la organización incluyendo al recurso humano.
- Minimiza potenciales responsabilidades legales.
- Provee material de entrenamiento para nuevos empleados.

2.2. Procesos principales en la creación de un plan de recuperación

2.2.1. Análisis de riesgo (AR) y análisis de impacto al negocio (BIA)

El proceso de análisis de riesgos provee la base del plan de recuperación. Este análisis implica identificar las posibles amenazas que en caso de concretarse podrían traer resultados desastrosos a la organización. El proceso de razonamiento con respecto a las posibilidades de crisis, le brinda a la compañía una mejor idea de lo que es importante para ésta. La organización como un todo también obtiene un valioso entendimiento del mecanismo de desastre dando como resultado mejores planes de contingencia.

Como un complemento al análisis de riesgo, el análisis de impacto de negocio (BIA por sus siglas en inglés), determina el efecto que cada tipo de amenaza potencial tiene sobre las funciones o departamentos de la organización. Entre los tipos de criterio que pueden ser usados para evaluar este impacto se incluye:

- Servicio al cliente
- Operaciones internas
- Asuntos legales
- Asuntos financieros

Recolectar la siguiente información durante un análisis BIA puede cambiar o influenciar la estrategia de respaldo de información que utiliza la compañía:

- **¿Qué aplicaciones son críticas o vitales?** Esta tarea consiste en asignarle una prioridad a las aplicaciones que deben recuperarse en caso de desastre, o sea, es determinar qué aplicaciones debo recuperar primero que otras.
- **¿Cuál es la mínima configuración de hardware aceptable?** Una vez que las aplicaciones críticas han sido definidas, el siguiente paso es identificar el hardware o equipo sobre el que se desempeñan estas aplicaciones. Desde la perspectiva de recuperación por desastre se puede encontrar equipo que es utilizado tanto por aplicaciones críticas como por no-críticas, de ahí que en una situación de emergencia el equipo podría tener más capacidad de la necesaria ya que solo se utilizaría para correr las aplicaciones críticas. Esto puede llevar el análisis a un paso más adelante: planificar una mínima configuración de equipo para soportar todas las aplicaciones críticas. Esto aunque requiere de asistencia técnica durante el desastre, puede reducir significativamente los costos.
- **¿Cuántos usuarios?** El análisis también contempla el número de usuarios que necesitarían acceso a las aplicaciones para continuar con el negocio en una situación de emergencia. Independientemente de la cantidad, se debe planificar un lugar para que el personal realice su trabajo.
- **¿Cuáles son los requerimientos funcionales del negocio?** Paralelamente a los requerimientos de aplicaciones y usuarios, el análisis también debe identificar para cada tarea crítica o función de negocio qué entradas son requeridas y qué salidas son producidas. Este análisis también puede identificar cualquier necesidad de formas pre-impresas, servicios de impresión, fotocopiado, courier, fax, correo, etc.

El análisis BIA es la clave para el desarrollo de la mayoría de objetivos del plan de recuperación por desastre. Muchas de sus actividades involucran entrevistas al personal de sistemas y usuarios finales, esta información se recolecta y documenta de forma que pase a ser un activo más de la organización.

Los cuatro objetivos básicos de un análisis de riesgos y un análisis de impacto al negocio son:

1. Identificar los activos de la compañía y las funciones que son necesarias para la recuperación del negocio en caso de desastre y priorizarlas de acuerdo a su criticidad (BIA).
2. Identificar las amenazas más probables a los activos y funciones (AR).
3. Crear objetivos para el desarrollo de estrategias que eliminen los riesgos eliminables y minimicen el impacto de aquellos riesgos que no se pueden eliminar (AR).
4. Crear objetivos para el desarrollo de estrategias para el respaldo y/o recuperación de aquellas funciones que son críticas para el negocio y que podrían verse afectadas en un desastre.

2.2.2. Tiempo y punto de recuperación de datos

El objetivo de hacer copias de seguridad de los datos que consideramos críticas para el negocio es estar en disposición de recuperarlas en caso desastre o pérdida de datos.

Teniendo claro que el objetivo de las copias de seguridad es garantizar la recuperación de los datos, es decir, la disponibilidad de los datos, hay que tener claro en qué condiciones recuperamos estos datos.

Para identificar las condiciones de recuperación de los datos hay dos valores temporales que siempre debemos valorar a la hora de diseñar un sistema de copias de seguridad y que se conocen como RTO y RPO.

- El RTO (Recovery Time Objective) es el tiempo en que se tarda en recuperar los datos en caso de pérdida.

- El RPO (Recovery Point Objective) es el punto de recuperación de los datos. Es decir, en qué momento temporal anterior a la pérdida se recuperan los datos.

Para entender mejor el significado de estos dos valores, a continuación se representan en la figura 3, en modo de ejemplo, y en una escala temporal.

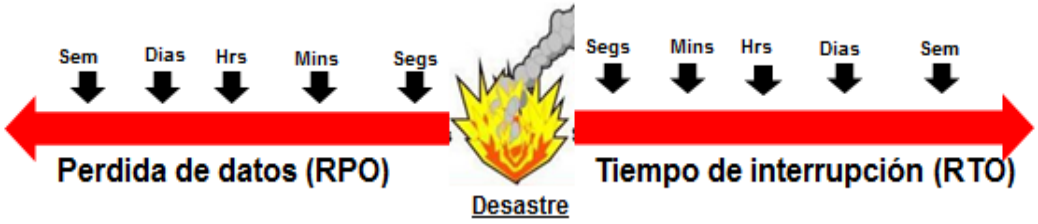


Figura 3. Escala temporal para RPO y RTO.

El período de tiempo en que los sistemas, aplicaciones o funciones deben ser recuperados. RTO se utilizan a menudo como la base para el desarrollo de estrategias de recuperación, y como un factor determinante en cuanto a si o no para aplicar las estrategias de recuperación durante una situación de desastre

El punto en el tiempo en que los sistemas y los datos deben ser restaurados. RPO, a menudo se utilizan como base para el desarrollo de las estrategias de copia de seguridad.

2.2.3. Identificación y priorización de las funciones operacionales

En el contexto del procesamiento de datos, las aplicaciones pueden clasificarse usando el siguiente espectro de tolerancia:

- **Críticas:** Estas funciones no pueden ser ejecutadas a menos que se tenga un ambiente idéntico al de la operación normal de la compañía. Las aplicaciones críticas no pueden ser reemplazadas por métodos manuales bajo ninguna circunstancia. La tolerancia a la interrupción es muy baja y el costo muy alto. Bajo estas características, la estrategia para recuperar estas aplicaciones debe tomar en cuenta el equipo necesario en un sitio alterno y un sistema de respaldos que se pueda cargar en este equipo de manera que se pueda reiniciar la funcionalidad afectada.
- **Vitales:** Estas funciones no pueden ser ejecutadas por medios manuales o al menos solo se pueden ejecutar manualmente por un corto periodo de tiempo. Tienen un poco más de tolerancia a la interrupción que las funciones críticas podrían recuperarse en menos de cinco días sin causar mayores contratiempos.
- **Sensitiva:** Esas funciones pueden ejecutarse por medios manuales con dificultad pero a un costo tolerable durante un periodo de tiempo más largo que el que se requiere en las aplicaciones vitales.
- **No Críticas:** Estas aplicaciones o funciones pueden ser interrumpidas por un extenso periodo de tiempo a un bajo costo para la compañía.

2.2.4. Identificación de las amenazas a los activos y funciones

Una vez que la criticidad de las funciones ha sido identificada, el siguiente objetivo es realizar un análisis de riesgo e identificar qué amenazas existen a las actividades de procesamiento normal del negocio.

Se considera una amenaza para las organizaciones, aquellos eventos o situaciones que podrían impactar directa o indirectamente la compañía afectando

total o parcialmente la razón de ser de la misma. Las potenciales amenazas que pueden causar un desastre en una organización se clasifican en cuatro grandes categorías:

ACCIDENTAL: Por ejemplo, pérdida de electricidad, accidente de transporte, contaminación química, humo tóxico, etc.

NATURAL: Inundaciones, terremotos, huracanes, tornados, etc.

INTERNAS: Sabotaje, robo, violencia de empleados o ex empleados, etc.

CONFLICTO ARMADO: Terrorismo, secuestro, etc.

2.2.5. Identificación de los medios de almacenamiento de datos y los sitios de recuperación

Uno de los elementos clave en cualquier plan de recuperación por desastre es tener un respaldo actualizado de programas críticos y datos los cuales puedan ser utilizados en caso de desastre. Esto es tan obvio que muchos ejecutivos sin experiencia podrían estar ignorando lo obvio, lo cual en determinadas circunstancias traería consecuencias incuantificables. Hay muchas estrategias para respaldar los activos de una organización:

Respaldo de datos

Un respaldo es una copia de un conjunto de datos definido. En un ambiente bien definido, estos respaldos usualmente son guardados en cintas o discos los cuales deben almacenarse en un sitio que no sea el lugar donde se encuentran los datos operativos de manera que los respaldos sobrevivan a un evento de desastre que destruya la fuente de datos principal.

Objetivos de una cinta de respaldo: Siempre se debe tener en mente que el objetivo general de una cinta de respaldo es que los datos puedan ser

recuperados, en caso de cualquier tipo de pérdida de información. En general, la estrategia de respaldos debe formularse para cumplir con los siguientes objetivos.

- Entender los objetivos de negocio de forma que se cuente con un ambiente de respaldo y recuperación de datos acorde a estos objetivos.
- Permitir que los servicios de información puedan ser reiniciados tan rápido como físicamente sea posible luego de alguna falla en los sistemas de información.
- Permitir un acceso a los datos respaldados acorde a las necesidades del negocio.
- Cumplir con las políticas regulatorias y de negocio en cuanto a los requerimientos de retención de datos.
- Cumplir con las metas de recuperación de datos en caso de desastre permitiéndole al negocio volver a su estado normal.

Ante la pregunta, ¿por qué se respaldan los datos?, cuestionamiento que aunque parece ser trivial, requiere ser contestado para cada dato en la empresa. Algunas de las respuestas más comunes son:

- Requerimientos de negocio.
- Recuperación en caso de desastre.
- Protección en caso de fallas en las aplicaciones o programas.
- Protección en caso de error en el usuario.
- Acuerdos específicos con los clientes o usuarios (“Service Level Agreements” – SLAs).
- Requerimiento legal.

Se necesita entender qué datos y qué sistemas caen dentro de cada una de las categorías anteriores. Las entrevistas con los dueños o administradores de datos permiten categorizar de mejor forma los datos a respaldar.

Cuando se diseña o actualiza una estrategia de respaldos y recuperación de información se deben tomar en cuenta los siguientes factores, los cuales le agregan complejidad a la estrategia utilizada:

- Capacidad para respaldar todos los datos: Para que la estrategia de respaldo sea útil, ésta debe garantizar que todos los datos están siendo respaldados.
- Frecuencia: La frecuencia de respaldo es esencialmente un balance entre recursos (redes, capacidad de procesador, equipo, acceso a la aplicaciones) y la necesidad de datos actualizados.
- Integración de todos los sistemas administradores de datos. En grandes organizaciones se pueden tener más de un sistema administrador de base de datos, cada uno con su propia forma de administrar los respaldos. La estrategia debe conjuntar las necesidades de todos estos sistemas.
- Disponibilidad continúa. En muchas organizaciones los sistemas deben estar disponibles todo el tiempo. Por lo tanto la estrategia debe adaptarse a la necesidad de disponibilidad de datos de la organización. También es importante valorar si se requiere una ventana de tiempo en la cual no pueden ejecutarse cierto debido a que se está generando el respaldo.
- Administración de los medios. Requerimientos regulatorios o de negocio pueden necesitar de grandes cantidades de medios de almacenamiento, lo cual puede hacer más complejo su administración.

Almacenamiento en sitio alterno

Almacenar los activos de la empresa, en un sitio alejado al lugar donde normalmente se desarrollan las operaciones de una compañía, es un asunto clave en el éxito de un plan de recuperación por desastre. Si no hay datos y procesos para recuperar entonces la recuperación no será posible. Para garantizar que la

información y los activos en general no sean consumidos durante el desastre, éstos deben ser respaldados en un sitio seguro, preferiblemente en uno diferente al productivo. En respuesta a esta necesidad de sentido común, muchas compañías se deciden por contratar los servicios de empresas dedicadas a este negocio. Este tipo de empresas se especializan en resguardar datos y equipo para que sean utilizados eficientemente en caso de desastre.

Al contratar los servicios de un tercero, para resguardar los activos de una empresa, se deben tomar en cuenta los siguientes aspectos:

- Acceso restringido.
- Facilidad de acceso a los activos las 24 horas del día, los 365 días del año.
- Construcción resistente a los desastres.
- Sistemas para prevención de incendios.
- Fuentes alternas de poder.
- Controles ambientales adecuados.
- Protección ante magnetismos.
- Comunicaciones a prueba de fallas.
- Personal de seguridad con el entrenamiento adecuado.

2.3. Creación del plan de validación o simulación del DRP

Los planes de recuperación por desastre son documentos vivos, y deben actualizarse cada vez que se requiera de manera que reflejen los cambios en las operaciones del negocio, cambios de personal e incorporaciones de cambios para corregir deficiencias encontradas en la etapa de pruebas.

Las mejores prácticas dictan que los planes se deben actualizar al menos una vez al año. Sin embargo las condiciones de la organización podrían hacer que se

requieran revisiones más continuas. La siguiente lista ayuda a determinar cuándo un plan debe ser actualizado:

- Cambios en el núcleo del sistema, tecnología o procesos de negocio La dependencia en la tecnología existente o en nueva tecnología se ve incrementada.
- Reestructuración organizacional (adquisición, “outsourcing”, salida de personal clave, etc.).
- El cliente, reguladores, inversionistas, aseguradores o acreditadores muestran interés en los esfuerzos relacionados con el DRP.
- Pérdida financiera (desastres anteriores han provocado pérdidas económicas).
- Caídas del sistema (desastres anteriores han provocado caídas del sistema).
- Incremento en las amenazas de desastre.
- El plan no ha sido actualizado o validado en el último año.

Las pruebas dan un alto grado de confiabilidad de que el plan funciona. Cada problema es diferente, pero un plan que ha sido validado tiene muchas probabilidades de ser exitoso cuando se requiera aplicar. Entre los beneficios más importantes que se obtienen al probar el plan se encuentran:

- Lograr demostrar que el plan funciona.
- Identificar planes de contingencias que hasta ese momento eran desconocidos.
- Verificar la disponibilidad de recursos.
- Determinar la duración verdadera del tiempo de recuperación.
- Entrenar al personal asignado a roles de recuperación.
- Hacer que el personal se identifique mejor con el plan de recuperación.
- Determinar las mejoras necesarias y debilidades del plan.

Los pasos para construir el plan son los siguientes:

1. Definición de los objetivos de las pruebas.
   a. Probar que el plan realmente funciona.
   b. Verificar que el sitio alterno cumple con las necesidades del DRP.
   c. Identificar las deficiencias y omisiones del DRP.
   d. Proveer entrenamiento.
2. Definición del personal requerido.
3. Definición del cronograma de las pruebas.
4. Determinación de la metodología de las pruebas, ya sea por medio de:
   a. Revisión Estructural: Esta prueba involucra crear un equipo de pruebas que analizará en detalle la totalidad del plan haciendo una revisión meticulosa de cada paso descrito en el plan. Esto asegura que cada paso está bien escrito y se entiende. Este mínimo escenario de pruebas al menos ayuda a que los equipos se comuniquen y se familiaricen con el plan como un todo.
   b. Checklist: Este método consiste en distribuir copias del plan a cada equipo el cual lo revisa y chequea los puntos listados asegurándose que el plan contiene todas las actividades necesarias.
   c. Pruebas de simulación: Las áreas operativas y de soporte se juntan para ejecutar el plan. Dado que es una simulación, la prueba consiste en instalar los equipos y sistemas en el sitio alterno.
   d. Pruebas paralelas: Este tipo de pruebas validan si el plan está listo o no, ya que la prueba consiste en instalar el equipo y los sistemas críticos en el sitio alterno y verificar que efectivamente el plan funciona. Cualquier discrepancia o diferencia entre los sistemas reales y los sistemas en el sitio alterno se resuelven y documentan de inmediato.
   e. Pruebas de interrupción completa: En esta prueba, las operaciones normales son suspendidas completamente y la operación se traslada al sitio alterno usando el material y personal disponible en el sitio remoto según el plan. Este tipo de pruebas tiene un riesgo muy alto ya que

podría fallar el paso de devolverse al ambiente normal generando una alteración en las operaciones regulares del negocio.

5. Definición de los resultados esperados de las pruebas: Para determinar la efectividad del DRP los resultados de las pruebas deben ser medidos contra resultados esperados que fueron predefinidos. Si los resultados no son los esperados se puede bajar la expectativa de los resultados o incrementar la efectividad de los procedimientos de prueba.
6. Planificación de los ejercicios de prueba con anticipación: Se debe escribir el plan de pruebas del DRP, también se deben detallar los pasos exactos que se seguirán durante la fase de pruebas, el personal o departamento involucrado y los resultados esperados.
7. Coordinación, ejecución y documentación del plan de pruebas.
8. Evaluación de los resultados: ¿Los resultados de las pruebas son los que esperaba?, si no, ¿qué se debe hacer para corregir el problema? ¿El problema se presenta por la forma en que se ejecutaron las pruebas?

2.4. Errores más comunes al formular un plan de recuperación en caso de desastre

Desarrollar y ejecutar un buen plan de recuperación ante desastre es el primer paso, sin embargo el esfuerzo no termina ahí. Un plan requiere modificaciones o correcciones tales como omisiones y errores detectados durante la etapa de desarrollo y pruebas. A continuación una lista de los principales errores que se cometen al desarrollar el plan.

Confiar ciegamente en el plan: Muchas organizaciones creen que el plan es suficiente, sin embargo éste será útil en la medida en que se le de mantenimiento y se compruebe su efectividad.

Alcance limitado: Un plan incompleto no abarcará todas las necesidades de recuperación que tiene la organización. El plan requiere cubrir procesos de

negocio, recuperación de sistemas, funciones de “back-office” y reemplazo de personal clave si es necesario.

Débil priorización: Hay una necesidad de priorizar las funciones claves de la organización. Sin ésta tarea, se gastará mucho tiempo y dinero en la recuperación de funciones que no son cruciales para la sobrevivencia del negocio.

Planes no actualizados: El plan debe ser actualizado, especialmente cuando se realizan cambios en los procesos productivos.

Ausencia de liderazgo: Se requiere en estos proyectos de alguien con poder de liderazgo, influencia, sentido de prioridad y de organización.

Problemas de comunicación: Es necesaria una comunicación clara y precisa con los empleados, proveedores, socios y clientes.

Pérdida de controles de seguridad: Durante el proceso de recuperación, los controles de seguridad podrían dejarse en un segundo plano resultando en una exposición mayor al riesgo.

Pérdida de apoyo del negocio: La continuidad del negocio y la recuperación por desastre no es solo un asunto del área de tecnología. Se requiere involucrar a todas las áreas de negocio en las etapas de análisis de riesgo e impacto.

2.5. Administración de proyecto

De acuerdo a los elementos involucrados en la creación de un plan de recuperación por desastre, la metodología y los principios que provee el PMI se adaptan perfectamente a las necesidades y expectativas generadas al crear un plan de esta índole. Entre los elementos de la administración de proyectos, propia de la metodología del PMI, se puede nombrar la administración de riesgos como el eje principal del proyecto. Con respecto al proceso de Administración de Riesgos,

es importante mencionar que se introduce en este proyecto, una variación a este proceso, a saber, la metodología ABCD, desarrollada por la transnacional EDS (Electronic Data Systems), líder mundial en “Outsourcing” de servicios tecnológicos. Más adelante se estará ampliando los detalles de esta metodología.

También se utiliza la etapa de planificación, como principal área de conocimiento aplicada en este tipo de proyectos, ya que brinda el sentido de pro actividad que necesita un esfuerzo de este tipo.

Sin embargo, hacen falta algunos elementos igual de importantes a los anteriormente citados, que en la metodología del PMI no se profundiza lo necesario para un proyecto como la recuperación en caso de desastre, a saber, la administración de cambios como proceso necesario para mantener siempre vigente el plan de recuperación y la administración de la configuración, como proceso vital en la identificación de equipo y aplicaciones necesarias para mantener la operación normal de una organización. Estos dos elementos se contemplan ampliamente en el marco de trabajo conocido como ITIL (Information Technology Infrastructure Library) desarrollado en Inglaterra en la década de los 80’s por la Agencia Gubernamental “Central Computer and Telecommunications Agency” (CCTA).

Por lo anterior, este proyecto debe tener una mezcla de varios métodos: Metodología del PMI, el “framework” ITIL y la metodología ABCD de EDS para la administración de riesgos. Esto garantiza que los elementos esenciales del plan, durante todo su ciclo de vida, estarán soportados por las mejores prácticas que ofrecen estas metodologías.

2.6. El proceso ABCD de administración de riesgo, PMI / EDS Riesgo

La escala ABCD está definida para múltiples usos a lo largo de la metodología y siempre significa lo mismo: A es siempre bueno y D es siempre malo, B y C

expresan tendencias a ambos extremos. Por lo tanto siempre se busca convertir las D y C en A y B.

A significa muy bueno, alta confiabilidad, sin importancia.
B significa bueno, confiabilidad razonable, no muy importante.
C significa pobre, incómodo, importante.
D significa muy pobre, poca o nula confiabilidad, críticamente importante.

El principio, en general, busca que se tome una opción entre bueno, alta confiabilidad y malo, baja confiabilidad.

El riesgo está inherente en todos los aspectos de una organización y se puede ver desde cuatro puntos de vista: financiero, inversionista, operacional y desde un enfoque de cambios por medio de programas y proyectos tal y como se muestra en la Figura 4.

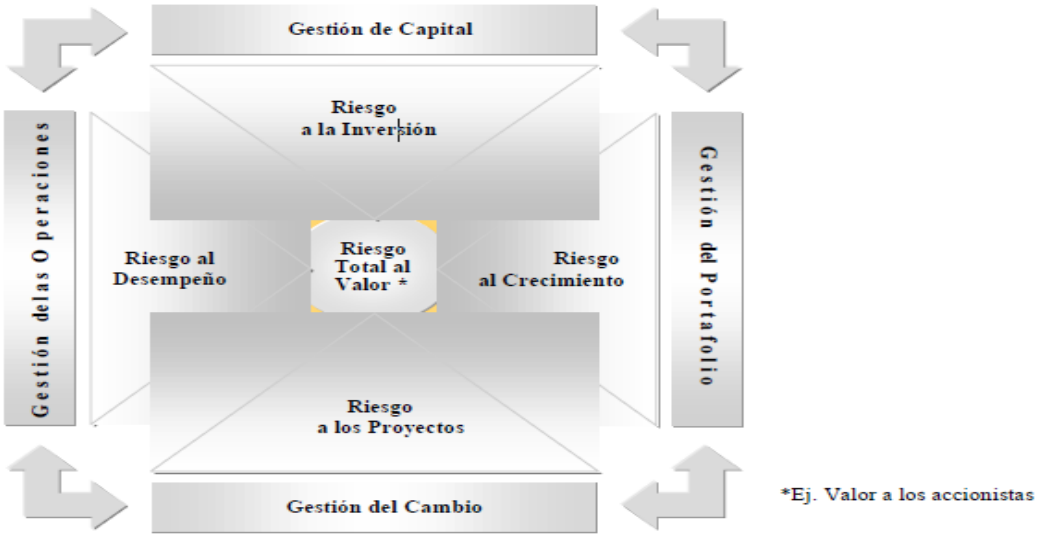


Figura 4. Multi-Dimensionalidad del Riesgo.

El riesgo es multi-dimensional y puede tener muchos escenarios y consecuencias, tanto positivas como negativas, sin embargo lo común es verlo en términos de posibles pérdidas e impacto negativo.

Muchos riesgos se relacionan con el día a día de los procesos de una organización, sin embargo, es cuando se presentan cambios en estos procesos que el riesgo aumenta, tanto en la probabilidad de que se presente como en el impacto.

2.6.1. Administración del riesgo

La siguiente definición de Administración de Riesgos, tomada del modelo de madurez CMMI:

"La administración de riesgos es un proceso técnico y organizado para identificar lo que puede causar daño o pérdida (identificación de riesgos). Evalúa y cuantifica los riesgos identificados y desarrolla e implementa, si es necesario, un procedimiento apropiado para prevenir o manejar las causas que originan los riesgos. Típicamente, la administración de riesgos es ejecutada por las unidades organizacionales de proyectos o desarrollo de productos".

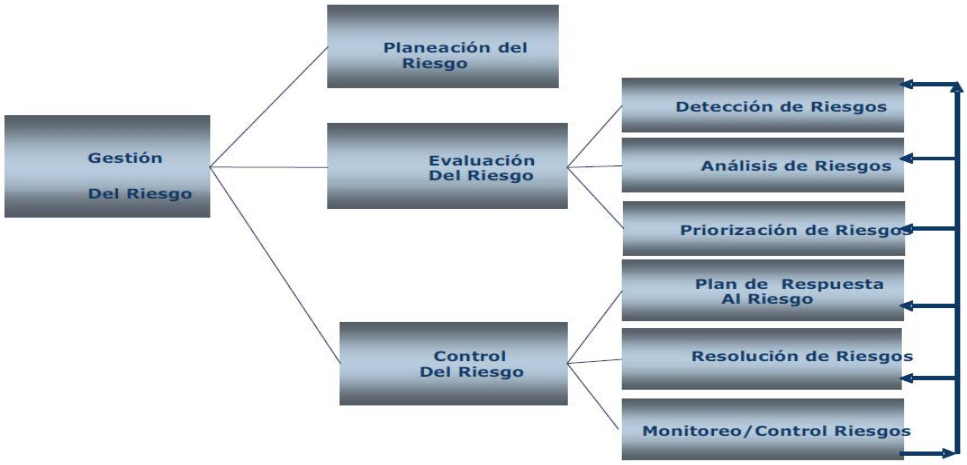


Figura 5. Proceso de Administración de Riesgos.

La gestión de riesgo es el punto central de la definición de una estrategia de seguridad perfectamente alineada con la visión de las empresas, dentro de su entorno de operación. La figura 5, muestra los elementos que componen el

proceso de administración de riesgo, identificando, evaluando y controlando los posibles riesgos.

2.6.2. Principios básicos de la metodología ABCD

La metodología de administración de riesgos ABCD, nació a partir de una evaluación detallada de los problemas que a menudo se encuentran en la administración de proyectos, y de las potenciales desventajas de los procesos tradicionales de administración de riesgos. Se tomaron en cuenta los buenos y malos principios y se introdujeron nuevas técnicas para atacar las deficiencias claves. El resultado fue ABCD, metodología que ha demostrado resultados tangibles en un gran número de implementaciones a través de muchas organizaciones. La metodología puede aplicarse a cualquier elemento del trabajo, pequeño o grande.

Comunicación de Supuestos

Cuando se creó la metodología ABCD, la fuente de falla que más frecuentemente se identificó fue la pérdida de calidad en la comunicación, tanto dentro de los grupos que atendían los riesgos como entre los grupos como entes individuales.

La mayoría de los problemas que ocurrieron pudieron evitarse si la información hubiera sido, efectivamente, comunicada y a tiempo. Sin embargo, hay mucha información que es difícil decidir si es necesario comunicarla y a quien debe comunicarse. Para superar esto, ABCD define los supuestos en la etapa de planificación. Cada elemento importante que surge al planear una serie de futuros eventos puede ser capturado y monitoreados como supuestos, por ejemplo:

- El trabajo se mide sobre una base de supuestos.
- Los hitos del proyecto son definidos de acuerdo a los supuestos.
- Las dependencias están basadas en supuestos.
- Los recursos se planean de acuerdo a los supuestos, etc.

- Por lo tanto, la captura, análisis y comunicación de supuestos son factores críticos para el éxito de los proyectos y forman el núcleo de la metodología ABCD para la administración de riesgos en EDS.

El Plan

Las probabilidades de éxito de un proyecto se incrementan al identificar lo que se necesita hacer, por quién y cuándo (planificación). Se dice que prácticamente no hay planes perfectos debido a que las actividades de un plan serán llevadas a cabo en el futuro y usualmente, hay un grado de incertidumbre asociado a los eventos futuros.

En ABCD, los riesgos son identificados al capturar y analizar los supuestos que se han hecho mientras se crea el plan. De esta forma, los supuestos hechos durante la planificación son utilizados para identificar lo que podría atentar contra el alcance de los objetivos del proyecto. Por lo tanto, los supuestos están efectivamente referenciados al plan y el plan provee un mayor enfoque hacia el proceso de administración de riesgos.

Este enfoque mantiene los riesgos específicos con una visión de futuro y ayuda a asegurar que el plan se mantenga siempre actualizado.

Incertidumbre y Riesgo

El riesgo es inherente a la incertidumbre, el nivel de incertidumbre varía en el tiempo según cambian las circunstancias. Los mejores jueces, con respecto a la incertidumbre, son aquellos a los que se les pide que realicen las tareas de estimación para el plan. En la mayoría de circunstancias, los que tienen que realizar el trabajo son las personas más apropiadas para hacer una evaluación de riesgos.

Combinar este principio con la definición de supuestos basados en el plan, conduce a una mejor clasificación de supuestos tanto en la calidad de los mismos

como en el grado de incertidumbre. El análisis se concentra en las áreas del proyecto donde se conoce menos y surgen las interdependencias que a menudo representan los riesgos más altos.

2.6.3. Evaluando el riesgo utilizando la escala ABCD

Utilizando esos simples términos de A, B, C y D para expresar el grado de incertidumbre, es posible motivar a las personas a revelar rangos de incertidumbre más amplios. También ayuda a persuadir a la gente a proveer una evaluación de riesgos cuando quizás no tenían planeado hacerlo. Esto es vital para obtener información sobre la incertidumbre que podría existir en el fondo de un proyecto sin haber preguntado aún por los riesgos.

La metodología ABCD consiste en un proceso cíclico que lógicamente progresa a través de:

- Evaluación de riesgos.
- Priorización de riesgos.
- Control de riesgos.

2.6.4. Aplicando la metodología ABCD

La metodología es cíclica, con "issues"[6] , supuestos y riesgos siguiendo una sola vía de flujo.

Los "issues": Ocurren principalmente al inicio de cualquier actividad ya que la ruta a seguir no está clara, sin embargo pueden surgir en cualquier momento del ciclo de vida del proyecto.

Los supuestos: Se definen en la fase de planificación, ya sea al inicio o si se requiere re-planear en algún punto del ciclo de vida del proyecto, también surgen

[6] ISSUES, Asuntos pendientes de resolver.

como respuesta a “issues” no atendidos. El análisis de supuestos entonces sirve para identificar los riesgos.

Los riesgos: Que no son administrados de forma exitosa podrían impactar y convertirse en uno o más “issues” y así se mantiene el ciclo.

Definición de “issues”

Los “issues” son problemas o interrogantes que están pendientes de la fase de planeamiento. Para dar una respuesta de calidad, los “issues” deben formularse en forma de pregunta, posteriormente deben ser clasificados en términos de criticidad con una fecha de solución requerida.

Un “issue” puede estar relacionado con problemas identificados durante el progreso del proyecto, tales “issues” ya están teniendo un impacto negativo sobre los hitos/eventos. Esos “issues” requieren acciones para identificarlos y resolverlos de forma inmediata.

Los “issues” son:

- Interrogantes que requieren ser respondidas (se deben estructurar en forma de pregunta).
- Están relacionados con los problemas vigentes y requieren una respuesta inmediata (usualmente dentro de 5 a 7 días).
- Surgen cuando no es posible obtener una decisión/respuesta estable sin escalamiento.

Por ejemplo, un “issue” podría iniciarse con lo siguiente: “Tengo un issue con el hardware”. Algunos posibles “issues” ABCD que se derivan de éste son:

- “¿Cómo me aseguro que los servidores estarán entregados a tiempo?”
- “¿Qué se puede hacer para modelar la carga del sistema?”

- “¿Qué plataforma debe seleccionar el usuario?”

NOTA: La respuesta a un “issue” nunca debe ser SI o NO.

Priorización de Issues

A los “issues” se les debe otorgar una clasificación según su criticidad de acuerdo a la importancia relativa de cada uno de estos. Las clasificaciones de criticidad son ROJAS, AMARILLAS y VERDES.

Es importante definir lo que cada clasificación significa de acuerdo a cada proyecto. Entender la relación de cada clasificación ayuda a mantener la consistencia en el proceso de priorización. Algunas posibilidades se muestran a continuación en la Figura 6:

CRITICIDAD	RELATIVO AL PRESUPUESTO	IMPACTO SI NO SE ATIENDE	RELATIVO AL COSTO
ROJO	>50% del presupuesto	El trabajo se detendrá	No hay idea
AMARILLO	>20% del presupuesto	Serios daños que disminuirán el progreso. Doloroso pero el trabajo continúa	Impacto mayor en el costo
VERDE	> 5% del presupuesto	Daños menores	Impacto moderado en el costo

Figura 6. Clasificaciones por criticidad

Los “issues” deben ser de vida corta, dado que son problemas que deben priorizarse lo más pronto posible, por lo tanto debe identificarse y registrarse la fecha para la cual se requiere una fecha de respuesta. La fecha de resolución y el

grado de criticidad, juntos, proveen el proceso de priorización de cada “issue”. Por ejemplo un “issue” ROJO que se debe resolverse en 5 días, es más importante que un “issue” AMARILLO, con una resolución en 2 semanas.

Cerrando los “issues”

Los issues se cierran cuando se da una de estas situaciones:

- Obtener una respuesta satisfactoria.
- Un evento (ej. Un cambio en la política) que resuelve o elimina el “issue”.
- Hacer un supuesto (el “issue” se convierte en supuesto) que mueve el “issue” para más adelante.

Análisis de Supuestos

El análisis de supuestos es la piedra angular de la metodología ABCD, este proceso puede realizarse en cualquier etapa del proyecto, sin embargo el proceso de análisis debe iniciarse tan pronto sea posible, con el objeto de capturar los “issues” que pueden resultar en supuestos.

Los supuestos se formulan para permitir el progreso del planeamiento y desarrollo de la solución. Si los supuestos son importantes y resultan ser incorrectos, pondrán en peligro el éxito del proyecto. Estos supuestos críticos son el corazón de los riesgos de cualquier pieza de trabajo.

Identificando fuentes de supuestos

Los supuestos se capturan generalmente por entrevistas, sin embargo también pueden determinarse a través de sesiones de trabajo, reuniones o de cualquiera involucrado en el proyecto. La mayoría de supuestos se esperan de los “stakeholders”[7]. Se puede agregar un ítem en la agenda de las juntas para analizar los supuestos o se pueden realizar sesiones exclusivas de manera que se le dé seguimiento al estatus de los supuestos o buscando nuevos supuestos.

[7] Stakeholders, son aquellas personas u organizaciones que están activamente involucrados en el proyecto, o cuyos intereses pueden verse afectados, positiva o negativamente, también pueden ejercer influencia en el proyecto y sus resultados.

Los supuestos pueden ser explícitos y se registran en muchos documentos, por ejemplo, especificaciones, estándares, propuestas, modelos de costo y por supuesto en los planes. Muchos supuestos son implícitos y solo se revelan al hacer un análisis detallado. Al principio es normal que existan muchos “issues” y pocos supuestos. Sin embargo, una vez que el proceso de planeamiento está en camino, los “issues” son efectivamente cerrados al generarse nuevos supuestos.

Formulando un Supuesto

Una buena forma de generar un supuesto es preguntarse “¿qué se necesita que ocurra y cuándo para que este trabajo sea exitoso?” Similarmente, “¿Quién debe hacer qué y cuándo?”.

Los supuestos deben ser sentencias específicas con respecto a lo que se necesita que ocurra para que se dé un resultado exitoso. Los supuestos deben formularse en futuro, ser fácilmente entendible, referirse solo a un aspecto del trabajo y ser descritos en forma positiva.

Supuestos de alto nivel como “El proyecto será exitoso” o “Los beneficios buscados serán conocidos” son de poco valor, ya que no indican que algo puede causar una falla. La pregunta que siempre se debe hacer es “¿por qué?”, aunque de otras preguntas abiertas también se puede obtener información valiosa.

Ejemplo: Refinando un supuesto

- “El proyecto será exitoso” – pregunta: ¿por qué podría fallar el proyecto?
- “Suficientes recursos será muy valioso” – pregunta: ¿qué significa suficientes recursos? y, ¿por qué podrían no estar los recursos disponibles?
- “Los especialistas en base de datos estarán disponibles a pesar del choque con el proyecto XYZ” – pregunta: ¿Cuántos especialistas en base de datos se necesitan?

- “8 especialistas en bases de datos estarán disponibles a pesar del choque con el proyecto XYZ” – pregunta: ¿Cuándo se necesitan los 8 especialistas en base de datos?
- “8 especialistas estarán disponibles en las semanas 23-29, a pesar del choque con el proyecto XYZ” – Este debe ser el supuesto final

2.6.5. Evaluación de la sensibilidad/estabilidad de los riesgos

Muchos supuestos planteados son considerados de alta calidad ya que están basados sobre una base relevante de conocimiento o experiencia. Otros supuestos son insignificantes al compararlos con los objetivos generales del proyecto. Es normal que ninguno de estos tipos de supuesto sea fuente de riesgos por lo que se requiere un método para filtrar los supuestos de alta calidad o los supuestos no importantes para que se les preste la debida atención.

El método de identificación de riesgos utiliza el conocimiento de los miembros clave del equipo para evaluar dos parámetros que son vitales para todos los supuestos.

Sensibilidad:

¿Qué tan importante es para los objetivos críticos (negocio, ej. Hitos y entregables), si el supuesto resulta ser incorrecto?

- Importa poco (impacto menor si el supuesto es incorrecto).
- Importa pero el impacto es manejable.
- Importa y el impacto es significativo.
- Importa mucho ya que el impacto es crítico

Estabilidad:

¿Qué tan confiable es el hecho de que el supuesto sea correcto?

- Hay mucha confianza de que el supuesto esté estable.
- Bastante confiable.
- Incómodo.

- Muy incómodo (es muy probable que el supuesto resulte ser incorrecto).

Usar este método conduce a un análisis sistemático de los supuestos en los cuales se base el proyecto. Las clasificaciones pueden estar representadas en un diagrama de Sensibilidad/Estabilidad como el que se muestra en la Figura 7.

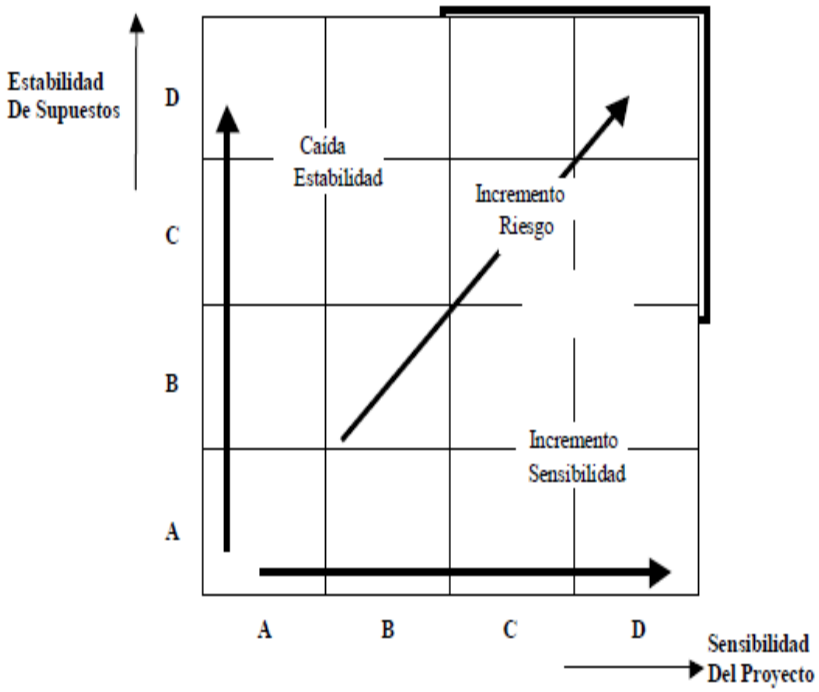


Figura 7. Diagrama de Sensibilidad/Estabilidad

La clasificación de un supuesto dentro del diagrama de sensibilidad/estabilidad, mientras sea más alejada de los puntos AA o BB, como indican las flechas en la figura 7, el supuesto tendrá una clasificación más riesgosa.

Documentando las razones de la clasificación de supuestos

Es parte integral de la metodología, que se registren las razones por las cuales se clasificó un supuesto dentro del diagrama Sensibilidad/Estabilidad. Este registro le da a cualquiera que revise esta clasificación un claro entendimiento del por qué un supuesto se clasificó de determinada forma. Esto mejora la comunicación y le permite al revisor/lector cuestionar las clasificaciones si existe

información actualizada o adicional que pueda cambiar estas clasificaciones. De esta forma, a través de la búsqueda de información de calidad y de una comunicación abierta, es posible identificar riesgos que de otra forma no hubiera sido posible identificarlos.

Adicionalmente, cuando se identifica un riesgo durante la clasificación de supuestos, la razón de sensibilidad provee un puntero al impacto de ese riesgo y la razón de estabilidad muestra un claro indicador de qué acción(es) tomar para mitigar el riesgo.

2.6.6. Cerrando los supuestos

Los supuestos se cierran cuando se demuestra o se tiene certeza de que los mismos son correctos o incorrectos, si son correctos se convierten en hechos. En el caso de los supuestos incorrectos, que soportan un riesgo, el supuesto se cerrará si el riesgo impacta.

2.6.7. Clasificación de supuestos

Los supuestos y riesgos son identificados por medio del análisis de supuestos, otorgando a cada supuesto una clasificación de sensibilidad y estabilidad. Para ayudar a entender, la clasificación de sensibilidad se pone primero cuando se están mostrando ambas clasificaciones en forma de doble letra.

Donde la clasificación de sensibilidad sea AA, AB, BA o BB, significa que el supuesto no es crucial para el proyecto y es normal que se compruebe que es verdadero. En estos casos no es esencial que se tomen acciones específicas, únicamente se deben monitorear en intervalos regulares hasta que el evento haya pasado.

Las clasificaciones AC, AD, BC, BD, CA, CB, DA y DB son riesgos potenciales. Esto es porque son inestables o sensibles. Esos supuestos deben ser

revisados con los expertos de forma regular y se deben identificar acciones que mantendrán bajas las clasificaciones.

Las clasificaciones CC, CD, DC y DD son consideradas para representar a los riesgos del proyecto. Esos riesgos requieren acciones para mantenerlos bajo control.

2.6.8. Formulación de riesgos

La formulación de riesgos es convertir en riesgo el supuesto añadiendo “Si no, entonces”, dejando claro el impacto si el supuesto resulta ser incorrecto.

Por ejemplo:
El supuesto es que....
“Seis desarrolladores en Oracle estarán disponibles para la captura de requerimientos iniciando el 12 de Febrero, a pesar de las demandas del proyecto XYZ, asegurando que esta actividad en la ruta crítica esté finalizada el 25 de Febrero”

Si no, entonces (el impacto es)...

“Actividad de la ruta crítica (12 al 25 de Febrero) se atrasará afectando la fecha de implementación del proyecto (actualmente para el 1 de Octubre)”.

Es importante expresar todas las consecuencias del riesgo, o al menos describir el impacto inmediato y el último.

Es importante recordar que la clasificación de supuestos irá cambiando conforme avanza el proyecto. Por esta razón, el análisis de supuestos es un proceso continuo con revisiones regulares a lo largo del ciclo de vida del proyecto.

2.6.9. Evaluación de riesgos

Los parámetros utilizados en ABCD para la evaluación de riesgos son:

- Criticidad
- Control
- Probabilidad
- Tiempo

Criticidad

La criticidad es usada para mostrar el impacto del riesgo sobre los factores críticos de éxito (FCEs) del proyecto. Generalmente se usa como el medio principal para priorizar los riesgos, aunque es preferible un proceso de priorización completo usando todos los parámetros. La criticidad está descrita en términos de "semáforo", rojo, amarillo o verde según los FCEs.

Es importante que se considere la criticidad de un riesgo en todos los niveles del proyecto. Por ejemplo un riesgo puede tener un impacto significativo sobre un hito, pero la criticidad del riesgo dependerá también de la criticidad del hito en los FCEs del proyecto en general.

Por ejemplo, en el caso de un proyecto que es parte de un programa:

Rojo

- Impacto crítico – El trabajo se detendrá en un proyecto crítico, con un efecto negativo en los entregables del programa. Como resultado, los objetivos no serán alcanzados, o,
- Impacto inaceptable en los costos para el negocio, o,
- No hay posibilidades de un plan de contingencias al menos aceptable, o,
- Impacto críticos en los negocios del cliente.

Amarillo

- Impacto significativo en los objetivos del proyecto, o,

- Atraso de un proyecto no crítico, o,
- Impacto significativo a los costos del proyecto o negocio, o,
- Plan de contingencia difícil de obtener, o,
- Impacto significativo en los negocios del cliente

Verde

- Impacto menor localizado en los objetivos del proyecto, o,
- Impacto menor en el costo, o,
- Plan de contingencia identificado y aceptable, o,
- Impacto menor en los negocios del cliente

Control

El control se representará como una métrica de confianza, de que el riesgo será administrado. La clasificación para el control, normalmente se asigna después de que el riesgo ha sido revisado y discutido por los líderes del equipo. La clasificación puede ser interpretada de la siguiente manera:

Muy Confiable: La administración puede tener mucho control sobre el riesgo. Hay planes de acción que demuestran ser satisfactorios.

Bastante Confiable: El riesgo, de forma general está bajo control. Hay un mínimo de planes de acción identificados.

Incómodo: El riesgo, en general está fuera de control. Hay un mínimo de planes de acción identificados.

Fuera de Control: No hay acciones de respuesta que sean efectivas. No hay planes para administrar el riesgo o los planes que hay fallaron. No hay control de la administración. El riesgo debe ser escalado a un mayor nivel de influencia, donde se tenga la autoridad suficiente para tomar decisiones y/o acciones para mitigar el riesgo.

Probabilidad

La probabilidad de un riesgo, es un estimado de cuan probable es que un riesgo impacte el proyecto. La probabilidad de que un riesgo impacte el proyecto está relacionada con la estabilidad del supuesto. Conforme progresa el proyecto y los planes de mitigación se van ejecutando, es común que la probabilidad vaya variando y deba ser reevaluada.

Fecha de Acción con Fecha Límite (Posicionándose en el tiempo)

Uno de los puntos más importantes que se debe saber acerca de un riesgo es la máxima fecha posible en que las acciones deben iniciar para evitar el impacto del riesgo. Para establecer esta fecha es importante identificar cuando el riesgo empezará a impactar el plan de trabajo, por ejemplo un hito del cronograma, y qué se requiere hacer para evitar este impacto. Trabajando en forma regresiva desde esta fecha final y calendarizando las acciones necesarias de mitigación, las “Fechas de Acción con Fecha Límite” están definidas como la última fecha posible para iniciar la primera de esas acciones.

Ejemplo.

“Seis desarrolladores Oracle son requeridos para el 12 de enero, y no se tiene ninguno en la organización. La experiencia muestra que se requieren dos semanas para obtener aprobación de reclutamiento externo y seis semanas más para completar el ejercicio de reclutamiento. Este conocimiento generará al menos dos fechas finales de acción: El reclutamiento debe iniciar el 1 de diciembre (seis semanas antes de la necesidad), y la aprobación debe estar para el 18 de noviembre”.

Conforme inicia cada acción, la fecha, cambiará a la fecha en que debe iniciar la siguiente acción. De esta forma, siempre será obvio qué punto del plan de mitigación está fallando, por ejemplo, cuando una actividad no ha iniciado a tiempo. Esto puede funcionar como disparador para invocar las acciones de

contingencia, o a una revisión crítica de la posibilidad de éxito de lo que queda pendiente del proyecto.

2.6.10. Cerrando los riesgos

Habiendo identificado los riesgos y decidido cual mitigar y cual aceptar, el objetivo de la Administración de Riesgos es que éstos sean eventualmente cerrados. La mayoría de riesgos se cierran cuando han sido exitosamente mitigados o cuando han impactado, la minoría se cierra debido a cambios en las circunstancias del proyecto independientemente de las acciones de mitigación.

Se deben ejecutar revisiones regulares al portafolio de riesgos validando la vigencia de las clasificaciones. Para administrar riesgos de forma exitosa, el objetivo es reducir el impacto (criticidad) y/o mejorar el control. Sin embargo, la revisión de riesgos debería también validar las clasificaciones de los supuestos subyacentes. Un supuesto con clasificaciones A o B realmente no constituye un riesgo, por lo tanto, los riesgos producto de clasificaciones de supuestos A o B deben cerrarse. Lo anterior está basado en que las actividades de mitigación serán exitosas, ya sea, incrementando la estabilidad o reduciendo la sensibilidad de los supuestos.

Los recursos usualmente son escasos, y aquellos asignados a la mitigación de riesgos pueden conservarse para asegurarse que estén dedicados 100% del tiempo a mover las clasificaciones de los supuestos a B. Esto cerrará el riesgo, pero el supuesto (y evidentemente sus clasificaciones) continuará siendo validado hasta comprobar que es verdadero.

2.6.11. Estimación del costo de los riesgos

La estimación correcta del costo del impacto de un riesgo ayuda a tomar la decisión de si un riesgo debe ser mitigado o no, precisamente al compararlo con el costo de su plan de mitigación.

Precisión

Identificar los costos asociados a un riesgo, es una tarea compleja, y los resultados deben expresarse como “el mejor estimado actual”, más que definirlos como un hecho comprobado. La complejidad está relacionada con la necesidad de escoger cuál de los muchos posibles cursos de eventos y consecuencias podrían resultar del impacto de un riesgo.

Todos los escenarios de costos deberán estar sustentados por la información que llevó a obtener un total, para permitir a otros ver la derivación de estos escenarios, juzgar su exactitud o precisión y estar de acuerdo o cuestionarlos. Los costos que han sido calculados deben mostrarse en los reportes de riesgos que se envían a la administración y a los altos niveles de la organización. Estos administradores deben usar su experiencia y conocimiento para revisar los costos mostrados en los reportes de riesgos y estar de acuerdo o hacer los cuestionamientos respectivos.

Límites en el análisis de costos

Inicialmente, los costos totales relacionados con los riesgos, deben ser calculados por el área de la organización donde se identifica el riesgo, por ejemplo, proyectos, desarrollo, contabilidad, etc. usando la información disponible por ese nivel.

A nivel general, es vital asegurarse que no haya doble conteo, es decir que un riesgo no se utilice sobre un mismo efecto más de una vez, o donde un riesgo afecte a más de un área. Si es necesario se debe generar un supuesto/riesgo separado.

Calculando la exposición al riesgo (Riesgo Factorado)

Para asegurar que un escenario muestre una representación más razonable del último efecto en las finanzas de la organización, el costo del impacto calculado

se modifica para mostrar la exposición al riesgo. Esto se conoce también como el costo del Riesgo Factorado y se calcula así:

Exposición al Riesgo = Costo X Probabilidad

Dónde:

Costo, es el costo total del posible impacto de un riesgo y probabilidad, es una evaluación, en términos de porcentaje, de la probabilidad de que el riesgo impacte.

La metodología ABCD no recomienda el uso del riesgo factorado como un parámetro en la priorización de riesgos, ya que se combinan dos parámetros distintos – costo del impacto y probabilidad – en una forma que frecuentemente disfraza información clave necesaria para la priorización. Esto es particularmente cierto en riesgos con baja probabilidad y alto impacto o alta probabilidad y bajo impacto.

Costo de la Mitigación

Cuando un riesgo ha sido identificado, se deben explorar las opciones para mitigar este riesgo. La estabilidad del supuesto debe proveer una indicación inmediata del trabajo requerido para mitigar este riesgo. El encargado de riesgos es normalmente la persona que estima el costo del plan de mitigación. El resultado se revisa con los encargados de otras áreas afectadas, de manera que se pueda identificar si otros se están viendo impactados, si lo están, los costos probablemente serán más altos.

Costo de las contingencias

La metodología recomienda que un plan de contingencia sea creado para cada riesgo Rojo, C o D.

Nota: Estos planes y actividades de contingencia no son los mismos planes y actividades de mitigación. La mitigación ocurre antes de que el riesgo impacte, la

contingencia se utiliza luego de que el riesgo impacta mediante procesos de recuperación para reducir el efecto del riesgo.

2.6.12. Priorización de riesgos

La priorización permite que recursos limitados sean dirigidos a atender los riesgos más críticos.

El objetivo de la priorización de riesgos es identificar los riesgos más significativos de entre el grupo de riesgos identificados por medio de una serie de métodos. Una vez que todos los riesgos han sido registrados en una lista, éstos deben ser ordenados de acuerdo a su prioridad y deben ser atendidos por medio de un programa lógico y planificado.

2.6.13. Registro de supuestos y registro de riesgo

Todos los supuestos capturados deben documentarse en un registro de supuestos, pero solo los supuestos críticos deben generar riesgos, los cuales se documentan en un registro de riesgos. Filtrando los supuestos y convirtiéndolos en riesgos, toda la información capturada será racionalizada agregando trazabilidad a los detalles de su fuente y las consecuencias.

Gráficos de Burbuja

Es difícil manejar tres parámetros para priorizar los riesgos. Los diagramas de burbuja son útiles para combinar esos parámetros de forma gráfica generando un simple perfil de riesgos que puede ser entendido por personal no especialista.

El tiempo se representa sobre el eje horizontal contra una escala de meses.

La criticidad se representa sobre el eje vertical, con los riesgos críticos (Rojo) tocando el eje X.

El control está representado por el tamaño de la burbuja. Las burbujas más grandes representan los riesgos sin control (D) y las más pequeñas muestran los riesgos clasificados como A.

El origen del gráfico, donde se juntan los ejes, representa el (los) objetivo(s) crítico(s) del proyecto. Si se permite que un riesgo en la burbuja, impacte el origen, es por definición, un riesgo que frena el proyecto. Por lo tanto, un perfil de riesgo es más aceptable en la medida en que se aleje del origen.

Se debe tener cuidado cuando se evalúa la calidad general del portafolio por medio del gráfico de burbujas, ya que los riesgos que están lejos del origen podrían ser mal administrados de manera que se pueden acercar al impacto. Por otro lado, los riesgos cerca del origen pueden ser administrados muy de cerca en escalas de tiempo muy cortas. La figura 8 es solo una foto de las clasificaciones ya que estas se mueven en el tiempo y no da detalle de los riesgos.

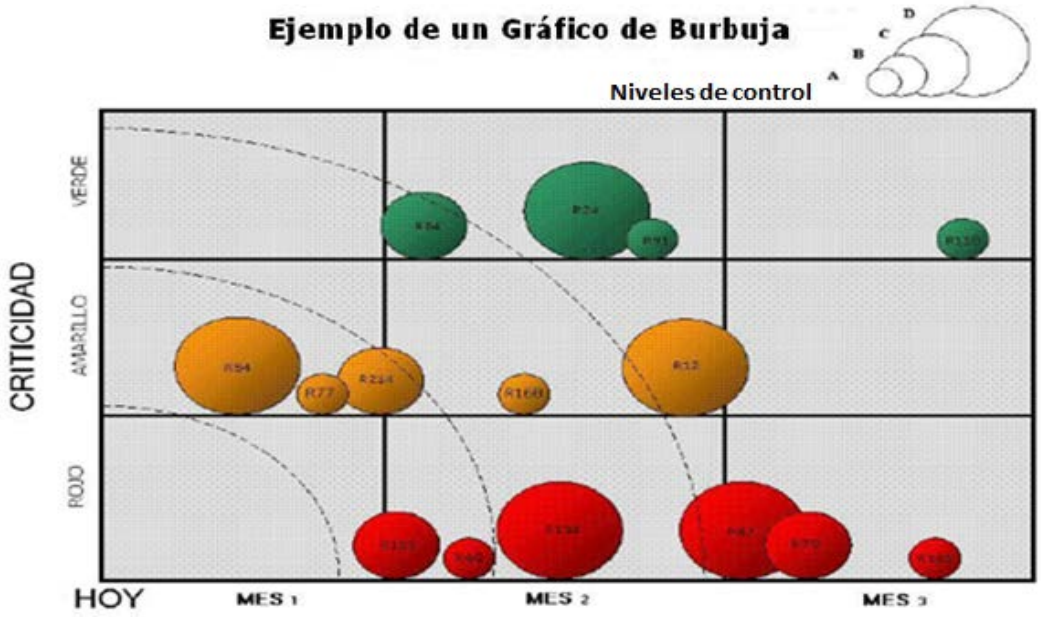


Figura 8. Diagrama de burbuja.

El análisis del diagrama de burbuja puede producir una priorización de primer nivel acerca de los riesgos del proyecto al mostrar:

- La posición de cada riesgo en el tiempo.
- La criticidad del riesgo con respecto a los FCEs del programa o proyecto (Rojo, Amarillo, Verde).
- El control (nivel de confianza) con la que el riesgo será administrado (A, B, C o D).

Los riesgos más serios son aquellos que están cerca del origen, éstos son urgentes y tienen alta criticidad. Los siguientes riesgos son aquellos que están cerca del eje X (alta criticidad), o los del eje Y (urgentes). Esto es útil para pensar en términos de arcos concéntricos, centrados sobre el origen del gráfico, donde los riesgos más cerca del origen son los de más alta prioridad, etc.
De esta forma, al día de hoy, un riesgo Amarillo B con fecha en dos semanas tiene una prioridad más alta que un Rojo C, con fecha de un mes adelante.

2.6.14. Control de riesgo

Los riesgos deben ser atacados tanto desde un nivel estratégico como desde un nivel táctico. El enfoque estratégico busca tendencias y causas subyacentes para grupos de riesgos, de manera que un conjunto de acciones puedan atacar más de un riesgo. El enfoque táctico toma cada riesgo de forma independiente de manera que estos son atacados de forma individual.

El enfoque táctico se ejecuta primero ya que cada riesgo debe atacarse lo antes posible. Es decir no se debe esperar a tener un conjunto de riesgos similares para atacarlos en conjunto.

Enfoques Tácticos

La mayoría de riesgos son atacados individualmente (un plan de acción para cada riesgo) para direccionarlos al supuesto subyacente. Los supuestos que son colocados dentro del área C y D, de la matriz de Sensibilidad/Estabilidad, son inestables y/o representan riesgos significantes, siendo peligroso continuar sin tomar acción.

Hay dos enfoques tácticos para lidiar con estos riesgos:

- Estabilizarlos, tomando la acción apropiada para mejorar la confianza del supuesto. Si esto no es posible dentro del equipo, el riesgo puede requerir ser escalado al siguiente nivel administrativo.
- Hacer el proyecto menos sensible al supuesto, por ejemplo, desensibilizar el riesgo al rediseñar o replantear.

Esas opciones están resumidas en la Figura 9.

Las acciones tomadas para atacar el problema pueden ser diferentes, dependiendo de si la intención es desensibilizar o estabilizar. Es normal que primero se trate de estabilizar el supuesto.

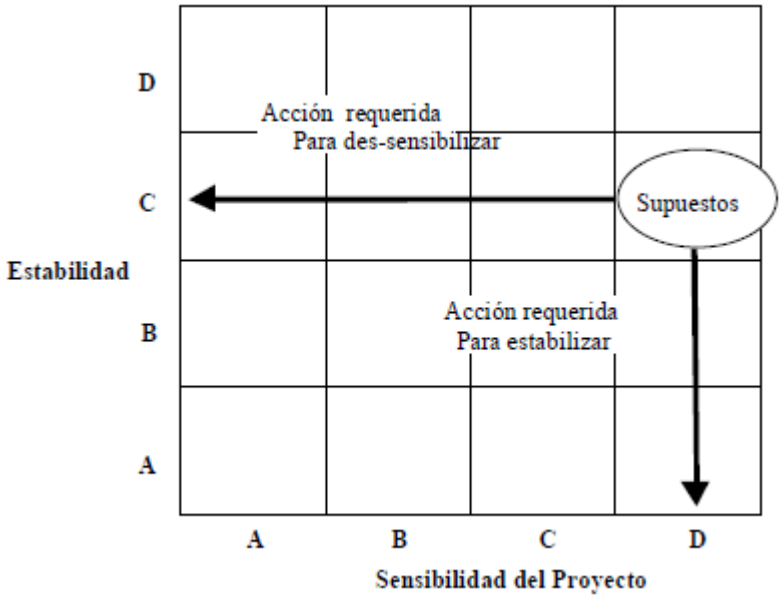


Figura 9. Objetivos básicos de las acciones reductoras de riesgo.

La figura 9, nos muestra una clasificación C, D para un supuesto en el diagrama de estabilidad/sensibilidad, esto quiere decir que el supuesto es potencialmente riesgoso y lo primero que tenemos que hacer, es tomar acciones

para poder estabilizar el supuesto, para luego rediseñar o replantear el supuesto. Realizando estos pasos, reduciremos el riesgo del supuesto.

Enfoques estratégicos – "Manejadores"

Para ayudar a encontrar estrategias que mitiguen los riesgos de un portafolio de riesgos grande, los supuestos y riesgos son revisados para encontrar causas comunes. ABCD tradicionalmente ha usado los Manejadores de Riesgos para alcanzar una vista estratégica del portafolio.

Cada supuesto tendrá al menos uno de los siguientes manejadores: Decisión, Hito, Recurso o Técnico. Los supuestos son por lo tanto revisados y colocados en la categoría más apropiada para mostrar qué está manejando las clasificaciones de calidad pobres. Cuando se clasifican los riesgos aplican los mismos manejadores:

- **Decisión:** Este manejador se refiere a un riesgo basado en decisiones de negocio sobre la política, estándares o prioridades.
- **Recurso:** Este driver se relaciona a riesgos basados en cualquier forma de recursos que requieren intervención administrativa para alcanzar el éxito.
- **Hito:** Este es utilizado donde las escalas de tiempo de las actividades están siendo muy ajustadas o existe una dependencias de tiempo sobre otras áreas, proveedores, etc. y el supuesto no sería problema si hay más tiempo disponible.
- **Técnica:** Estos manejadores ocurren donde la complejidad del proyecto está manejando las clasificaciones. (Ejemplo diseños no probados, restricciones de hardware y software, organizaciones complejas, etc.) La complejidad es tal, que los errores son comunes.

Categorizar los supuestos y riesgos de esta forma identifica los principales manejadores de los riesgos, simplifica la identificación de tendencias y asiste en el desarrollo de apropiados planes para el manejo de riesgos.

	Técnicos	Hitos	Recursos	Decisión	Total
Rojo	7	15	4	19	*45*
Amarillo	12	19	15	26	*72*
Verde	10	6	12	12	*40*
Total	**29**	**40**	**31**	**57**	**157**

Figura 10. Manejadores de Riesgo

A manera de ejemplo, la figura 10 indica donde se requiere un esfuerzo particular. El relativo alto número de riesgos basados en decisión sugiere que el trabajo se está poniendo en riesgo al tener que esperar por decisiones, probablemente dentro de la organización. Una junta de los líderes de la compañía podría potencialmente resolver la mayoría de esos riesgos. Adicionalmente, si el trabajo está en las etapas iniciales, ya hay señales de que el factor tiempo es ambicioso ya que aparece un alto número de riesgos de Hito.

2.6.15. Acciones o planes para manejar los riesgos

Acciones – (Mitigación Simple)

Los pasos que deben seguirse para mitigar un riesgo pueden ser divididos en simples o complejos. Algunos riesgos pueden ser resueltos rápidamente, por ejemplo por medio de una llamada telefónica o una simple tarea. Para estos riesgos, monitorear el estatus de las acciones identificadas en el Reporte del Registro de Riesgos es suficiente y minimiza la burocracia. Es importante que estas acciones documentadas claramente identifiquen qué se necesita hacer, quién lo hará y cuándo será completado. En la administración de riesgos muchas acciones simples pueden ser identificadas.

Planes – (Mitigación compleja)

Los riesgos que requieren una administración más compleja, por ejemplo, donde las actividades de mitigación planeadas se extienden sobre un periodo de más de cinco días hombre, pueden requerir recursos y tiempo significativos para

resolverlas, y para estas, se recomienda un plan para manejo de riesgos (PMR), estos planes pueden incorporarse a los planes normales del proyecto.

La decisión de incorporar un PMR a los planes principales del proyecto está basada en la duración del PMR con respecto al plan principal.

Componentes de un plan formal para el manejo de riesgos

Un plan para el manejo de riesgos estructurado clarificará el pensamiento, otorgando la visibilidad necesaria y alimentando los planes principales del proyecto.

Los componentes básicos de un PMR son

- La declaración de supuestos subyacentes, su originador y sus clasificaciones.
- La declaración de riesgos y sus clasificaciones, junto con una referencia al identificador de riesgos en el registro de riesgos, para una referencia cruzada a los detalles del riesgo.
- Dueño del riesgo y administrador de la acciones.
- Enfoque de la administración del riesgo (mitigarlo, aceptarlo o transferirlo).
- Objetivos del PMR (ejemplo. Estabilizar o des-sensibilizar el supuesto).
- Criterios de éxito (Cómo identificar que se alcanzaron los objetivos).
- Resumen del PMR (Cuáles son los pasos necesarios para alcanzar los objetivos).
- Recursos adicionales requeridos.
- Proceso de monitoreo (cuán a menudo y por quién).
- Re-evaluación de los supuestos subyacentes (a ser completado luego de la ejecución del PMR).
- Planes de contingencia y regresión, entendiendo como plan de regresión al procedimiento o los procedimientos necesarios para regresar un sistema a su estado original (Ejemplo: ¿Qué se debe hacer si el PMR falla?).

- Disparadores de contingencia (Ejemplo: ¿Qué constituye una falla del PMR que requiere invocar las acciones de contingencia?).
- Presupuesto de contingencia, incluyendo cómo tener acceso a los fondos.
- Internos/Externos. El riesgo interno puede ser direccionado dentro del proyecto, el externo no.
- “Stakeholders”.
- Decisiones y acciones tomadas. ¿Cuándo y por quién?

Creando los planes para manejo de riesgos

Es preferible desarrollar un número de PMRs alternativos antes de tomar la decisión de implementar uno de estos. La técnica de análisis utilizada para identificar riesgos puede ser usada para ayudar a entender qué tipo de planes pueden ser apropiados. No hay reglas en firme que indiquen el enfoque para generar un PMR, pero si se sigue una simple lógica, será más fácil asegurarse de que todas las posibles estrategias han sido consideradas.

Dos enfoques deberían ser considerados para cada supuesto crítico

- Uno para estabilizar el supuesto, aumentando la probabilidad de que resulte verdadero.
- Otro, para desensibilizar el proyecto con respecto a los supuestos, haciendo que importen menos.

Hay muchas formas de administrar riesgos. Algunas opciones son:

- Planeamiento detallado de áreas sensitivas.
- Recalendarizar módulos y actividades.
- Reestructurar la estructura de trabajo.
- Reacomodo de las responsabilidades sobre los elementos del trabajo.
- Exportar ciertos elementos a otras agencias.
- Formar sub-proyectos.
- Construir modelos y prototipos.
- Resolver “issues” con los recursos.

- Procedimientos de control de programas especiales.
- Planear actividades paralelas.
- Identificación de hitos enlazados con otros proyectos.
- Monitorear las dependencias externas.

También puede ser útil revisar los manejadores de riesgo para identificar mejor el o los cursos de acción.

Seleccionando planes particulares para el manejo de riesgos

La selección de un PMR particular es normalmente un proceso simple, ya que el plan que promete ser más exitoso casi siempre es obvio. La experiencia y buen juicio serán suficientes, en la mayoría de circunstancias, para escoger el plan más apropiado sobre una base de simplicidad, costo, tiempo de implementación u opciones de éxito.

Cuando considere las características de varios PMRs hay un número de factores que deben ser evaluados:

- Tiempo disponible antes de que el riesgo sea reducido a un nivel aceptable.
- Duración del PMR propuesto.
- Costo del impacto del riesgo.
- Cuando considere cuánto invertir en un PMR es importante conocer cuánto tiempo disponible hay antes de que el riesgo impacte el proyecto. Si el riesgo se ve muy lejano en el tiempo, el equipo debería analizar muy cuidadosamente antes de implementar un PMR de forma inmediata lo cual implicará un gran esfuerzo.
- Cualquier PMR tiene un riesgo inherente de falla.
- Podría ser más conveniente encontrar más del riesgo con un pequeño plan antes de implementar un ataque más agresivo.
- Si un plan modesto funciona se ahorrarán recursos.
- Si un plan modesto falla, aún se puede implementar uno más agresivo.

Ejecutando el plan para manejo de riesgos

Una vez que el PMR ha sido acordado y aprobado, el siguiente paso es implementarlo. Para esto se debe seguir el plan e ir reportando el progreso del mismo al dueño del riesgo y al Project Manager con respecto al tiempo y recursos gastados.

Cerrando los planes para manejo de riesgos

Hay una gran diferencia entre cerrar un plan y detenerlo. Los PMRs deben detenerse si no hay resultados exitosos. El cierre solo debe autorizarse cuando los objetivos han sido alcanzados. Es realmente crítico que un PMR sea detenido o cerrado en el momento apropiado.

Un PMR debe detenerse cuando:

- Se nota que va a fallar.
- Ya no es necesario.

Es esencial que no se gaste dinero en PMRs inefectivos, o el valor del proceso entero será cuestionado.

Cuando un PMR cumplió sus objetivos se debe:

- Obtener el acuerdo con el dueño del riesgo de cerrar el mismo.
- Asegurarse que todos los cambios necesarios producto del PMR están incorporados al plan principal del proyecto, a la documentación y a las especificaciones.
- Evaluar si queda algún riesgo residual que deba analizarse.
- Documentar el cierre en el Registro de Riesgos.

2.6.16. Roles y responsabilidades

La definición e implementación efectiva de los roles y responsabilidades en la Administración de Riesgos es crucial para el éxito del proceso de Administración de Riesgos.

Cada riesgo necesita un dueño y cada Acción/PMR debe tener un administrador para asegurarse que el riesgo está siendo atacado en la forma apropiada. Cada uno de esos roles debe tener las responsabilidades publicadas. Los roles pueden ser de tiempo completo o en parte de acuerdo al tamaño, complejidad y criticidad del proyecto.

En algunos casos, el rol de administrador de proyectos podría ser combinado con el de administrador de riesgos o con el de administrador de acciones para riesgos. Sin embargo, mientras sea posible, el rol de dueño del riesgo no debe combinarse con el rol de administrador de acciones, ya que el dueño del riesgo cumple un rol que no requiere profundizar en el tema, solo valida y mantiene el balance del sistema.

Administrador del Proyecto

Los roles y responsabilidades con respecto a la administración de riesgos son:

- Evaluar el proyecto con base en el diagrama de complejidad/criticidad y así recomendar el nivel de Administración de Riesgos apropiado.
- Asegurar que se ejecute un apropiado proceso de Análisis de Riesgos tan pronto como sea posible en el ciclo de vida del proyecto.
- Presentar los detalles de la estrategia de administración de riesgos del proyecto a niveles más altos de la organización.
- Obtener la autorización del presupuesto para la administración de riesgos.
- Contabilizar continuamente el uso del presupuesto para riesgos.

Administrador de Riesgos

El administrador de riesgos asegura que el proceso de administración de riesgos sea proactivo y con sentido futuro.

- Recomienda a los equipos de programas/proyectos soluciones apropiadas para la administración de riesgos.
- Crea y mantiene el proceso de priorización del proyecto. (Ver apéndice B).

- Crea y facilita el proceso de "governance"[8] de los riesgos del proyecto.
- Entrevista al personal clave, donde se utilicen entrevistas.
- Mantiene el registro de "issues", supuestos y riesgos del proyecto.
- Conduce sesiones periódicas para el análisis del Registro de Riesgos.
- Escala los riesgos al siguiente nivel cuando es necesario.
- Presenta documentación de metodologías de administración de riesgos al equipo cuando es necesario.
- Reporta los cambios en los riesgos más importantes a los niveles superiores.
- Monitorea y reporta el desempeño de los dueños de las acciones y/o riesgos cuando estos son externos a la organización.
- Se asegura que los procedimientos que son parte del proceso de administración de riesgos sean apropiados y usados.
- Se asegura que el equipo del proyecto sea entrenado adecuadamente en el proceso de administración de riesgos.

Dueño del Riesgo

El dueño del riesgo debe ser el más interesado en resolver un riesgo y es el más indicado para evaluar si éste está siendo administrado apropiadamente.

- Revisa las distintas alternativas del plan/acciones de riesgos en conjunto con el administrador de las acciones de riesgos.
- Decide cual acción/plan de riesgos debe implementarse y cuándo.
- Revisa los objetivos específicos de las acciones/PMR de riesgos en conjunto con la junta revisora de riesgos.
- Define los criterios de éxito generales de las acciones/planes de riesgos.
- Monitorea la evaluación del administrador de las acciones de riesgos con respecto al progreso del plan.
- Cierra el plan cuando los objetivos han sido alcanzados, también cierra el riesgo si es necesario.

[8] Identificación y tratamiento de los riesgos a los que la tecnología de la información expone al negocio.

- Detiene el plan cuando se ve que va a fallar y re-planea el PMR si es necesario.
- Detiene el plan si éste ya no es necesario y cierra el riesgo si se requiere.
- Valida que los objetivos hayan sido alcanzados y que los detalles han sido documentados en el Registro de Riesgos.
- Evalúa cualquier riesgo residual y se asegura que el Registro de Riesgos se actualice correctamente.
- Evalúa los nuevos supuestos que surgen durante el PMR.

Administrador de las acciones de riesgos

- Es el encargado de ejecutar el PMR.
- Valida la fuente de los riesgos.
- Define los objetivos de cada posible plan/acción de riesgos.
- Detalla las acciones requeridas en cada plan/acción de riesgos.
- Define los recursos requeridos en cada plan/acción de riesgos.
- Identifica los criterios de éxito de cada plan/acción de riesgos en conjunto con el dueño del riesgo.
- Calcula el costo de cada plan/acción de riesgos para compararlo con las diferentes alternativas si es necesario.
- Presenta alternativas al dueño del riesgo y ejecuta el plan escogido por éste.
- Alerta al dueño del riesgo cuando el proceso de administración de riesgos no es efectivo.
- Reporta el progreso del plan/acción de riesgos al dueño del riesgo.
- Reporta cuando el plan ha sido exitosamente completado.
- Reporta si el plan está empezando a fallar.

2.6.17. Estructura de "Governance"

La Junta Revisora de Riesgos (JRR) puede ser un punto en la agenda de las reuniones de un proyecto o programa. Cada organización debe

utilizar los siguientes términos de referencia como guía cuando desarrolla los planes de comunicación.

Términos de Referencia

El punto central del proceso de control de riesgos es la junta revisora de riesgos, la cual se reúne al menos una vez al mes. Esta junta asegura que los roles y responsabilidades estén asignados, que los riesgos estén entendidos al nivel apropiado dentro de la organización, que los planes de acción estén definidos y que se diseminen por medio de los flujos de comunicación a los niveles mayor de la organización.

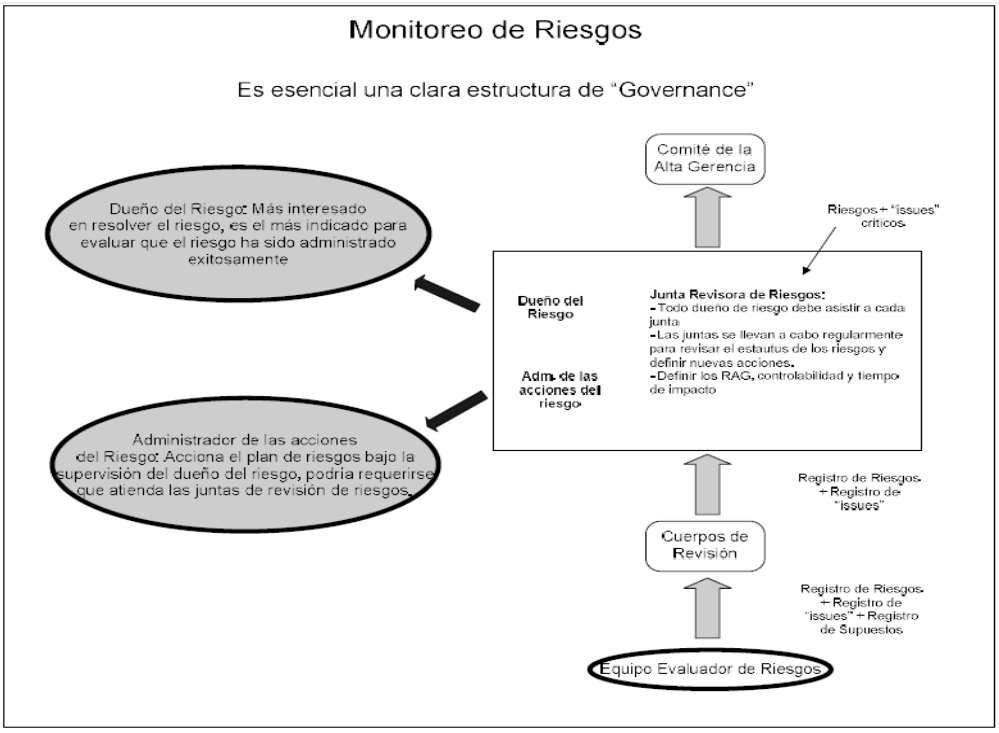


Figura 11. Junta de Revisión de Riesgos (JRR)

La figura 11, nos muestra cómo se puede organizar a las personas para poder monitorear los riesgos del proyecto, donde se realizan reuniones regulares (JRR), para poder administrar, registrar y controlar los riesgos.

Representación de la Junta Revisora de Riesgos

Los administradores “senior” (ej. Administradores de proyectos de un programa) normalmente forma el núcleo de esta junta. Es necesario que todos los dueños de riesgos asistan. Los administradores de acciones de riesgos (de los riesgos críticos) también podrían ser requeridos para que describan los planes de acción y el estatus de los mismos. La junta debe estar dirigida por el director del programa/negocio y facilitada por el administrador de riesgos del programa.

Antes de la reunión de la JRR

El registro de riesgos debe enviarse a todos los miembros de la JRR al menos un día antes de la reunión. Es responsabilidad de cada dueño de riesgo revisar, antes de la reunión, los riesgos de los cuales ellos son responsables. Los dueños de los riesgos deben asegurarse también que entienden totalmente los riesgos, deben estar de acuerdo con las clasificaciones y estar claros con respecto a las acciones que vienen en camino. Para lograr esto, posiblemente sea necesario que el dueño del riesgo se comunique con el dueño del supuesto.
Adicionalmente, cada dueño de riesgo debe revisar el registro de supuestos para validar otros supuestos que pueden estar relacionados con su riesgo. Si hay desacuerdos mayores, el caso debe elevarse a la junta de revisión de riesgos. Las solicitudes menores se pueden resolver con el administrador del proyecto.

Durante la reunión de la junta de revisión de riesgos

La junta discutirá los riesgos en orden de prioridad, según se indique en el diagrama de burbuja, ocurriendo lo siguiente:

- Designar/Confirmar los dueños de los riesgos para los nuevos riesgos, quienes deben aclarar los mismos si es necesario.
- Confirmar o cambiar las clasificaciones de criticidad.
- Para los riesgos existentes, el dueño del riesgo debe reportar el progreso de los planes/acciones.
- Confirmar o cambiar las clasificaciones de control.
- Confirmar o cambiar las acciones de fecha final.

- Acordar el sistema de monitoreo del PMR con el dueño del riesgo y el administrador de las acciones.
- Acordar y autorizar el presupuesto del PMR con el administrador de las acciones.
- Asignar los recursos apropiados a los PMRs.
- Asegurarse que los PMRs están integrados en el plan principal del proyecto.
- Monitorear los reportes de progreso con respecto al plan.
- Cuando se considera que el riesgo se ha resuelto, el dueño del riesgo acordará el proceso de cierre.

Después de la reunión de la junta de revisión de riesgos

El registro de riesgos y el diagrama de burbuja serán actualizados dándoles el seguimiento apropiado.

2.7. Administración de cambios (CMMI)

La administración de cambios existe para asegurar que todos los cambios introducidos a la infraestructura de tecnología de la organización no afecten negativamente los niveles de servicio acordados. Los cambios deben hacerse utilizando métodos y procedimientos estandarizados de una manera pronta y eficiente para minimizar el impacto. Por lo tanto un cambio es una acción que altera el estatus de un elemento de la configuración que se encuentra dentro de la infraestructura tecnológica de la organización.

Actividades de la administración de cambios:

- Filtrado, responde a la pregunta, ¿se puede hacer el cambio?
- Determinar la clasificación y prioridad con respecto a la urgencia y al impacto que tendrá el cambio en la organización.
- Autorización, una junta de personal debe autorizar el cambio con base en el impacto en el negocio, los servicios, impacto de no hacer el cambio, recursos y costo, mantenimiento, etc.

- Coordinar el cambio, consiste en construir, probar e implementar el cambio.
- Revisión post implementación. Se deben responder a preguntas como ¿qué causó la necesidad del cambio? O ¿qué puede hacerse para evitar el problema que causó el cambio?

2.7.1. Beneficios de la administración de cambio

- **Alineación:** El administrador de cambios alinea todos los servicios de tecnología de la información con las necesidades de negocio basados en los cambios que se deben realizar, para esto requiere entender el impacto de cada cambio en el negocio.
- **Incremento de la productividad**: Tanto de los usuarios como del personal de tecnología.
    - **Usuarios:** Mayor calidad en los cambios con menos interrupciones
    - **Personal:** El administrador de cambios asegurará que el personal de soporte adecuado trabaje en los cambios asignados resultando en un mejor uso de los recursos.
- **Riesgo:** Al filtrar las solicitudes de cambio, el análisis realizado minimiza el riesgo de los cambios aprobados.
- Mejores reportes de cambios implementados
- Incremento en el volumen de cambios

2.8. Administración de la configuración (CMMI)

Administrar la configuración es la necesidad de controlar los activos y servicios del área de tecnología de la información conocidos como CI o Configuration Item (elemento de la configuración) entre los que se pueden incluir equipo, programas, aplicaciones y documentación. La información que se tendrá disponible es:

- Historial del CI
- Información de todos los activos (tipo de equipo, localización, atributos, etc.)

- Relaciones entre activos (Computadoras conectadas a un servidor por ej.)
- Información de proveedores que están relacionados con algún servicio activo.
- Información para planes de recuperación por desastre.

Atributos de un CI

- Serie o número
- Modelo
- Licencia
- Tipo
- Versión

Relaciones de un CI

- Conectado a
- Parte de
- Copia de

2.8.1. Beneficios de la administración de la configuración

- Brinda soporte a todos los procesos de la organización.
- Brinda información sobre el impacto y análisis de tendencias para problemas y cambios.
- Asiste en la adherencia a obligaciones legales y contractuales.
- Reduce el riesgo de contar con programas no autorizados.
- Ayuda a la planificación financiera.

3. MARCO METODOLÓGICO

Se pretende al inicio del presente trabajo, familiarizar, tanto al autor como al lector, con los diferentes aspectos relacionados con el tema de la recuperación de sistemas informáticos en caso de desastre.

La metodología se aplicará con el objetivo de crear una guía para que los potenciales usuarios de este trabajo puedan crear los siguientes planes:

1. Creación del plan de recuperación.
2. Creación de un plan para darle mantenimiento al plan de recuperación.
3. Creación de un plan para validar el plan de recuperación, de forma tal que, el mismo siempre esté vigente y actualizado. Este plan servirá de guía para la ejecución de los simulacros de desastre.

3.1. Desarrollo de la guía

3.1.1. Identificación de los objetivos y metas

Antes de darse a la tarea de definir el plan, se deben identificar los requerimientos de negocio, entre los que se pueden incluir:

- Minimizar las interrupciones del negocio.
- Reiniciar las operaciones críticas en un tiempo mínimo.
- Minimizar las pérdidas financieras.
- Mantener una buena imagen antes y después de un desastre.

3.1.2. Identificación del líder del proyecto

Típicamente se conoce a esta persona como el líder del DRP y entre sus responsabilidades se encuentran:

- Determinar los objetivos, políticas y factores críticos de éxito.
- Organizar, coordinar y administrar el proyecto.

- Proveer un punto de contacto para la organización con respecto al DRP.
- Presentar el proyecto a la administración y staff.
- Desarrollar el plan del proyecto.
- Definir y recomendar la estructura y administración del proyecto.

3.1.3. Establecimiento de un equipo de continuidad para el plan

Todas las áreas de la organización, deben tener al menos un representante en el equipo del proyecto DRP. Algunos de los equipos típicos y sus deberes incluyen:

- Coordinador del plan de continuidad: Administra los procesos y coordina los equipos.
- Patrocinador: Aprueba el plan, asigna presupuesto y define las expectativas.
- Recursos humanos: Contrata el personal necesario.
- Relaciones con el medio: Interactúa con el medio con respecto a los efectos del desastre.
- Equipo legal.
- Equipo de seguridad de la información.
- Equipo de seguridad física.
- Administración de servicios.
- Equipo de respuesta a la emergencia: Responde al desastre al poner el DRP en acción.
- Equipo evaluador del daño.
- Equipo para el sitio alterno: Mantiene los activos en el sitio alterno.

3.2. Creación del plan de recuperación en caso de desastre

Para crear el plan de recuperación en caso de desastre se deben realizar tres actividades:

- Identificación de las áreas a recuperar.

- Creación de un laboratorio para realizar pruebas.
- Definición del procedimiento de respaldos de información.

3.2.1. Identificación de áreas a recuperar

Para efectos de este proyecto, cuando se trata de áreas o procesos a recuperar, se debe pensar en el proceso de identificar el hardware (equipo de cómputo) y software (programas) utilizado para realizar las diferentes funciones operativas dentro de la organización.

Para identificar las áreas, sistemas o procesos a recuperar mediante el plan de recuperación en caso de desastre, conocido como DRP, se ejecutará un análisis de impacto o como se conoce por sus siglas en inglés BIA.

Un análisis de impacto de negocio es un proceso sistemático mediante el cual la organización reúne y analiza la información de sus funciones y procesos. Esta información se utiliza posteriormente para determinar cómo se verá impactada la organización si estas funciones y procesos no están disponibles por un determinado periodo de tiempo debido a un desastre o situación de crisis.

El análisis BIA deberá responder a las siguientes preguntas:

- ¿Cuáles sistemas y procesos de información son críticos para la organización?
- ¿Qué tan rápido se deben recuperar los sistemas y procesos claves antes de que ocurra una pérdida inaceptable o irrecuperable?
- ¿Cuál es la interdependencia entre los diferentes sistemas y procesos de información?
- ¿En qué orden se deben recuperar los sistemas y procesos claves luego de un desastre?

El análisis BIA que se utilizará está compuesto de cinco fases:

i. Inicio

ii. Adquisición de la información

iii. Análisis de la información

iv. Documentación

v. Presentación de reportes a la administración

I - INICIO:

Este paso consiste en obtener el patrocinio de parte de la administración de la compañía. Para esto se deben presentar los objetivos, metas, alcance y todos los datos que ayuden a que la administración compre la idea provean los recursos necesarios para que el proyecto funcione sin problemas.

II - ADQUISICIÓN DE LA INFORMACIÓN:

Se deben recolectar una amplia variedad de información incluyendo la siguiente:

- Descripción detallada de los sistemas y procesos de información de la compañía.
- Identificación de los usuarios de los sistemas y procesos.
- Descripción de la interdependencia entre los procesos y sistemas.
- Análisis cualitativo y cuantitativo que describa el costo de no contar con los sistemas y procesos claves.

Para obtener esta información, se deben realizar entrevistas a los diferentes usuarios y expertos los cuales deberán contestar el siguiente cuestionario:

- Pérdida financiera si el sistema de información no está disponible en 1 hora, 8 horas, 1 día, 2 días, 4 días, 1 semana, 2 semanas y 1 mes.
- En una escala de 1 a 10, ¿cuál sería el impacto en los siguientes factores si el sistema de información no está disponible? (1 = No hay impacto, 5 = Impacto moderado, 10 = Impacto severo)

- Reducción en la moral del personal
- Violación de la ley o las regulaciones
- Incapacidad para ejecutar las actividades necesarias con los socios de negocio y de investigación
- Violación de acuerdos o contratos
- Incapacidad para ejecutar tareas críticas propias de la misión de la organización
- Destrucción o daño en los servicios básicos de la organización
- Reducción en la confianza del público hacia la organización
- Otros

III Análisis de la Información:

Se debe hacer una reunión con la administración para determinar los niveles aceptables de riesgo. En síntesis se deben definir las siguientes variables:

- Máximo tiempo de caída tolerable (MTD por sus siglas en inglés). Es el más largo periodo de tiempo que puede pasar inoperable un proceso de negocio, antes de que pierda la capacidad de recuperarse totalmente o antes de que impacte severamente a la organización.
- Objetivo de tiempo de recuperación (RTO).
- Objetivo de punto de recuperación (RPO).

La información obtenida durante la fase de adquisición necesita ser cuidadosamente examinada y analizada, para identificar procesos y sistemas críticos, interdependencias y tiempos óptimos de recuperación de los procesos y sistemas más importantes para la organización. La salida principal del análisis de información, es la asignación de una categoría de criticidad a los diferentes procesos y sistemas de información. Los procesos deben ser categorizados utilizando la siguiente tabla:

Categoría de Criticidad	Tiempo de Respuesta
Altamente Crítico	• El sistema de información debe ser recuperado antes de 24 horas • El sistema es altamente importante para el funcionamiento de la organización
Crítico	• El sistema de información debe ser recuperado antes de 48 horas • El sistema es importante para el funcionamiento de la organización
Criticidad Media	• El sistema de información debe ser recuperado antes de 7 días • El sistema tiene un nivel medio de importancia para el funcionamiento de la organización
No Crítico	• El sistema de información debe ser recuperado antes de 14 días • El sistema no es sustancialmente importante para el funcionamiento de la organización

Figura 12. Niveles de criticidad.

Los niveles de criticidad nos permiten considerar la indisponibilidad del sistema, en función del grado de criticidad, a partir de esta toma de conciencia, se podrá calcular y a menudo negociar un coste de implementación de la infraestructura. Figura 12.

IV Documentación de la información encontrada:

Los datos encontrados mediante el análisis BIA deben ser documentados en un reporte formal. Este reporte debe incluir la siguiente información:

- Resumen ejecutivo.

- Objetivos.
- Alcance.
- Metodología utilizada para reunir y analizar los datos.
- Resumen de la información encontrada.
- Detalle de la información encontrada por departamento o área funcional.
- Gráficos para ilustrar pérdidas potenciales.
- Recomendaciones.

V Presentación de reportes a la administración:

Este reporte debe presentarse formalmente al nivel gerencial de la organización.

Esta presentación debe visualizarse, como una excelente oportunidad para explicar a la gerencia, la importancia del plan de recuperación por desastre y por qué se debe implementar el plan.

Con base en el inventario de equipos, que se obtiene luego del análisis BIA mencionado en los puntos anteriores, se debe realizar un proceso de adquisición de equipo, para efectos de construir un laboratorio para pruebas.

Ya sea que el equipo se compre o que se utilice equipo existente en la organización, es importante mencionar que en la medida que el laboratorio simule el ambiente real, en esa medida será la calidad de las pruebas, es decir, a mayor similitud se obtendrá mayor confiabilidad en las pruebas.

3.3. Creación del laboratorio

Una vez que se tiene el equipo en el sitio destinado para el laboratorio, se debe proceder con la configuración del equipo, instalación de todos los programas necesarios para su correcto funcionamiento, tales como el sistema operativo, programas cliente para acceso a base de datos, configuraciones de los

programas, entre otros. Posteriormente se procede con la construcción una red aislada del ambiente productivo de manera que cualquier cambio en el ambiente de laboratorio no afecte los datos productivos. Finalmente se debe realizar la instalación de las aplicaciones que son propias del proceso normal del sistema SAP Productivo, es decir, todos los programas utilizados para la operación diaria del sistema.

3.4. Diseño del procedimiento diario de respaldos

Para poder hacer el diseño del procedimiento de respaldos de información se requiere llenar el siguiente cuestionario durante una reunión con los expertos en bases de datos e infraestructura. Este cuestionario proveerá la información necesaria para crear el diseño del proceso de respaldo y recuperación de datos necesarios en una situación de desastre.

- Dominio y dirección IP del Servidor de datos.
- Cantidad promedio de datos en GB que se deben respaldar diariamente.
- Características del medio de almacenamiento del respaldo (cinta, disco, etc.) o la unidad que se utilizará para realizar el respaldo (unidad de cinta, SAN, discos en espejo).
- Detalle el momento o la hora en la que se debe realizar el respaldo.
- Detalle el procedimiento y requerimientos del proceso de recuperación de los datos respaldados.
- Principales sistemas afectados si no se tiene acceso a este sistema de datos.
- Periodicidad con la que se debe hacer el respaldo.
- Prioridad de este servidor con respecto al plan de recuperación en caso de desastre.

Luego de la(s) reunión(es) con los expertos en bases de datos e infraestructura, se debe tomar cada cuestionario y distribuir su información en los siguientes puntos:

- Por prioridad (alta, media, baja)
  - Por periodicidad

- Tipo de medio de almacenamiento
  - ❖ Sistema y unidad de negocio al que pertenece
  - ❖ Cantidad de datos en GB de todos los sistemas a respaldar

EJEMPLO:

Prioridad: ALTA

Periodicidad: DIARIO

Medio: CINTA

- ❖ Servidor XYX, Base de Datos..... 600 GB.
- ❖ Servidor XYX, Sistema SAP.....2200 GB.

Medio: DVD

- ❖ Servidor XYS, Instaladores (Medios).....3 GB.

Periodicidad: SEMANAL

Medio: CINTA

- ❖ Servidor XYXZ, Sistema Datawarehouse.....2300 GB.
- ❖ Servidor XYXX, Archivos FTP.....800 GB.

3.4.1. Procedimiento de replicación de datos al sitio alterno

Se deben examinar los sitios que son candidatos a utilizar como lugar alternativo para recuperarse en caso de un desastre en el lugar donde estos sitios ofrecen sus servicios. Algunos de los cuestionamientos que se deben hacer son los siguientes:

- ¿Existen varios sitios a utilizar como lugar remoto?
- ¿Cuáles son los términos del contrato?
- ¿Cuánto tiempo se puede usar el servicio luego del desastre?
- ¿Cuál es la política con respecto a la disponibilidad del sitio para realizar pruebas?
- ¿Cuántos clientes y de qué lugares usan el sitio?
- ¿Cuáles son los precios?
- ¿Qué tan aislado está el sitio de eventos que puedan afectar a la organización?

Evaluación del hardware y software del sitio alterno: Se debe asegurar que la información y el equipo son los necesarios para cumplir con los objetivos de recuperación.

Evaluación de los sistemas de comunicación: En la mayoría de casos, la capacidad de comunicación es menor que la que se tiene en el sitio de operaciones normales. Por lo tanto el plan debe contar con este tipo de degradación.

Evaluación de los procesos de restauración y respaldo: La información debe ser transferida a los sistemas de respaldo. Si la información se pierde como resultado de un desastre, esta debe ser recuperada (o creada) en el sitio alterno.

Evaluación del área de servicio al cliente: Si la organización brinda servicio al cliente final, se debe validar si el sitio alterno cuenta con lo necesario para seguir brindando el servicio o si se debe recurrir a un tercero.

3.4.2. Traslado de información al sitio alterno

Las dos formas más comunes de trasladar la información respaldada al sitio alterno son:

- Por respaldos incrementales. Con esta opción se envían periódicamente respaldos de la información sustituyendo siempre el respaldo anterior con el más reciente.
- Por replicación directa. En este caso los cambios que se presentan en la información en ambiente productivo se reflejan automáticamente en el sitio alterno. Es un método más costoso y requiere de un excelente sistema de comunicación apoyado por un excelente servicio de internet, enlaces satelitales y terrestres principalmente.

Se debe hacer una presentación al patrocinador del proyecto de las ventajas y desventajas de uno u otro método. A continuación la figura 13, que compara ambos métodos con respecto a los principales factores implicados en el traslado de datos al sitio alterno. Es evidente que la recomendación es trasladar los datos por replicación directa manteniendo servidores en espejo (cada dato que se actualiza en el origen, se actualiza automáticamente en el servidor destino) en el sitio alterno.

ESQUEMA	RTO-RPO	DUPLICIDAD DE DATOS	DESINCRONIZACION DE DATOS	PERDIDA DE INFORMACION POR CINTAS CORRUPTAS	ANCHO DE BANDA REQUERIDO
Actualización por respaldos incrementales	Alta probabilidad de que se Increment en debido a los incidentes que se podrían presentar al momento de recuperar el sitio alterno.	Alta probabilidad de que se presenten, si el último respaldo se ejecuta mientras están corriendo aplicaciones del sistema	Alta probabilidad de que se presente	Probabilidad: Baja Impacto: Muy alto (RPO sube a 48 horas).	Menos de 1 GB. (aprox.)
Actualización por Replicación directa de datos	Probabilidad baja debido a que la cantidad de incidentes que se pueden presentar es menor	Baja probabilidad ya que únicamente se perdería el log de replicación saliente	Baja probabilidad ya que únicamente se perdería el log de replicación saliente	Probabilidad: nula. Menor probabilidad de errores humanos	1 GB. (aprox.)

Figura 13. Respaldos incrementales vs Replicación de Datos.

La replicación es el proceso de copia de datos de un sitio a otro por bloques y de forma diferencial. Por lo tanto, como la replicación se suele llevar a cabo a

nivel de archivo o paquetes, a medida que cambian cosas en el paquete en cuestión, los bloques que han cambiado en la fuente se replican inmediatamente en el destino.

La tecnología de replicación síncrona no reconoce el registro de la aplicación primaria hasta que se ha replicado el bloque en el sitio de destino. La replicación asíncrona, en cambio, primero reconoce el registro y luego replica el bloque al cabo del tiempo.

3.4.3. Mantenimiento del sitio alterno

Este proyecto parte del supuesto de que la organización cuenta con una política de administración de cambios. En términos generales, el proceso de administración de cambios, busca asegurar que solo se utilicen métodos y procedimientos estandarizados para el manejo de cambios en los programas y equipo utilizado en la organización.

Los resultados de contar con un procedimiento formal para la administración de cambios se pueden resumir en:

- Implementación consolidada, controlada y estructurada de cada cambio.
- Control sobre la asignación y consumo de recursos.
- Mejoras en la comunicación de cambios a los elementos del sistema.
- Mejoras en la administración del riesgo.
- Aumenta la capacidad de acomodar altas tasas de cambio dentro de un reducido impacto al negocio.

Una organización que cuente con una política de administración de cambios, tendrá en sus procesos un documento o subproceso llamado solicitud de cambio, el cual se utiliza cada vez que se requiere promover una modificación o inclusión de equipo o programa. Por lo tanto, para efectos de mantener idéntico el sitio alterno al sitio productivo, de forma tal que pueda ser utilizado en caso de

desastre, se debe agregar una sección a la solicitud de cambios donde el promotor del cambio pueda indicar si el cambio requiere ser ejecutado también en el sitio alterno, de manera que se mantenga la similitud en ambos ambientes.

3.5. Plan de validación o simulación

No importa qué tipo de validaciones o simulaciones se realicen, siempre se busca probar la mayor parte del plan que sea posible. El plan de pruebas por lo tanto depende directamente del apoyo que se tenga de la gerencia de la organización en un momento dado. A continuación, se detallan los pasos que se recomiendan tomar en cuenta para crear un plan de simulación. Queda a discreción del equipo de atención de desastres definir qué actividades se estarían realizando en un experimento de este tipo.

1. Alerta inicial de desastre.
   a) Contactar a las personas por teléfono.
   b) Describir el desastre.
   c) Hacer un reporte preliminar de los daños.
   d) Notificar a los demás grupos y personas.

2. Evaluación del daño causado por el desastre.
   a) Enviar el equipo de respuesta.
   b) Realizar una visita al área afectada.
   c) Determinar los servicios básicos que sufrieron algún daño.
   d) Determinar el daño en el equipo.
   e) Restringir el acceso al sitio del percance.
   f) Estimar el tiempo de recuperación.

3. Activación de los planes de recuperación por desastre.
   a) Revisar la evaluación del daño.
   b) Determinar si el plan se debe activar en forma completa, parcial o si se debe abortar. Notifique al personal y a la administración.
   c) Buscar ayuda sobre asuntos legales y de contrato.

d) Monitorear las actividades de recuperación.

4. Planes de reacción para el cliente.
   a) Planear la reubicación del ambiente productivo a un sitio alterno.
   b) Validar los procesos para recuperar y sincronizar las bases de datos.
5. Estrategias de procesamiento alterno.
   a) Decidir si va o no va con el plan de recuperación.
   b) Identificar una estrategia de procesamiento alterno.
   c) Identificar el tiempo que estará sin operaciones debido a la estrategia utilizada.
   d) Determinar si los sitios dañados deben ser reconstruidos.
   e) Determinar los costos para la parte de seguros.
6. Determinar cuál equipo debe ser reemplazado, recuperado o comprado.
   a) Identificar los activos recuperables.
   b) Identificar los medios de recuperación.
   c) Aislar los activos recuperados en un sitio apropiado.
   d) Ordenar el reemplazo de los activos no recuperables.
7. Preparar el sitio alterno.
   a) Coordinar las instalaciones.
   b) Validar los sistemas.
   c) Asegurar la disponibilidad de suministros.
8. Restauración del ambiente operativo.
   a) Identificar los medios requeridos para restaurar los datos en el sitio alterno.
   b) Arreglar lo relacionado con el transporte, viaje y hospedaje del equipo que enviará al sitio alterno.
   c) Notificar a las personas que deban viajar.
9. Recuperación de aplicaciones.
   a) Preparar las aplicaciones críticas.
   b) Crear cronogramas de recuperación.

c) Revisar los medios magnéticos recuperados para su posible utilización.

d) Restaurar los datos.

e) Definir la pérdida de información y las necesidades de reprocesamiento de datos.

f) Verificar los puntos de sincronización de bases de datos.

10. Restaure las comunicaciones.

a) Restaurar las comunicaciones que soportan a los sistemas y procesos críticos.

b) Restaurar el resto de las comunicaciones.

Se deben planificar simulaciones regularmente para las partes más importantes del plan, o sea, las que están relacionadas con las funciones críticas del negocio.

ANUALMENTE

Se valida la recuperación en el sitio alterno de los principales sistemas, incluyendo sistemas operativos, periféricos, etc. Adicionalmente, los gerentes deben verificar la eficiencia del plan y el entrenamiento de su personal a cargo.

SEMESTRALMENTE

El área de operaciones de los sistemas de información debe ejecutar las siguientes funciones:

- Verificar los respaldos de datos.
- Probar el sistema de recuperación de datos.

CONTINUAMENTE

- Actualizar el DRP cada vez que se dé un cambio en el sistema.
- Revisar los planes con el personal para verificar su entendimiento.
- Validar los equipos y sistemas en el sitio alterno.

3.6. Administración de la comunicación

La gestión de las comunicaciones del proyecto, es el área de conocimiento que incluye los procesos necesarios para asegurar la generación, recopilación, distribución, almacenamiento, recuperación y destino final de la información del proyecto en tiempo y forma. Los procesos de gestión de las comunicaciones del proyecto proporcionan los enlaces cruciales entre las personas y la información, necesarios para unas comunicaciones exitosas.

De acuerdo al proyecto de Recuperación en caso de Desastre, los procesos de Gestión de las comunicaciones del proyecto, incluyen lo siguiente:

3.6.1. Planificación de las comunicaciones

En un proyecto en el que se ve involucrado la mayoría de personas dentro de la organización, el plan de comunicaciones se convierte en un factor crítico de éxito o fracaso del proyecto. En la medida en que se comunique el plan del proyecto y, por medio de estos comunicados se involucre a todas las personas relacionadas con las distintas fases del proyecto, en esa medida aumentarán la probabilidad de éxito del mismo.

La siguiente matriz (figura 14), muestra un ejemplo de los distintos tipos de comunicación que se podrían utilizar en el proyecto, bajo el supuesto de que el equipo del proyecto se encuentra ubicado en el mismo lugar, haciendo énfasis en los siguientes puntos:

1. Nombre o tipo de comunicación.
2. Intención o propósito de la comunicación.
3. Responsable de la comunicación.
4. Distribución de la comunicación.
5. Medio a utilizar en la comunicación (Ej. Reunión, conferencia telefónica, correo electrónico, etc.).
6. Frecuencia (tiempo) de la comunicación.
7. Consideraciones especiales.

TIPO (1)	PROPÓSITO (2)	RESPONSABLE (3)	DISTRIBUCIÓN (4)	MEDIO (5)	FRECUENCIA (6)	CONCIDERACIONES ESPECIALES (7)
Reuniones con el Comité Ejecutivo.	• Informar a la gerencia de la Organización acerca del avance del proyecto y los resultados obtenidos al momento. • Comunicar los principales "issues" del proyecto, sobre todo los que requieren de la intermediación de la alta Gerencia. • Comunicación de cambios en el alcance o los objetivos.	Ernesto Rivera / Director del proyecto.	Equipo del proyecto Comité Ejecutivo.	Reunión presencial en la sala de capacitación de la Empresa.	De Lunes por medio, 09:00 AM	Se debe distribuir la agenda anticipadamente. Se debe generar una minuta de la reunión la cual será guardada en la carpeta del proyecto.
Reuniones de liderazgo extendido.	• Seguimiento al cronograma • Aprobar y tomar decisiones. • Resolver los asuntos relacionados a los recursos del proyecto.	Director del proyecto.	• Gerente Infraestructura. • Gerente de Desarrollo. • Director del Proyecto. • Administrador de la Base de Datos. • Expertos invitados.	Reunión presencial en la sala de capacitación de la empresa.	Cada Martes, 09:00 hrs. AM	Se debe generar una minuta de la reunión, la cual será guardada en la carpeta de proyecto.
Reunión de seguimiento con el equipo del proyecto.	Actualizar a la audiencia con información corporativa, local y del equipo del proyecto.	Director del proyecto.	Equipo del proyecto.	Reunión presencial en la sala de capacitación de la empresa.	Cada Miércoles, 09:00 hrs AM	Informal.
Boletines por correo electrónicos	Comunicar asuntos importantes del proyecto a toda la organización.	Liderazgo de toda la organización. Director del proyecto.	Empleados de toda la organización.	Correo electrónico.	Por demanda.	Publicar en la Web Site, sección de noticias.

Figura 14. Ejemplo de una Matriz de Comunicaciones.

En la matriz de comunicación, prácticamente todas las áreas de la organización se ven relacionadas con un proyecto que pretende habilitar las principales funciones de la organización en caso de desastre, por lo tanto es de suma importancia que se respete la columna de distribución contemplada en la Figura 14.

Es importante que el proyecto cuente con un sitio web, preferiblemente en la intranet de la organización, en el cual se publiquen las noticias más relevantes del proyecto, los “issues”, necesidades, formatos y toda aquella información que se deba compartir y permear en la organización. También es importante fomentar el ingreso al sitio web de manera que el proyecto se asegure de que la información está llegando a todas las áreas involucradas.

Finalmente, al finalizar cada fase del proyecto o cuando el director del proyecto lo considere, se deben generar sesiones de lecciones aprendidas en las cuales se analicen las oportunidades de mejora y se fortalezcan las ideas que han tenido éxito a lo largo del ciclo de vida del proyecto. El resultado de una sesión de lecciones aprendidas debe almacenarse en la carpeta del proyecto en forma de minuta de manera que se convierta en un activo más de la organización.

4. SOLUCIÓN TECNOLÓGICA

4.1. Infraestructura plataforma SAP ERP

Se propone un escenario de última generación tecnológica, de manera que la solución disponga de todos los componentes, recursos e infraestructura necesaria para permitir un alto nivel de seguridad, redundancia, certificación, robustez y performance.

Con el propósito de satisfacer la necesidad de servicios para la aplicación SAP ERP, se ha definido continuar con el esquema actual de la infraestructura compuesta por dos servidores independientes de manera de disponer de continuidad de servicios, proveer tecnología, escalabilidad y una capacidad de procesamiento de varias veces el crecimiento, respecto de la actual infraestructura.

La solución definida, consta de una capa de servidores perteneciente a la familia Power Systems, con procesadores de última generación IBM Power7, con propiedades para soportar tecnología de multi-cores, esto es procesadores desde six-cores hasta eight-cores, con un máximo de hasta 32 cores, con 4 MB de L3 cache por core, crecimiento en memoria hasta un máximo de 256GB.

Esta arquitectura de procesadores definida en la solución está enfocada a organizaciones que requieren escalabilidad, alto rendimiento y un extremo nivel de paralelismo en el procesamiento asociado a altas cargas de trabajo. La tecnología Power7 entrega ventajas comparativas respecto a otras plataformas, tales como:

- Innovadora arquitectura de memoria basada en mayor capacidad, reflejado en mayor velocidad de transferencia de datos.
- Procesadores de dos controladores de memoria DDR3, con cuatro canales de memoria.

- Capacidad para combinar diferentes modelos de expansiones dependiendo de las necesidades del negocio.
- Redundancia de componente y auto-reparación concurrente.
- Procesadores con propiedades Intelligent Threads, dependiendo del nivel de carga en demanda.
- Capacidad de optimizar múltiples clases de workload.
- Procesadores con consumo inteligente de Energía.
- Incorporación de tecnología Integrated Virtual Ethernet adapter (IVE) o Host Ethernet Adapter (HEA).
- Nuevo protocolo asociado a canales de fibra sobre Ethernet (FCoE).
- Tecnología InfiniBand Architecture (Bus de comunicaciones serie de alta velocidad, diseñado tanto para conexiones internas como externas).
- Live Partition Mobility (componente de la característica de hardware PowerVM Enterprise Edition, ofrece la posibilidad de mover particiones lógicas AIX, IBM).
- Single processor checkstop (arquitectura permite que un sistema informático se detenga de inmediato cuando se produce un fallo o error).

El dimensionamiento de la infraestructura de servidores, se detallan a continuación:

Site	Función del Servidor	Nombre Servidor	Tipo de Servidor	Storage	Sistema Operativo	Base de Datos	CPU (cores)	Memoria (GB)
Providencia (Primario)	Servidor Central	cmpcr3p	Power 770 3.1 GHz	DS8800	AIX 7.1	DB2 10.1	5.5	52
	Aplicativo Dialogo	cmpcapp6					2.0	30
	Aplicativo Dialogo	cmpcapp8					2.0	30
	Aplicativo Batch	cmpcappw1					2.0	22
San Bernardo (Secundario)	Servidor Central	cmpcr3s	Power 770 3.1 GHz	DS8800	AIX 7.1	DB2 10.1	5.5	52
	Aplicativo Dialogo	cmpcapp7					2.0	30
	Aplicativo Dialogo	cmpcapp9					2.0	30
	Aplicativo Batch	cmpcappw2					2.0	22

Figura 15. Dimensionamiento de la Infraestructura.

El dimensionamiento de la infraestructura se realizó mediante una técnica de IBM llamada Techline, la cual se utiliza para generar estimaciones basadas en los requerimientos del cliente. Su funcionalidad permite definir los requerimientos del cliente y llevarlos a un plano físico, que ayude a determinar los servidores y otros componentes requeridos para poder entregar el servicio solicitado.

El servidor SAP ERP, está compuesto de un servidor central el cual contiene la base de datos, cuatro servidores de dialogo (conexiones para usuarios SAP), dos servidores para procesos de fondo y un servidor imagen del servidor central.

Estos servidores se dividen en el sitio de Providencio (Primario) y sitio de San Bernardo (Secundario).

4.2. Sistemas de Base de Datos Plataforma SAP ERP

Actualmente el sistema de administración de base de datos, utilizado para la plataforma que soporta el aplicativo SAP ERP es IBM DB2 v9.7. Esta versión permite potenciar el servicio entregado con la incorporación de funciones y productos que permitan a la actual base de datos entregar un servicio que permita una continuidad operacional continua, soporte de mantenciones en línea de parches, alta disponibilidad y balanceo de carga.

Para llevar a cabo esta solución, se ha definido una estrategia de solución planificada en dos etapas, las cuales incluirán funcionalidades como actualización hacia una nueva versión del actual sistema de base de datos IBM DB2 9.7 a IBM DB2 10.1, de modo de permitir la continuidad del negocio, lograr mantenciones en línea de parches, disponer de réplicas remotas en caso de corrupción o borrado accidental de datos, balanceo de carga e instancias en modalidad activa-activa.

La primera etapa comprendida en esta estrategia define un periodo de seis (6) meses, que corresponden a la fase de transformación y salida en régimen de la nueva infraestructura, con la cual se comenzará a operar.

Esta etapa corresponde la incorporación de nuevas funcionalidades de la base de datos IBM DB2 v9.7, tales como réplica remota entre nodos independientes, re direccionamiento automáticos de las aplicaciones entre nodos alertas y ejecución automático antes eventos de failover y suministrar un ambiente activo-pasivo. Para lograr este cometido se implementará el producto conocido por IBM DB2 HADR.

IBM DB2-HADR, define una estructura compuesta por dos nodos en servidores independientes o en particiones lógicas (LPARES) para plataformas virtualizadas que se asocian a los siguientes roles: nodo primario y nodo standby.

El nodo primario representa al ambiente principal de la base de datos y es quien soporta los servicios mediante operaciones de lectura y escritura a la base de datos, además de las conexiones activas de usuarios y aplicaciones.

El nodo standby representa al ambiente que soporta la réplica continua de datos proveniente del nodo primario, a través de los archive logs de la base de datos primaria y que son transportados hacia una base de datos en modalidad standby residente en este nodo. Posteriormente ante la ocurrencia de una falla en el nodo primario, el nodo standby asumirá el rol del nodo primario, activando la base de datos en modalidad activa.

Las ventajas que se desprenden del producto IBM DB2 HADR se pueden resumir en:

- Permite ejecutar lecturas desde el nodo standby.
- Permite re ruteo automático (ACR) de la aplicación al nodo standby.
- Recuperación en menos de 15 segundos ante la falla del nodo primario.
- Permite replica remota hacia la base de datos standby.
- Permite actualizaciones de parches sin bajar el servicio.

- Incorporación del Tivoli System Automation (TSAM), para monitoreo del clúster y ejecución automática del takeover.
- Mantiene el mismo nivel de alta disponibilidad.

A continuación se presenta un diagrama con los principales elementos de la arquitectura asociada a DB2 HADR.

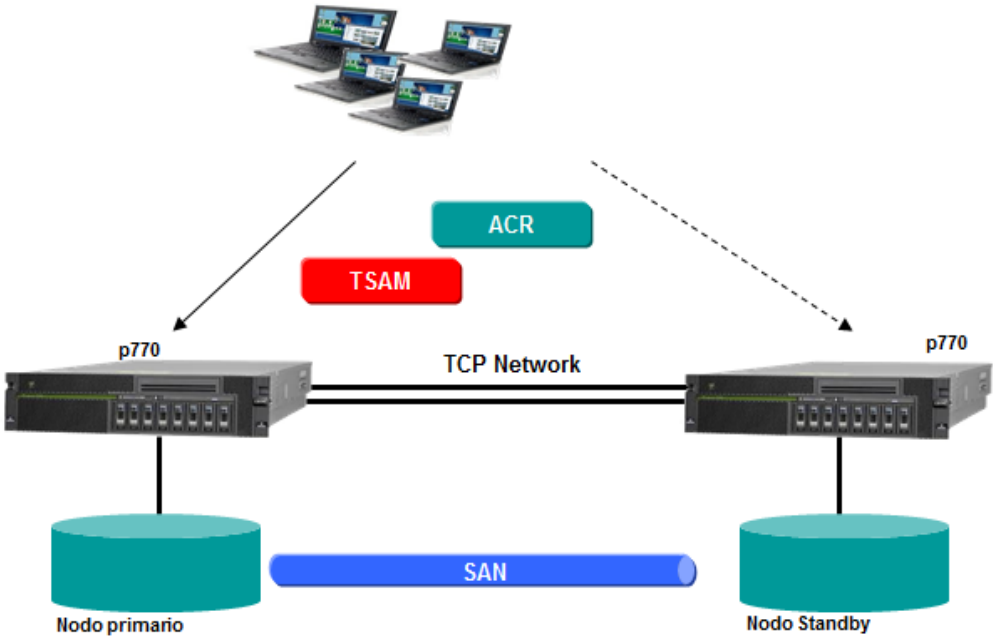


Figura 16. Solución Etapa 1.

La figura 16, representa la implementación de la etapa1 con la solución propuesta dada por IBM DB2 v9.7 HADR, la que está contenida en la infraestructura asociada al aplicativo SAP ERP. Esta define la configuración del producto IBM DB2 V9.7 HADR en la infraestructura Power7, descrita anteriormente y que comprende la instalación del nodo primario en una partición lógica (LPAR) de un Power 7 y del nodo standby en otra LPAR del otro Power7.

Entre cada nodo se establecerá una conexión redundante TCP/IP por donde fluirá la réplica de los archive logs de la base de datos.

Para esta primera etapa, el punto de recuperación (RPO) esperado es de 3 a 5 segundos, mientras que el objetivo de tiempo de recuperación (RTO) esperado, es de 3 horas.

La segunda etapa de esta estrategia, define un inicio de actividades una vez finalizada la etapa de transformación y una vez el nuevo servicio se encuentre en la etapa de régimen.

Para el desarrollo de la segunda etapa, se proyecta proveer una versión mejorada del actual sistema de administración de base de datos, que permitirá suministrar un servicio que entregue continuidad operacional, servicios en modalidad de clúster con instancias activa-activa, balanceo de carga automático, mantenciones, en línea, incorporación o eliminaciones de nodos dinámica, sin afectar el servicio, re direccionamiento balanceado y automático de la aplicación ante la falla de un nodo, hacia el resto que permanece entregando servicios.

El producto que IBM ofrece y que cumple con todas estas nuevas funcionalidades es DB2 10.1 pureScale.

Debido a lo reciente en el mercado de este producto, se ha definido como estrategia, planificar la implementación de este producto en forma progresiva definiendo un conjunto de fases previas a la implementación del producto en los ambientes que prestan el servicio en régimen.

Con esta nueva funcionalidad, el punto de recuperación esperado (RPO) es de 1 a 0 (cero) segundo y el objetivo de tiempo de recuperación (RTO) esperado, también es de 1 a (cero) segundos.

Piloto y Ambientes Operacionales

Como primera fase se configurará la creación de un ambiente Piloto, definiendo este ambiente en una partición lógica (LPAR) en cada servidor Power7 asociado a la infraestructura SAP ERP, posteriormente se habilitar este ambiente,

para la ejecución de pruebas funcionales, de certificación, de performance y todos los escenarios que se crean necesarios para permitir que la implementación de este nuevo producto en la solución actual, sea lo más confiable, eficiente y estable, de modo de no afectar la operación del negocio.

De modo de minimizar los riesgos asociados a la incorporación de este producto a los ambientes críticos, se ha dispuesto, una vez certificado este ambiente de prueba, una implementación inicial del producto en los ambientes pre-productivos y finalmente en los ambientes productivo.

A continuación, se presenta un diagrama con los principales elementos de la arquitectura asociada a DB2 10.1 PureScale.

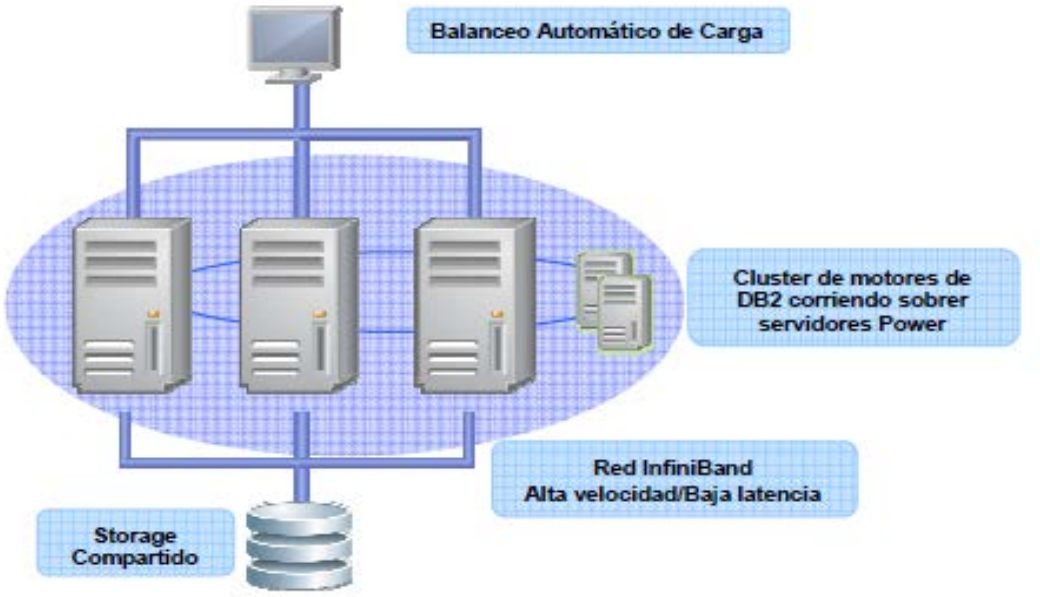


Figura 17. Solución Etapa 2: Arquitectura DB2 10.1 pureScale.

Esta solución apunta a ofrecer un completo esquema de instancia activa-activa ofreciendo con ello un verdadero ambiente de operación continua del servicio, entregando un servicio libre de indisponibilidades por efectos de fallas de un nodo o mantenciones de hardware o actualizaciones de base de datos.

La replicación sincrónica tiene la ventaja de estar continuamente actualizada en el sitio de destino. Se tiene siempre la certeza de que los datos existentes en la sitio de destino, están tan al día, como los datos del sitio de origen.

La solución DB2 10.1 pureScale, nos permite soportar grandes cargas de trabajo, manteniendo balanceo automático de carga en cluster de motores de base de datos DB2. Además, a la incorporación de la solución InfiniBand, nos permite una alta velocidad a baja latencia[9] para largas distancias.

4.3. Infraestructura de Respaldo y Monitoreo

Los servicios de respaldo y monitoreo representan una componente critica en el compromiso de mantener la continuidad del negocio.

Pensando en esta componente y potencial punto crítico de falla, se incorpora un ambiente de alta disponibilidad asociado a los servicios de respaldo y monitoreo.

A continuación se muestra una diagrama asociada a esta solución:

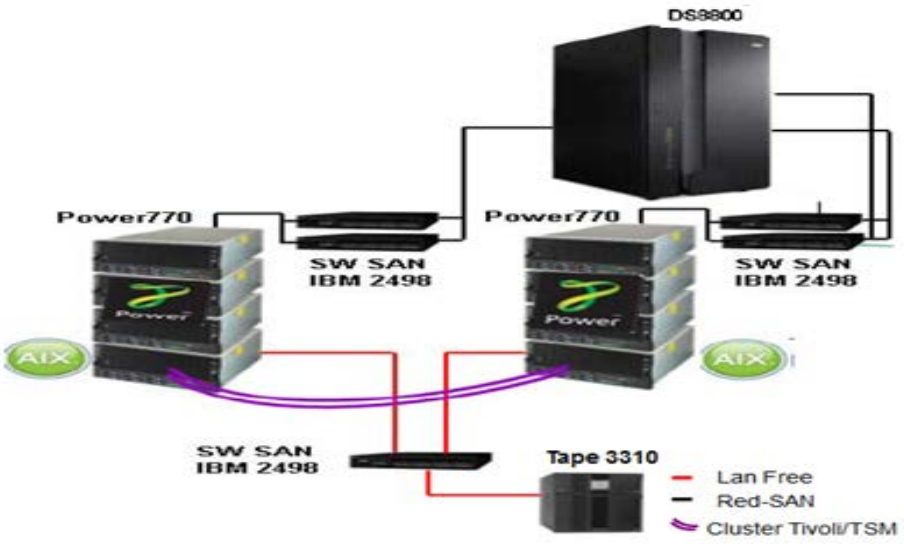


Figura 18. Infraestructura de respaldo y monitoreo.

[9] Suma de retardos temporales dentro de una red.

La solución está compuesta con tecnología Power7, esto es una partición lógica (LPAR) que contenga los servicios de respaldo y otra LPAR conteniendo los servicios de monitoreo, luego ante una falla de alguno de estos servicios este sea soportado y contenido por la (LPAR) activa.

Las unidades de respaldo conectadas, son TS3310 con dos expansiones provista de 4 drivers LTO4 y 6 drivers LTO5 (SAS[10]), este tipo de unidad utiliza el último estándar de la industria con una interfaz de 6 GB por segundos.

El servicios de administración de respaldos es Tivoli Storage Management v6.1 (TSM). Este software ofrece protección de datos automatizada y centralizada para reducir los riesgos asociados con la pérdida de datos, además centraliza las operaciones de gestión de almacenamiento.

4.4. Almacenamiento

Respecto al ambiente de almacenamiento externo de datos, se propone en su estrategia la consolidación, simplicidad, escalabilidad y virtualización de manera de que ésta este alineada con la estrategia de virtualización de servidores con el fin de proveer una infraestructura dinámica y escalable.

Para poder llevar a cabo estos objetivos, se ha propuesto en su solución, el uso de un sistema de almacenamiento de última generación denominada Serie IBM System Storage DS8800.

A través de esta solución, se ofrece un producto que permite estabilidad, robustez y confianza, que son reflejadas por las siguientes características:

- Mayor performance con la incorporación de procesadores de la familia Power7.
- Reducción del espacio físico asociado al uso de discos más pequeños.
- Mayor capacidad de almacenamiento.

[10] Serial Attached SCSI.

- Mayor capacidad de memoria por procesador.
- Mejoras respecto de la conectividad con 4 y 8 Port Fibre .Channel/FICON.
- Incorporación Thin Provisioning.
- Dinamic Volumen Expansion, simplifica la administración asociada al aumento de espacio en línea y migraciones con grandes volúmenes de datos.
- Incorporación de FlashCopy SE, disminuyendo el volumen de espacio requerido por el FlashCopy tradicional.
- Continuidad de negocio por medio de funciones avanzadas de copia de disco.

4.5. Sitio de Contingencia

Como complemento a la solución del sitio principal y a una solución del tipo DRP, se ha resuelto proponer, la implementación de un sitio de contingencia que pueda entregar una alta disponibilidad y contingencia de los servicios críticos SAP ERP, ante la caída del sitio principal, una óptima distribución del hardware, redundancia en enlaces y redes extendidas TCP/IP y SAN, mínimos tiempos de recuperación entre sitios.

A modo de entregar la mejor solución de contingencia reflejada en confiabilidad, disponibilidad, crecimiento y robustez, ha definido una estrategia que permitirá disponer de un sitio de contingencia que cumple con todas las normas asociadas y estándares a un sitio del tipo Tier 3+[11].

La definición de la distribución del hardware en el sitio de contingencia de estará definida de la siguiente manera:

[11] Estándar internacional (TIA-942) que indica los grados de disponibilidad con los que pueden clasificarse los centros de datos. La tasa de disponibilidad de un Tier 3 es de 99.982%.

- Un servidor Power7 en cada sitio, dejando los servicios críticos de CMPC en el sitio principal y los de media y baja criticidad en el sitio 2 además de los ambientes de contingencia de los servidores críticos.
- Un Blade Server en cada sitio de manera de asegurar alta disponibilidad y contingencia para los servicios que están sobre la plataforma virtual.
- Sistema de Almacenamiento DS8800 como réplica del sistema de almacenamiento principal DS8800.
- Unidad de storage adicional de manera de eliminar puntos de fallas asociados al resguardo de los datos y definir un respaldo cruzado de datos.

A continuación se presenta, la solución asociada al sitio de contingencia:

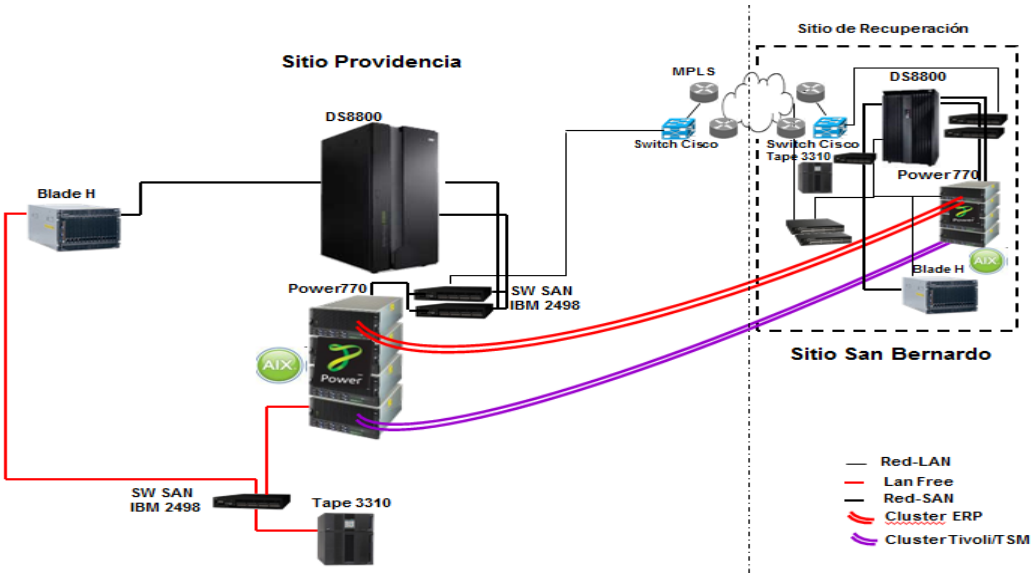


Figura 19. Solución con ambos sitios (Providencia – San Bernardo).

Como alternativa de falla a la solución anterior, figura 19, se proveerá con un sistema de almacenamiento en modo de alta disponibilidad local DS8800, permitiendo con ello en caso de un falla de disco, inconsistencia o borrado accidental de los datos, tener un sistema de almacenamiento alternativo que puede ser activado en un tiempo mínimo.

5. IMPLEMENTACIÓN DEL PLAN

5.1. Creación del equipo del proyecto

En un proyecto donde es necesario el apoyo de toda la organización se requiere de un soporte constante de los niveles gerenciales de la compañía. Por esta razón, se recomienda crear una estructura de equipo dividida en un comité ejecutivo y un comité operativo, cada uno de estos con roles y responsabilidades particulares los cuales se detallan a continuación.

5.2. Comité ejecutivo del Proyecto

Estará conformado de acuerdo a los requerimientos estratégicos de la empresa, en él participan los patrocinadores del proyecto. Su función principal será la de controlar desde una perspectiva gerencial, el buen desarrollo del proyecto y que se cumpla según los parámetros establecidos en el plan del proyecto y los compromisos entre las partes. La figura 20, muestra un ejemplo de un posible comité ejecutivo.

PUESTO	NOMBRE	DEPARTAMENTO
Gerente-Empresas CMPC	Javier Cáceres	Gerencia
Gerente Tecnología	Pedro Cabezas	Tecnología
Gerente Desarrollo	Oscar Castro	Desarrollo
Director PMO	Juan Montes	Administración Proyectos

Figura 20. Comité Ejecutivo.

El objetivo de este comité es darle al contrato un control estratégico y asegurar la oportuna toma de decisiones sobre aspectos que lo modifiquen en tiempo, alcances y costo. Se reunirá semestralmente o cuando sea requerido por el comité operativo.

5.3. Comité operativo

El objetivo de este comité es el de realizar la gestión táctica y operativa del proyecto. Deberá estar conformado por representantes del comité ejecutivo, el director del proyecto, asesores del proyecto y los representantes de cada producto a recuperar en el sitio alterno. Se reunirá semanalmente durante los períodos de mayor actividad o criticidad del contrato o cuando los gerentes de proyecto lo requieran.

Debe dar solución o acciones de solución a inconvenientes presentados durante el proyecto siempre y cuando estos no afecten al mismo en alcance, tiempo y costos, así como alertar a los miembros del comité ejecutivo sobre situaciones que excedan su competencia. Además de, controlar el avance del proyecto y la calidad de las entregas.

5.4. Roles y Responsabilidades

Con la finalidad de cumplir con los objetivos trazados, se establecen los siguientes roles y responsabilidades dentro del equipo del proyecto.

Los roles están agrupadao como grupos lógicos de tareas. Estos no están agrupados para que coincidan con ninguna estructura específica organizacional:

- Varios roles pueden ser ejecutados por el mismo individuo.
- Un rol puede ser dividido entre varios individuos.

Coordinador del plan:

- Planificar el plan de recuperación con todos los involucrados en la misma.
- Coordinar el plan durante la recuperación.
- Identificar mejoras al plan acordado.
- Asegurarse que todo el personal involucrado en el plan esté familiarizado con los procedimientos de recuperación.

- Asegurarse que se generen las evidencias definidas para analizar resultados.
- Planificar reuniones de análisis y revisión del plan.

Cliente:

- Identificar el impacto del negocio.
- Evaluar, acordar o definir el plan de Disaster Recovery, según se hayan definido en el contrato.
- Acordar soluciones tanto en pruebas como en caso de desastre real.
- Notificar cambios en los requerimientos de negocio.
- Declarar la situación de contingencia.

Líder de Plataforma:

- Colaborar en el armado de la solución de TI para la recuperación.
- Informar a las partes posibles mejoras de TI en la implementación.
- Informar cualquier cambio en la configuración o infraestructura de los equipos que estén involucrados en el plan que afecten la recuperación.
- Implementar la solución definida.

5.5. Visión general del Proceso Disaster Recovery

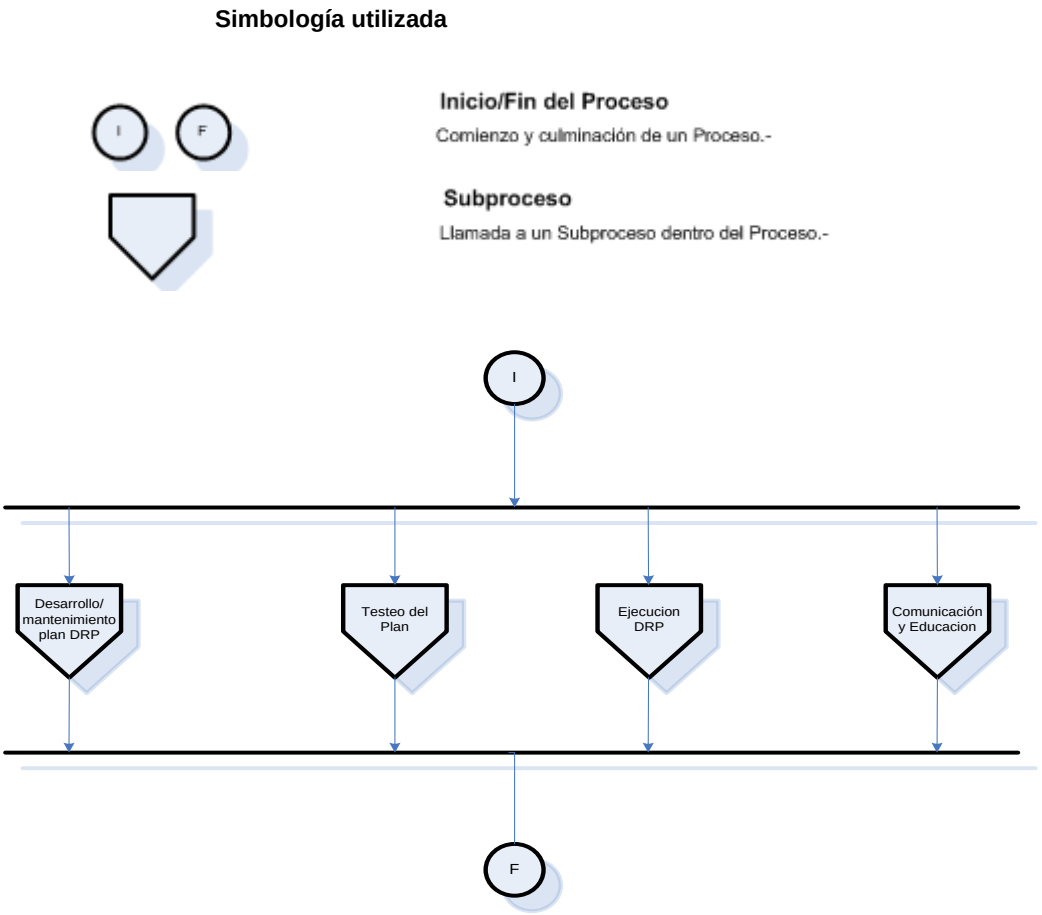


Figura 21. Visión general del Procesos Disaster Recovery

El Proceso Disaster Recovery, es una proceso compuesto por cuatro subprocesos (desarrollo y mantenimiento del plan, testeo del plan, ejecución DRP, y Comunicación y educación).

El Proceso Disaster Recovery está diseñado para proveer la estrategia de recuperación, planificación y pruebas de recuperación del sistema SAP ERP, detallado como el sistema crítico de los negocios en el caso de ocurrir una interrupción no programada calificada como desastre.

5.5.1. Componentes del Proceso Disaster Recovery

Objetivo:	Recopilar y traducir las necesidades de negocio criticas del cliente para implementar soluciones eficientes. Generar y mantener la documentación de los resultados de los planes llevados a cabo, tanto en pruebas programadas como en un caso de desastre. Evaluar el correcto funcionamiento de los planes acordados mejorando y/o actualizando el mismo si fuese necesario. Asegurarse que los planes estén vigentes, realizando un seguimiento de los cambios que afecten en la recuperación acordada. Reducir al mínimo el impacto de una interrupción del servicio en caso de desastre garantizando la disponibilidad de servicio.
Roles:	Coordinador del plan. Cliente. Líder de plataforma.
Prerrequisitos:	Acuerdo de servicio.
Entradas:	Contrato firmado por el cliente.
Salidas:	Proceso, procedimientos, plan, capacitación. Ejecución del test. Restauración del servicio.
Controles:	PC1: Acordar condiciones en test. PC2: Generar plan de testeo. PC3: Analizar resultados en prueba o situación real.

5.5.2. Componentes del Desarrollo / Mantenimiento plan DRP

Objetivo:	Crear y actualizar el plan basado en el acuerdo con el cliente para poder implementar la solución de contingencia en caso de pruebas o cortes de servicio no programados.
Roles:	Cliente. Coordinador del plan.
Prerrequisitos:	Acuerdo de solución.
Entradas:	Contrato firmado con el cliente. Plan previo Requerimientos del cliente.
Salidas:	Plan DRP.
Controles:	N/A
Evento:	Definición y actualización solución.

5.5.3. Componentes del Testeo del Plan

Objetivo:	Realizar pruebas para probar el correcto funcionamiento del plan acordado, documentar debilidades y mejorar el funcionamiento.
Roles:	Coordinador del plan. Team líder de plataforma. Cliente.
Prerrequisitos:	Solución de TI Definida.
Entradas:	Calendario de ejecución.
Salidas:	Documentación de los test para realizar mejoras y/o actualizaciones. Informe de resultados de ejecución del test.
Controles:	PC1 Acuerdo de alcance en test. PC2 Generación plan de testeo. PC3 Análisis de resultados en prueba o situación real.
Evento:	Según Calendario.

5.5.4. Componentes de Ejecución DRP

Objetivo:	Ejecutar el plan según lo planeado y analizar los resultados.
Roles:	Cliente. Líder de plataforma. Coordinador del plan.
Prerrequisitos:	Acordar el plan y la solución con el cliente.
Entradas:	Documentación de ejecución del plan. Información de inicio de actividad de DRP.
Salidas:	Ambiente recuperado siguiendo las tareas planificadas.
Controles:	PC3 Análisis de resultados en prueba o situación real.
Evento:	Declaración de contingencia.

5.5.5. Componentes Comunicación y Educación

Objetivo:	Educar y comunicar sobre el proceso vigente realizando charlas y cursos.
Roles:	Coordinador del plan.
Prerrequisitos:	Conocer el proceso Disaster Recovery. Entender el alcance del proceso.
Entradas:	Proceso, procedimientos y planes.

Salidas:	Cursos y charlas educativas del proceso.
Controles:	N/A
Evento:	Necesidad de capacitación.

5.5.6. Puntos de control

Un punto de control es un medio utilizado para evaluar el proceso de forma tal de poder determinar si el servicio se brinda de acuerdo a lo que el dueño del proceso definió y acordó.

Punto de Control Numero	**PC1**
Nombre del Punto de Control	Acuerdo de condiciones en test.
Objetivo del Punto de Control	Verificar que se haya acordado el alcance del test.
Quien lo realiza	Coordinador del plan.
Frecuencia	Según pactado en el contrato.
Actividades donde aplica	Acordar Condiciones.

Punto de Control Numero	**PC2**
Nombre del Punto de Control	Generación plan de testeo.
Objetivo del Punto de Control	Generar un plan para implementar en la prueba de recuperación.
Quien lo realiza	Coordinador del plan.
Frecuencia	Según pactado en el contrato.
Actividades donde aplica	Generar plan de testeo.

Punto de Control Numero	**PC3**
Nombre del Punto de Control	Análisis de resultados en prueba o situación real.
Objetivo del Punto de Control	Verificar la existencia del informe de resultados.
Quien lo realiza	Coordinador del plan.
Frecuencia	Según pactado en el contrato.
Actividades donde aplica	Analizar resultados.

5.5.7. Matriz de Responsabilidades

A continuación se plasman dos Figuras. La primera mapea las áreas versus los roles del proceso y la segunda mapea las áreas versus las actividades del procedimiento.

Rol / Area	líder de Plataforma	Coordinador DRP	Cliente
Dueño del Proceso		**X**	
CMPC			**X**
Plataforma UNIX	X		
Plataforma Storage	X		
Base de Datos	X		
Plataforma SAP			X

Figura 22. Áreas versus roles del proceso.

Rol	Coordinador DRP	líder de Plataforma	Cliente
Área / Actividad	Dueño del proceso	(ver figura superior)	CMPC
Acordar condiciones	X		X
Generar plan de testeo	X		
Ejecutar testeo	X	X	X
Analizar resultados	X		X
Definición / Actualización solución DRP			
Desarrollo / Mantenimiento plan DRP			
Generar informe de resultados	X		
Iniciar ejecución del plan	X	X	X
Seguir procedimientos definidos	X	X	
Analizar resultados	X		X
Restauración del servicio a operación normal	X	X	

Figura 23. Áreas versus actividades del procedimiento.

5.6. Fases del proyecto

El servicio se divide en cinco (5) fases, cada una con actividades específicas, las cuales se detallan a continuación. Se indica un período de transformación de seis (6) meses, y a partir del mes siete (7) el proyecto entrará en su fase de régimen.

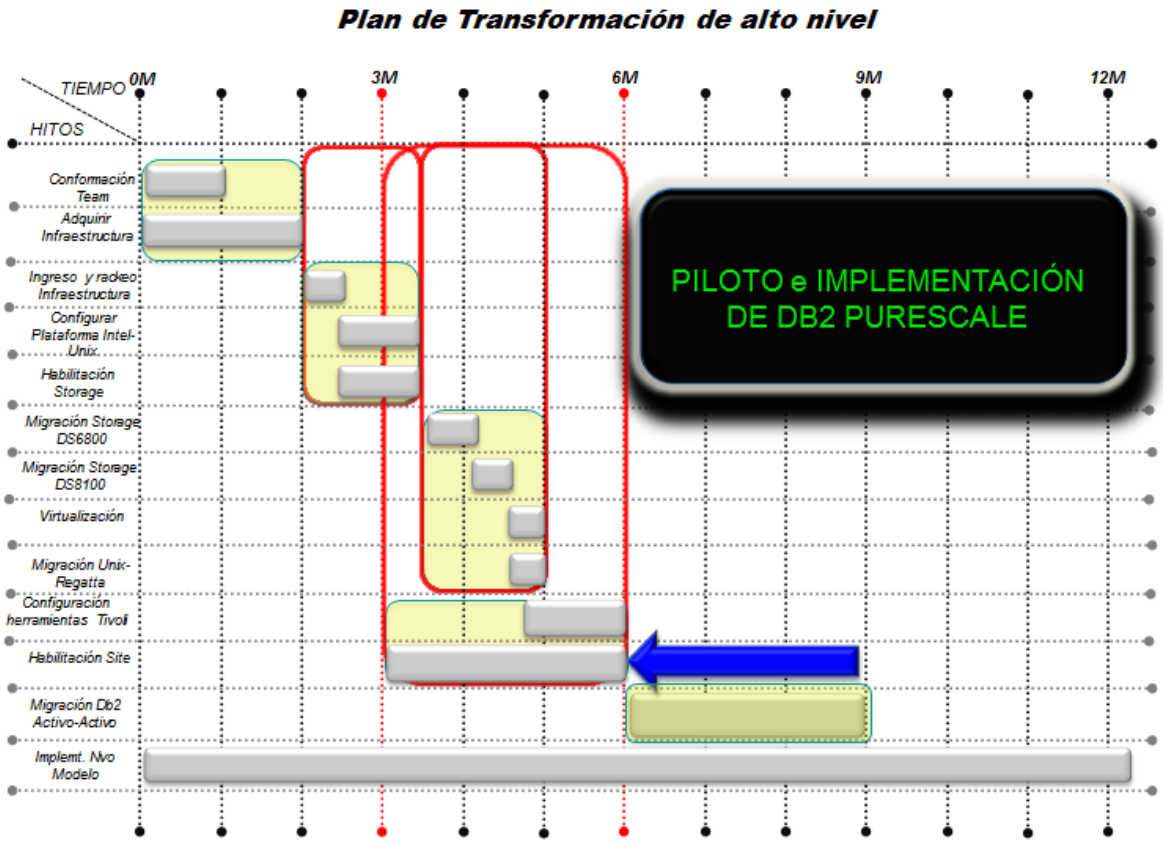


Figura 24. Fases del proyecto.

La actividades para el piloto e implementación de DB2 pureScale, se realizaran después de tener todas las condiciones disponibles en ambos sitios, Providencia (Primario) y San Bernardo (Secundario). Las condiciones de tecnologías necesarias son de conexión, comunicación, hardware, software y actualizaciones según recomendaciones estándares que describiremos en las fases siguientes.

5.6.1. Fase 1: Adquisición de infraestructura

Esta fase comprende la solicitud a la planta de la infraestructura requerida para la solución técnica ofrecida y comprende las siguientes etapas.

Etapa 1 — Envío de infraestructura desde la planta hacia la bodega de IBM:

En esta etapa se realiza la configuración de las solicitudes a plantas y comprenden de acuerdo a la infraestructura requerida diferentes procesos que resultan en diferentes procesos de envíos de ésta hacia la aduana en Chile.

Etapa 2 — Traslado de Bodega de IBM hacia al sitio donde residirá la Infraestructura:

Una vez trasladada la infraestructura desde la aduana a la bodega de IBM, el siguiente paso es generar la solicitud para que la infraestructura sea trasladada al sitio respectivo donde ésta deberá ser instalada y configurada. Una vez ingresada la infraestructura al sitio el cual ya estará con la energía e instalaciones de redes necesarias para soportarla, se procederá a instalar y configurar en los racks y espacios en donde residirán en forma permanente.

5.6.2. Fase 2: Habilitación infraestructura

Esta etapa comprende la conexión entre las diferentes partes de la infraestructura que requieran ser relacionadas, virtualización de los servidores y sistemas de almacenamiento, y por último la instalación de todo el software base en los servidores que se requieran. Las principales actividades definidas para esta fase son:

Etapa 1 — Unidad de Almacenamiento:

- Conectividad módulos de discos en la unidad de almacenamiento.
- Conectividad switch de comunicación y de Fibra.
- Actualización de micro código y licenciamiento.
- Configuración de zonas.
- Definición componentes de virtualización para la migración de datos desde la unidad de almacenamiento actual.
- Configuración de la organización de los discos para soportar la migración.

Etapa 2 — Infraestructura Intel Blade

- Instalación VMware en hojas del nuevo Blade H.
- Instalación y configuración software base en sistema lógicos.
- Configuración conectividad switch LAN y SAN.
- Virtualización y consolidación hojas en los Blades.
- Configuración Virtual Center y Vmtools.
- Instalación software asociado al cluster.
- Configuración Blades con funcionalidades de alta disponibilidad**.**

Etapa 3 — Infraestructura Unix Power 7

- Instalación y configuración Vios Server.
- Creación de Lpares.
- Configuración conectividad switch LAN y SAN.
- Instalación y configuración software base.
- Configuración de red LAN y SAN.
- Configuración asociada a las funcionalidades de la plataforma Power7.
- Instalación software asociado al cluster.

5.6.3. Fase 3: Migración y virtualización de infraestructura

Esta etapa comprende la migración desde la infraestructura actual a la nueva que prestará el servicio en CMPC. Esta define tanto la migración de los datos, como del software base y funcionalidades entre las plataformas que serán migradas. Las principales actividades que comprenden esta fase son:

Etapa 1 Migración de Datos

Etapa 1.1 Migración DS6800 - DS8800

- Configuración plataforma de virtualización para la migración.
- Respaldo de seguridad de datos.

- Configurar conectividad de fibras y comenzar la migración de datos en línea.
- Certificación técnica y funcional.
- Configuración funciones de réplica de datos local y remota.

Etapa 1.2 Migración DS8100 — DS8800

- Configuración plataforma de virtualización para la migración.
- Respaldo de seguridad de datos.
- Configurar conectividad de fibras y comenzar la migración de datos en línea.
- Configurar plataforma de servidores Unix al nuevo sistema de almacenamiento.
- Certificación técnica y funcional.
- Configuración funciones de réplica de datos local y remota.

Etapa 2 — Virtualización Intel Blade

- Configuración vmtools en hosts.
- Migración de datos vía vmware desde Blade H.
- Migración de datos vía vmware desde Servidores externos.
- Virtualización y consolidación hojas en los Blades H.
- Consolidación y virtualización servidores externos.
- Configuración agentes Tivoli.

Etapa 3 — Virtualización Unix Power 7

- Configuración Sistema Operativo.
- Copia Homogénea de SAP ERP.
- Licenciamiento aplicativo en nuevo hardware.
- Configuración power HA para Tivoli/TSM.
- Configuración DB2 HADR y nodos asociados al clúster.
- Pruebas power HA y DB2 HADR.

- Activación power HA Tivoli/TSM.
- Activación modo de réplica DB2-HADR.
- Configuración nodo standby con operaciones de lectura.

5.6.4. Fase 4: Configuración herramientas de apoyo

Esta fase comprende la instalación y configuración de las herramientas de apoyo a la solución entregada a Empresas CMPC, compuestas por las que soportan el servicio actual de modo de adecuarlas a la nueva infraestructura, como de las que se incorporan en la nueva solución. Las principales actividades definidas para esta fase son:

Etapa 1 Reconfiguración Tivoli /TSM

- Instalación y configuración de agentes en nuevos servidores.
- Redefinición de umbrales y alertas de acuerdo a la nueva infraestructura.
- Configuración de componentes de clúster parea agentes donde sea requerido.
- Configuración de respaldos en nueva infraestructura.
- Entrada en régimen de la nueva configuración de las herramientas.

Etapa 2 Instalación y Configuración Herramientas de Apoyo

- Instalación y configuración de herramientas de apoyo.
- Instalación y configuración agentes.
- Definición de Alertas y Umbrales.
- Definición de repositorios donde almacenar la información de monitoreo.
- Entrada en régimen de las nuevas herramientas de apoyo.

5.6.5. Fase 5: Piloto configuracionDB2 pureScale

El principal objetivo de esta última fase es la incorporación del administrador de base de datos DB2 pureScale V10.1, el cual representa la última

tecnología de IBM respecto a soluciones de alta disponibilidad con nodos activo-activo y con continuidad operacional permanente. Esta base de datos reemplazará al DB2 HADR v9.7 que a esta fecha estará entregando servicios. Las principales actividades definidas para esta fase son:

Etapa 1 Implementación del Piloto

- Creación y configuración de Lpares en infraestructura Power7.
- Creación y configuración Sistema Operativo.
- Configuración GPFS files Systems.
- Instalación DB2 v10.1 pureScale.
- Instalación SAP ERP sobre DB2 v10.1.
- Configuración DB2 pureScale.
- Configuración switch de alta velocidad asociados al pureScale.
- Configuración Instancia y ambientes de SAP ERP.
- Ejecución de pruebas técnicas y funcionales.
- Análisis de performance y conclusiones.

Etapa 2 Configuración DB2 PureScale en Ambientes Pre productivo

- Copia Homogénea de pre producción a nuevo ambiente.
- Configuración estructura GPFS.
- Configuración DB2 10.1 pureScale.
- Asignación de datos al nuevo ambiente.
- Post configuración DB2 pureScale.
- Actualización Enhanced Packages de SAP ERP.
- Configuración servidor de aplicaciones para ambiente pre productivo.
- Generación Going Live.
- Certificación y conclusiones**.**

Etapa 3 Configuración DB2 pureScale en Ambientes Productivo

- Copia Homogénea de producción a nuevo ambiente.

- Configuración estructura GPFS.
- Respaldo full de la plataforma.
- Configuración DB2 10.1 pureScale.
- Asignación de los datos al nuevo ambiente.
- Post configuración DB2 pureScale.
- Configuración switch de alta velocidad.
- Configuración capa de transportes y sistemas externos.
- Actualización Enhanced Packages de SAP ERP.
- Configuración Servidor de aplicaciones.
- Generación Going Live.
- Certificación y conclusiones**.**

5.7. Ejecución prueba DRP

En caso de una ejecución de un test el coordinador del plan deberá proceder a cumplir los siguientes lineamientos:

Recursos Humanos: Se deberá revalidar la asignación de recursos de los equipos de personas para la ejecución del test y proceder a la formalización de su asignación. Cualquier modificación en el equipo de personas asignadas deberá ser plasmada en el documento de contactos (*Ejemplo: Procedimientos de Contactos).*

Accesos: El coordinador deberá gestionar los accesos al sitio de contingencia y al DataCenter de los recursos asignados a través de la base de accesos.

Características Técnicas: El esquema de contingencia consiste en activar el servidor SAP CMPCR3P residente en el equipamiento ‘Providencia’ en el equipamiento ‘San Bernardo’ en LPAR CMPCR3S.

La metodología de copia se basa en replica DB2 HADR con sincronización adicional de los Filesystem de SAP mediante MetroMirror.

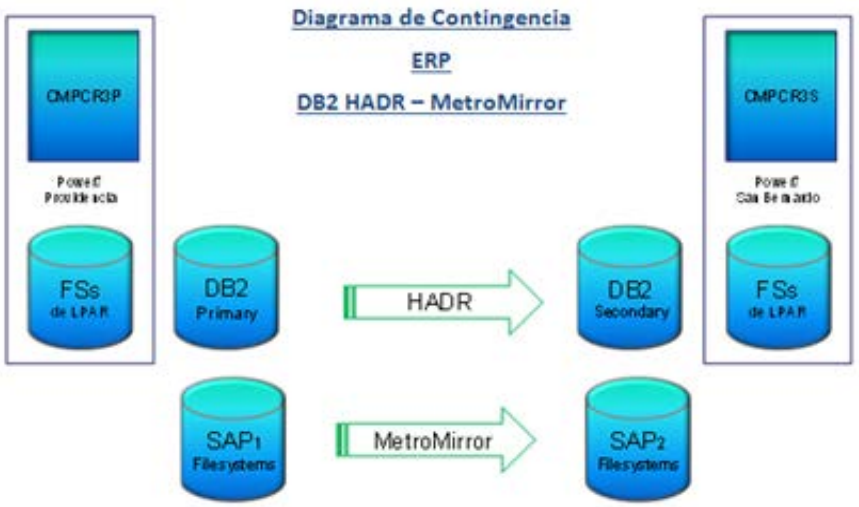


Figura 25. Diagrama de contingencia.

La tecnología DB2 HADR, nos permite que la base de datos secundaria tome el control como base de datos primaria con funcionalidad de DB2 completa. También es posible que se vuelva a activar la base de datos primaria original y que se devuelva a su estado de base de datos primaria.

MetroMirror, es un tipo de copia remota que crea una copia síncrona de los datos a partir de un volumen primario a un volumen secundario. Con copias síncronas, las aplicaciones host graban en el volumen principal, pero no reciben confirmación de que la operación de escritura se ha completado hasta que los datos se escriben en el volumen secundario. Esto asegura que tanto los volúmenes de la base de datos de Providencia, como la de San Bernardo, tengan datos idénticos cuando la operación de copia sea completada. La función de espejo de MetroMirror, mantiene una copia completamente sincronizada de los datos de origen, en el sitio objetivo en todo momento.

Respecto a los servidores aplicativos, existen tres servidores aplicativos idénticos en cada sitio, cmpcappw1, cmpcapp6 y cmpcapp8, están en el sitio de Providencia y los servidores aplicativos, cmpcappw2, cmpcapp7 y cmpcapp9, están en el sitio de San Bernardo.

Figura 26. Plataforma Power7.

Todos estos servidores aplicativos están activos y dando servicio. Cuando se activa la contingencia, solo los servidores aplicativos de San Bernardo quedan dando servicio, junto con el servidor centra cmpcr3s, quien contiene la base de datos.

5.7.1. Proceso de FailOver (Power7 Providencia – Power7 San Bernardo)

1.- Certificación de la replicación

- Sincronizada de DB2 en HADR.
- Replicación sincronizada de discos con MetroMirror.

2.- Detención de los servicios SAP sito Providencia

- Detener servicios SAP aplicativos.
- Detener Instancia central y base de datos.

3.- Simulación de la Pérdida de Power7 de Providencia

- Apagado de servidores cmpcr3p.
- Apagado de servidores cmpcappw1.
- Apagado de servidores cmpcapp6.
- Apagado de servidores cmpapp8.

4.- Activación del Failover a Power7 de San Bernardo

- Certificar desactivación IP virtual en cmpcr3p.
- Ejecutar Failover Recovery en San Bernardo.

- Ejecutar Failover de base de datos a su nodo secundario (HADR en DB2).
- Certificar IP virtual en cmpcr3s.

5.- Verificación de los servicios SAP

- Verificación SAP de instancia central y servidores de aplicación (solo San Bernardo).
    - servidor cmpcr3s
    - servidor cmpcappw2
    - Servidor cmpcapp7
    - Servidor cmpcapp9
- Verificación técnica y funcional.
- Certificación del sistema para finalizar la prueba de FailOver.

5.7.2. Proceso de FailBack (Power7 San Bernardo – Power7 Providencia)

1.- Activar Power7 Providencia

- Ejecutar Failback Recovery en Providencia.
- Encendido de servidor cmpcr3p (Levantar la base de datos, pero sin instancia SAP).
- Restablecimiento del HADR “San Bernardo -> Providencia”.

2.- Activar FailBack a Power7 de Providencia

- Certificación estado ‘peer’ de la réplica HADR del DB2.
- Certificación de la sincronización de volúmenes en MetroMirror.
- Ejecutar switch (FailBack) de base de datos a su nodo secundario.
- Certificar IP Virtual en cmpcr3p.
- Encendido de servidores aplicativos (sin subir SAP).
- Verificación de los servicios de todos los servidores.

3.- Activación de los servicios SAP

- Activación SAP en instancia central y servidores de aplicación.
- Verificación de servidor centran (cmpcr3p) y servidores aplicativos de Providencia y San Bernardo.

- Verificación técnica y funcional.
- Certificación del sistema para finalizar la prueba FailBack.
- Entrega del sistema a producción.

6. CONCLUSIONES Y RECOMENDACIONES

La frase “...espere lo mejor, pero prepárese para lo peor” resume la esencia de un plan de recuperación en caso de desastre.

Ocuparse por la continuidad del negocio debe ser una de las principales estrategias que deben desarrollar las organizaciones modernas, ya que, como se ha demostrado vastamente, un desastre ocurre cuando menos se espera y de esto depende, en la mayoría de los casos, la continuidad o el final de una empresa. Esto significa que debe dedicarse un rubro importante del presupuesto, al desarrollo, implementación y mantenimiento de un plan que garantice la continuidad de la operación.

A lo largo del trabajo desarrollado en esta tesis, se trató de plasmar una guía que le permita al lector conocer las principales actividades que debe desarrollar para implementar un plan de recuperación por desastre.

El plan abarcó la recuperación del Sistemas SAP ERP y sus procesos como un todo, sin embargo, vale la pena destacar la base de datos como elemento vital a proteger y restaurar antes de que un desastre impacte la organización.

El objetivo general de este proyecto consistió en diseñar una guía, con una serie de aspectos relevantes, que debe tomar en cuenta un gerente de proyectos a la hora de formular un plan de recuperación por desastre en el sistema informático de una compañía. Como objetivos específicos se planteó la creación de una guía para crear un plan de mantenimiento que le otorgue vigencia al plan maestro y un plan de simulacros que permita comprobar la efectividad del plan de recuperación.

En general, se recomendó tomar en cuenta los siguientes aspectos a la hora de formular el plan de recuperación:

- Determinar el alcance del proyecto, identificando qué es crítico para la organización desde un punto de vista funcional u operativo.
- Determinar la rapidez con la que se requiere recuperar la operación o parte de ésta.
- Determinar el impacto de no tener disponible un sistema o proceso por medio de un análisis de categorías de criticidad.
- Desarrollar los procedimientos de recuperación con base en las conclusiones de los pasos anteriores.
- Probar que los procedimientos de recuperación funcionan por medio de planes concretos de simulación de desastre, en los cuales se involucre al 100% de los miembros de la organización. En este punto se hizo énfasis en la creación de un laboratorio que permita probar unitaria e integralmente cada módulo del sistema.
- Desarrollar un plan de mantenimiento para los procedimientos desarrollados de manera que el plan esté siempre vigente por medio de la aplicación del proceso de administración de cambios.

Se considera que los objetivos planteados fueron exitosamente alcanzados ya que en el futuro, un gerente de proyectos que tenga a cargo desarrollar e implementar un plan de recuperación en caso de desastre para un sistema SAP ERP, puede seguir estos pasos y con muy pocas adaptaciones podrá asegurar la continuidad del negocio, brindando una alta disponibilidad de los sistemas que soportan el día a día de la organización patrocinadora del proyecto.

Recomendaciones

- Se requiere del apoyo y soporte de la alta gerencia, quienes deben participar como patrocinadores del proyecto tomando decisiones de forma proactiva.
- Es necesaria una participación activa de toda la organización, ya sea como parte del equipo del proyecto o como ejecutores del procedimiento en caso de desastre.

- No se debe perder de vista la operación diaria de la organización. Este tipo de proyectos absorben mucho tiempo y recursos, por lo que se debe analizar la necesidad de nuevas contrataciones de personal de manera que el proyecto no afecte el día a día de la organización.
- En la medida de lo posible, se recomienda utilizar como sitio alterno, una empresa con experiencia que se dedique a brindar este tipo de servicios.
- El sitio alterno escogido debe estar localizado geográficamente lejos del sitio normal de operación.
- Las aplicaciones, sistemas y datos deben estar instalados en el sitio alterno, de manera que el plan se concentre en el levantamiento y validación de los sistemas. Esto evita el costo de tener que instalar todo desde cero en caso de desastre y facilita el mantenimiento del sitio alterno.
- Es importante determinar el tiempo mínimo que la operación puede estar fuera de servicio en caso de desastre y la cantidad máxima de datos que podría estar dispuesta a perder. A partir de esta información se deben desarrollar los procedimientos de recuperación.
- Finalmente, se debe tener muy claro, cuáles son los eventos o circunstancias que implican declarar la organización en desastre. En otras palabras, tener claro cuál es el disparador del plan de recuperación por desastre.

7. BIBLIOGRAFÍA

Internet

- (Jon William Toigo) http://www.disaster-resource.com/articles/wwtoigo.shtml
- www.sap.com
- http://es.scribd.com/doc/46054639/Manual-Tecnico-ITIL-v3-EN-ESPANOL
- www.sei.cmu.edu/CMMI
- (Disaster Recovery Planning Process) http://www.drj.com/new2dr/w2_002.htm
- www.ibm.cl
- http://www.resiliencia.cl/

Libros

- P.M.I (Project Management Institute), Guía de los Fundamentos de la Dirección de Proyectos, PMBOK Guide.
- Toigo, Jon William. Disaster Recovery Planning: Managing Risk and Catastrophe in IS. Yourdon Press, Prentice-Hall, Inc.
- Disaster Recovery Planning, Roopendra Jeet. Sandhu
- Disaster Recovery, Brenda Phillips
- Disaster Recovery Planning: Getting to Business-Savvy Business Continuity, Jon William Toigo

8. GLOSARIO

RED SAN

Una red de área de almacenamiento, en inglés SAN (Storage Area Network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Una red SAN es utilizada para transportar datos entre servidores y recursos de almacenamiento. La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor. (http://www.mundocisco.com).

RED LAN

LAN significa Red de área local. Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología (la más utilizada es Ethernet).

Una red de área local es una red en su versión más simple. La velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps (por ejemplo, en una red Ethernet) y 1 Gbps (por ejemplo, en FDDI o Gigabit Ethernet). Una red de área local puede contener 100, o incluso 1000, usuarios. (http://www.mundocisco.com).

TCP/IP

Son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés *Transmission Control Protocol/Internet Protocol*), un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

Servidor BLADE

Blade Server es una arquitectura que ha conseguido integrar en tarjetas todos los elementos típicos de un servidor. Éstas tarjetas (blades) se insertan en el backplane dentro de un chasis que a su vez integra y permite compartir los elementos comunes como son la ventilación, los switches de red, la alimentación, etc. Reduciendo el consumo eléctrico, cables, sistemas de enfriamiento, etc.

Una tarjeta Blade es un servidor completo. La memoria RAM, el disco duro, la CPU, están contenidos en el "Blade", éstas son instaladas mediante la simple inserción. Las bandejas pueden ponerse cuando se quiera y quitarse de igual manera, no sufriendo el servidor modificación alguna y permaneciendo siempre a pleno rendimiento. (www.ibm.com).

InfiniBand

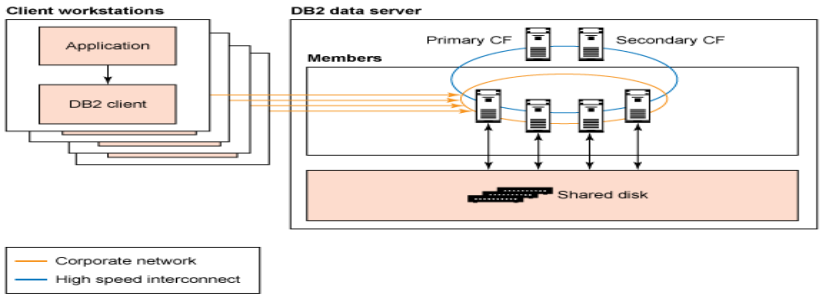
InfiniBand es un bus de comunicaciones serie de alta velocidad, diseñado tanto para conexiones internas como externas. Sus especificaciones son desarrolladas y mantenidas por la Infiniband Trade Association (IBTA). (www.ibm.com).

DB2 pureScale

El dispositivo DB2(R) pureScale(TM) ayuda a reducir el riesgo y costo del crecimiento empresarial proporcionando una capacidad casi ilimitada, una disponibilidad continua y transparencia de las aplicaciones. DB2 pureScale se beneficia de una interconexión de baja latencia, tal como InfiniBand, y está construido sobre la arquitectura de un disco compartido. Para lograr la baja latencia, se utiliza Power Systems InfiniBand Host Channel Adapters (HCA) y los

interruptores, y un canal de fibra SAN proporciona el acceso a los discos compartidos. (www.ibm.com).

Figura 1. Una vista de los principales componentes en un entorno de DB2 pureScale



Data center (centro de cómputos, centro de proceso de datos)

Es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento. Generalmente incluye fuentes de alimentación redundantes o de respaldo, conexiones redundantes de comunicaciones, controles de ambiente (por ejemplo, aire acondicionado) y otros dispositivos de seguridad.

Sitio del tipo Tier 3+

El concepto de Tier se refiere a un estándar internacional (TIA-942) que indica los grados de disponibilidad con los que pueden clasificarse los centros de datos. Estos Tiers están basados en información desarrollada por el Uptime Institute, un consorcio internacional dedicado a proveer a sus miembros las mejores prácticas en la planificación y administración de data centers.
Infraestructura, seguridad, sistemas eléctricos, mecánica y telecomunicaciones son algunos de los elementos que evalúa este estándar.

A mayor número de Tier, mayor grado de disponibilidad. Por ejemplo, tener nivel Tier 3, significa que el data center, puede realizar cualquier actividad planeada sobre un componente de la infraestructura, sin interrupciones, como por ejemplo: Mantenimiento preventivo, reparaciones o reemplazo de componentes, agregar o eliminar componentes y realizar pruebas de sistemas, entre otros.

Debe existir suficiente capacidad y doble línea de distribución de los componentes. Así, es posible realizar mantenimiento o pruebas en una línea, mientras que la otra atiende la totalidad de la carga. La tasa de disponibilidad de un Tier 3 es de 99.982%.

NFS (**Network File System)**

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.

General Parallel File System (GPFS)

Es un sistema de ficheros distribuido de alto rendimiento desarrollado por IBM. GPFS proporciona un acceso concurrente de alta velocidad a aplicaciones que se encuentran ejecutando en múltiples nodos de un cluster dando una visión de un disco compartido entre todos ellos. La configuración existente de mayor tamaño superaba los 2000 nodos.