UNIVERSIDAD PARA LA COOPERACIÓN INTERNACIONAL

(UCI)

GUÍA PARA CREAR UN PLAN DE RECUPERACIÓN EN CASO DE DESASTRE EN EL SISTEMA INFORMÁTICO DEL CENTRO DE DATOS DE UN GRUPO FINANCIERO

JORGE SALAZAR VILLALOBOS

PROYECTO FINAL DE GRADUACIÓN PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR POR EL TÍTULO DE MASTER EN ADMINISTRACIÓN DE PROYECTOS

San José, Costa Rica

Enero – 2008

UNIVERSIDAD PARA LA COOPERACIÓN INTERNACIONAL

(UCI)

Este proyecto Final de Graduación fue aprobado por la Universidad como
Requisito parcial para optar por el grado de Máster en
Administración de Proyectos

___Ing. Alejandro Rubinstein N., MBA.____

PROFESOR TUTOR

_____

LECTOR No.1

_____

LECTOR No.2

_____Jorge Salazar Villalobos_____

SUSTENTANTE

DEDICATORIA

A Dios, por darme tantas bendiciones en la vida, incluyendo la oportunidad de instruirme, permitiéndome ser un ser humano cada día mejor.

A mi esposa Karla y a mis hijos José Mario y Fabiola, 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 y hermanas por construir las bases que hoy me permiten afrontar y disfrutar los retos que se presentan en mi camino.

AGRADECIMIENTOS

A la organización Electronic Data Systems (EDS) por la oportunidad de crecimiento profesional y el apoyo incondicional que me brindaron por más de siete años (2001-2008).

A la Universidad para la Cooperación Internacional (UCI), incluyendo a todos sus profesores, por compartir con nosotros los estudiantes, sus experiencias y conocimientos, permitiéndonos ser mejores profesionales y mejores personas.

INDICE

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

LISTADO DE ABREVIATURAS

AR.....Análisis de Riesgos

BCP.....Siglas en inglés de Plan de Continuidad del Negocio (Business Continuity Planning)

BIA.....Siglas en inglés del término Análisis de Impacto del Negocio (Bussiness Impact Analysis)

BRP.....Siglas en inglés de Plan de Recuperación del Negocio (Business Recovery Planning)

CCTA.....Siglas en inglés de la Agencia Central de Computadores y Telecomunicaciones (Central Computer and Telecommunications Agency)

CI.....Siglas en inglés del término Elemento de la Configuración (Configuration Item)

CMMI.....Siglas en inglés de la metodología Integración de Modelos de Madurez (Capability Matuirity Model Integration)

DRP.....Siglas en inglés de Plan de Administración de Desastres (Disaster Recovery Plan)

EDS.....Siglas en inglés de la compañía Sistemas de Datos Electrónicos (Electronic Data Systems)

FCE.....Factores Críticos de Éxito

GB.....Giga Bytes (cantidad de datos que corresponde a 1024 Mega Bytes)

ITIL.....Siglas en inglés de Librería de Infraestructura de Tecnología de la Información (Information Technology Infrastructure Library)

JRR.....Junta Revisora de Riesgos

MTD.....Siglas en inglés del término máximo tiempo de caída tolerable (Maximal Time Down)

PMI.....Siglas en inglés del Instituto de Administración de Proyectos (Project Management Institute)

PMO.....Siglas en inglés de la Oficina de Administración de Proyectos (Project Management Office)

PMR.....Plan de Manejo de Riesgos

RPO.....Siglas en inglés del término objetivo de punto de recuperación (Recovery Point Objective)

RTO.....Siglas en inglés del término objetivo de tiempo de recuperación (Recovery Time Objective)

SLA.....Siglas en inglés del término Acuerdos de Niveles de Servicio (Service Level Agreements)

SUGEF.....Superintendencia General Financiera

RESUMEN EJECUTIVO

El término desastre, de acuerdo a Toigo (1989), 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 planeación 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. (Hiatt, 2000)

El negocio del procesamiento de tarjetas de crédito, mueve diariamente una cantidad de dinero tal, que requiere una alta disponibilidad (entre 99% y 100%) de los sistemas informáticos que soportan este procesamiento. Dada la competencia que se desarrolla en el mercado de las tarjetas de crédito, un fallo en los sistemas de información, que impida completar las transacciones que ingresan a estos sistemas, puede significar pérdidas importantes, tanto monetarias como en la imagen de las compañías emisoras de tarjetas. Por lo anterior, es de gran valor para las compañias procesadoras de tarjetas de crédito, 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 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 tarjeta de crédito ubicado en el centro de datos de un grupo financiero, 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.

La metodología que se utilizó para satisfacer los objetivos antes mencionados consistió en una mezcla de teorías, a saber, la de administración profesional de proyectos que recomienda el PMI *(Project Management Institute),* la cual se utilizó para desarrollar el plan de recuperación por desastre (DRP) y el marco de trabajo que provee ITIL (*Information Technology Infrastructure Library*) el cual se utilizó como soporte, tanto para crear el plan de mantenimiento del DRP como para desarrollar el plan de simulación o validación del DRP, el cual pretende comprobar que el DRP planeado funciona. Como proceso de administración de riesgos, se utilizó la metodología ABCD, creada por la organización EDS, líder mundial de "outsourcing".

Para desarrollar el DRP, se propuso identificar las áreas más sensibles de la organización, posteriormente identificar el equipo y aplicaciones que soportan estas áreas haciendo un análisis de criticidad al ejecutar un análisis de impacto BIA (*bussiness impact analysis*). También se propuso crear un laboratorio el cual funcionará como la base para probar que todos los pasos del plan funcionan. En este laboratorio se instalarán todas las aplicaciones y funciones que son parte del plan de recuperación por desastre. También se propuso diseñar un proceso de respaldos de información que en caso de desastre se puedan restaurar en el sitio alterno y a partir de este punto se inicie el proceso de recuperación.

Para desarrollar estos planes se sugirió utilizar principalmente cuestionarios a los expertos, lluvias de ideas y reuniones con los expertos de cada área. Con esto se pretende obtener la base para los análisis que mostrarán las áreas más sensibles de la organización.

A lo largo del proyecto se determinó que el apoyo y soporte de las gerencias y niveles superiores de la organización en general, es vital para el éxito de un proyecto de este tipo. Se destacó la importancia de definir el alcance del proyecto, esto significa que se debe determinar los activos que tiene sentido recuperar con base en el análisis del tiempo mínimo que está dispuesta la organización a no tener disponible un servicio, proceso, sistema o activo en general.

Se encontró que se debe cuantificar el impacto que provoca la pérdida de un servicio o activo en una escala de tiempo, ya que esto determina las características y costo del proceso de recuperación a implementar. Finalmente se hizo hincapié en la necesidad de tener planes de mantenimiento y planes de prueba que garanticen la vigencia y calidad de los procedimientos definidos para recuperar la organización en caso de declarar un desastre en las operaciones de la misma.

1-INTRODUCCIÓN

Un desastre dentro de una 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 organizaciones no sobreviven 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.

La mayoría de personas practican diariamente la acción de evitar, transferir o mitigar un riesgo. Por ejemplo, tome el carro que usted maneja, éste tiene una llanta de repuesto y una herramienta para levantar el carro ("gata", como se conoce en muchas partes) para mitigar el costo y la cantidad de tiempo perdido en caso de que requiera cambiar una llanta durante el camino. En lugar de llamar una grúa, usted mismo puede cambiar la llanta afectada y buscar un centro de servicio para repararla. Si usted no pensara en que existe la posibilidad de que se le estalle una llanta, probablemente no cargaría una llanta de repuesto ni "la gata" aprovechando mejor el espacio que estos objetos ocupan en su automóvil. Por lo tanto, usted piensa que no puede evitar una llanta estallada o desinflada, sin embargo ha encontrado una forma de reducir el impacto de este inconveniente.

En el ambiente y jerga de recuperación por desastre, se manejan algunos conceptos que en primera instancia parecieran significar lo mismo, sin embargo, cada área tiene sus características particulares. Básicamente, existen tres grandes áreas en las que se ubica la estrategia de una organización para administrar el riesgo inherente a su operación diaria, estas son:

Plan de Recuperación en caso de Desastre, DRP por sus siglas en inglés (*Disaster Recovery Planning*). Consiste básicamente en las acciones para recuperarse en caso de que se presente un desastre. **Plan de Recuperación del Negocio**, BRP por sus siglas en inglés (*Business Recovery Planning*), ésta área va un paso más adelante del DRP, ya que además del procesamiento de datos, enfoca sus esfuerzos en recuperar el resto de las operaciones de la compañía y finalmente el concepto de **Plan para continuidad del negocio**, BCP por sus siglas en inglés (*Business Continuity Planning*), este tipo de planes le permiten al negocio, aunque sea de forma reducida, funcionar durante e inmediatamente después de declarada la emergencia. (Hiatt, 2000)

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 de una compañía procesadora de tarjetas de crédito, de manera que los procesos se puedan habilitar en un sitio alterno y la procesadora continúe su operación normal desde otro lugar mientras se recupera el sitio original.

Por lo tanto el trabajo a realizar en este proyecto tiene un enfoque para ser aplicado en una procesadora de tarjeta de crédito, organización que tiene centralizada la operación diaria de tarjeta de crédito de una o más instituciones financieras. Esto significa, en términos generales, que todas las gestiones, sistemas y procesos relacionados con una tarjeta de crédito de un Banco procesado, son ejecutadas por medio de los sistemas de información de la procesadora.

Las tarjetas de crédito funcionan en un ambiente globalizado, es decir, una tarjeta emitida en Costa Rica puede funcionar como medio de pago en cualquier comercio del mundo que esté afiliado a la misma marca de la tarjeta (VISA, Master Card, American Express, etc.). En el procesamiento de tarjetas de crédito, entran en juego muchas organizaciones, las cuales cobran una comisión por cada

transacción que pase por sus sistemas, es decir, sobre todas las transacciones enviadas y recibidas por cada ente involucrado, tales como las operadoras de tarjeta de crédito, las compañías emisoras, las compañías adquirentes de comercios, las marcas de tarjeta como VISA, se cobra una comisión que multiplicada por cientos de transacciones diarias representan miles de dólares cada día. Por lo anterior, la disponibilidad de los sistemas de información que soportan todas estas transacciones y la necesidad de asegurar la continuidad de este negocio se convierten en un asunto de vital importancia para las organizaciones relacionadas con el proceso.

Solo en Costa Rica se emiten anualmente alrededor de 300,000 tarjetas de crédito VISA, las cuales se distribuyen entre 21 emisores de tarjeta autorizados por la SUGEF. (Visa OnLine, 2007). Esto significa que hay una fuerte competencia entre las compañías de tarjeta de crédito, lo que genera un mercado cada vez más exigente que está siempre en busca de mejores tasas de interés, promociones, facilidades de pago, valor agregado y todo lo que involucra eficiencia en el servicio.

El servicio más elemental que puede esperar un usuario de tarjeta de crédito que se encuentre al día en sus pagos, es que al utilizar su tarjeta en un comercio como medio de pago, ésta le funcione sin problemas y le permita realizar el pago en pocos segundos de forma que simule lo mejor posible la utilización de dinero en efectivo al realizar el pago. Si la expectativa al realizar el trámite descrito anteriormente se incumple, parcial o totalmente, habrá un impacto negativo directo en el usuario con respecto a la imagen del emisor de la tarjeta, llegando incluso a cambiar de emisor o a cancelar el servicio. Indirectamente, también habrá un impacto similar, del emisor hacia la compañía que le procesa o administra su sistema de tarjeta de crédito, es decir, una interrupción del sistema de tarjeta de crédito va a generar una cantidad importante de incidentes o reportes de mal servicio y por ende todos los involucrados se verán impactados.

Es por esta razón que la alta disponibilidad de un sistema de tarjeta de crédito 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 en caso de desastre, haciendo que los incidentes en el sistema sean lo más transparentemente posibles al usuario.

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 para esta función en una empresa especializada y con reconocimiento mundial para este tipo de actividades. Estos últimos cuentan con todas las facilidades en equipo, infraestructura y seguridad, sin embargo, tienen 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.

Finalmente es importante mencionar que en una procesadora de tarjeta de crédito, el sistema informático es tan amplio y las aplicaciones alrededor de éste son tan numerosas que difícilmente se contemplen todas en una primera fase del proyecto. Esta investigación se concentrará en lo que se conoce como el “core” o núcleo del sistema, abarcando únicamente las áreas de base de datos, sistema de autorizaciones, sistemas de intercambio con las marcas VISA y Master Card y

procesos operativos diarios realizados por el centro de datos, tales como cierre de cajas, fines de día, generación de reportes, entre otros.

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

- Diseñar una guía que permita crear un procedimiento de recuperación ante desastre, natural o inducido, para el sistema informático de tarjeta de crédito ubicado en el centro de datos de un grupo financiero, 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.

También se tienen los siguientes objetivos específicos:

- 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.

2- MARCO TEÓRICO

El término desastre, de acuerdo a Toigo (1989), significa la interrupción del negocio debido a la pérdida o incapacidad de acceso a los activos que contienen la información requeridos para la operación normal. 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 los datos. La pérdida de datos puede presentarse debido a borrados accidentales o intencionales o por la destrucción de los medios de almacenamiento. Esta pérdida puede ser causada por fenómenos naturales o inducida por el factor humano.

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, 2004).

Una crisis o desastre puede categorizarse en tres niveles de acuerdo a su nivel de riesgo. (Hiatt, 2000):

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.

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. (Toigo 1989):

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

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

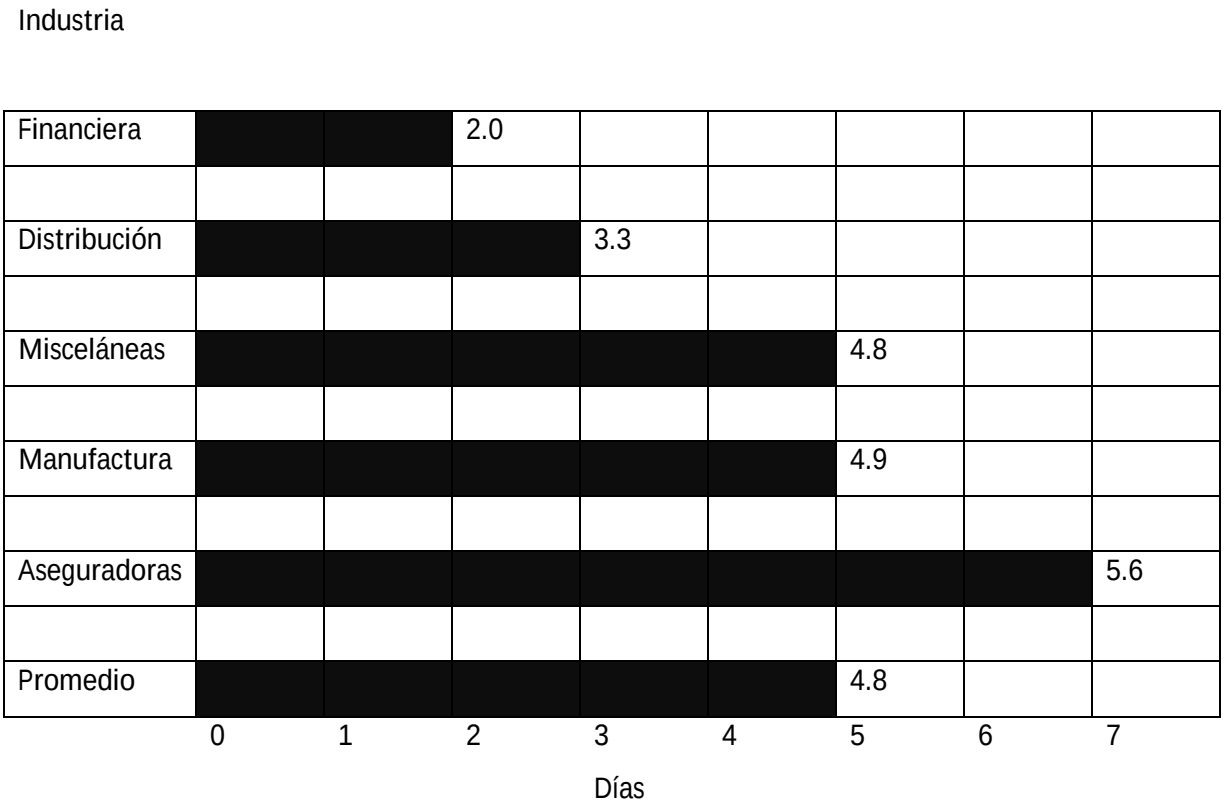
INTERNAS: Sabotaje, robo, violencia de empleados o ex empleados, etc.

CONFLICTO ARMADO: Terrorismo, secuestro, etc.

Para mitigar el efecto o impacto de un riesgo, el cual representa una amenaza para la organización, las compañías desarrollan planes de contingencia que son en pocas palabras respuestas para superar o mitigar el impacto de situaciones inesperadas (Toigo, 1989).

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 Cuadro 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. (Hiatt, 2000)

Cuadro 1. Máximo tiempo permitido para estar sin sistema por tipo de industria. (Hiatt, 2000)



Aunque el estudio de la Universidad de Minnesota tiene más de 20 años, muchos expertos consideran que su grado de exactitud aún se mantiene. (Hiatt, 2000)

Otro estudio de la Universidad de Wisconsin señala que el desastre más importante en una compañía financiera consiste en una interrupción en los sistemas de comunicaciones. En la primera hora, el 80% de las instituciones financieras calculan pérdidas a razón de $1000 por hora, un 10% de los encuestados indican pérdidas de más de $100,000 por hora. (Hiatt, 2000)

Un 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. (Hiatt, 2000)

El siguiente cuadro documenta algunas estadísticas con respecto al impacto de que han causado algunos desastres en las distintas compañías. (Robertson, 1997)

Cuadro 2. Estadísticas con respecto a desastres (Robertson, 1997)

El gasto en recuperación por desastres en 1995 fue de aproximadamente $3.1 billones y se estimó que crecería anualmente un 20%.
Los “apagones” contabilizaron el 28% de los desastres en sistemas informáticos entre 1982 y 1985, seguido de tormentas 11.7%, inundaciones 9.6%, errores en hardware 7.7%, bombas 7.2%, huracanes 6.3%, incendios 5.6%, errores en software 5.4%, terremotos 4.9%
Cada desastre tardó en promedio 4 horas para recuperarse y produjo en promedio pérdidas por $329,000
El sector financiero tuvo la mayor cantidad de compañías con planes de recuperación, cerca del 70%, versus un 50% de las compañías de bienes para consumo y un 43% de las compañías de seguros.
En promedio cada hora fuera le costó a las empresas $78,000
El 60% de las compañías afectadas por un desastre, salieron del mercado en los siguientes dos años

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)

En el ambiente y jerga de recuperación por desastre, se manejan algunos conceptos que en primera instancia parecieran significar lo mismo, sin embargo, cada área tiene sus características particulares. Básicamente, existen tres grandes áreas en las que se ubica la estrategia de una organización para administrar el riesgo inherente a su operación diaria (Hiatt, 2000), estas son:

- **Plan de Recuperación en caso de Desastre**, DRP por sus siglas en inglés (*Disaster Recovery Planning*). Consiste básicamente en las acciones para recuperarse en caso de que se presente un desastre. Incluye la planeación de pasos para evitar riesgos, mitigarlos o transferirlos a alguien más por medio de seguros. 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.
- **Plan de Recuperación del Negocio,** BRP por sus siglas en inglés (*Business Recovery Planning*), ésta área va un paso más adelante del DRP, ya que además del procesamiento de datos, enfoca sus esfuerzos en recuperar el resto de las operaciones de la compañía, incluyendo todo lo relacionado a relaciones con el cliente y proveedores, de manera que la recuperación del problema de se de en forma integral.
- **Plan para continuidad del negocio,** BCP por sus siglas en inglés (*Business Continuity Planning*), este tipo de planes le permiten al negocio, aunque sea de forma reducida, funcionar durante e inmediatamente después de declarada la emergencia.

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 (Hiatt, 2000):

- Le permiten a la organización evitar ciertos riesgos o mitigar el impacto de éstos al:
    - Minimizar potenciales pérdidas económicas
    - Decrementar 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 Riesgos (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 (Wold y Shriver, 1997):

- 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. (Toigo, 1989).

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 (AR) y un análisis BIA son (Hiatt, 2000):

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 IDENTIFICACIÓN Y PRIORIZACIÓN DE LAS FUNCIONES OPERACIONALES

En el contexto del procesamiento de datos, las aplicaciones pueden clasificarse usando el siguiente espectro de tolerancia (Toigo,1989):

- **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 y 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.

2.2.3 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, es identificar qué amenazas existen a las actividades de procesamiento normal del negocio. El mejor método para identificar las amenazas es buscar el fenómeno, independientemente del origen, que típicamente causaría una pérdida de la funcionalidad normal del sistema. (Toigo, 1989). La Figura 1 refleja el resultado de un estudio realizado por Contingency Planning Research que investigó las principales causas que provocaron caídas del sistema de cómputo. (Schreider, 1998).

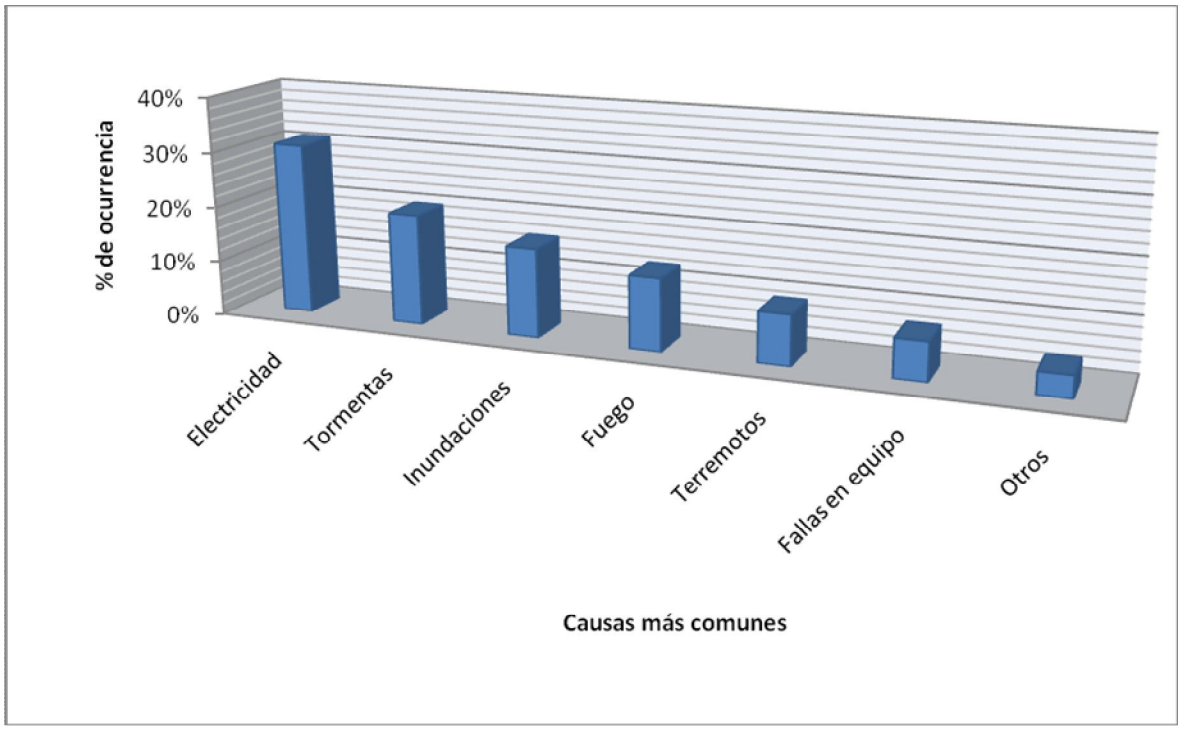


Figura 1. Incidentes que causaron caídas del sistema de cómputo por más de 12 horas. (Schreider, 1998).

La razón más común para que los datos de una compañía no puedan ser recuperados es debido a fallas al salvar la información en una copia de respaldo. Como muestra el Cuadro 3, los errores humanos causan el daño más grande. (Hiatt, 2000).

Cuadro 3, principales motivos por los que no se puede recuperar información (Hiatt, 2000).

Causas	Porcentaje
Errores humanos no intencionales	50-80%
Empleados deshonestos	10-17%
Desastres naturales	10-15%
Sabotaje de empleados	3-4%
Agua	2-3%
Personas ajenas a la compañía	1-3%

Otros puntos a considerar cuando se determina la probabilidad de un desastre específico son. (Wold, 1996):

- Localización geográfica
- Topografía del área
- Proximidad a fuentes de poder, fuentes de agua o aeropuertos
- Grado de accesibilidad a la organización.
- Historial de interrupciones
- Historial del área a las amenazas naturales

2.2.4 IDENTIFICACIÓN DE LOS MEDIOS DE ALMACENAMIENTO DE DATOS Y LOS SITIOS DE RECUPERACIÓN

Una 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 (Wallace y Webber, 2004):

- 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
- Protección en caso de falla en el equipo
- 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 las 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 continua. 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 (Wallace y Webber, 2004):

- 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 cuando un plan debe ser actualizado (Weil, 2004):

- 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 (Weil, 2004):

- Se logra demostrar que el plan funciona
- Se identifican planes de contingencias que hasta ese momento eran desconocidos
- Se verifica la disponibilidad de recursos
- Se determina la duración verdadera del tiempo de recuperación
- Sirve para entrenar al personal asignado a roles de recuperación
- Hace que el personal se identifique mejor con el plan de recuperación.
- Se determinan las mejoras necesarias y debilidades del plan.

Los pasos para construir el plan son los siguientes (Weil, 2004):

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. Planeación 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 (Wallace y Webber, 2004).

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 DEL 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 (2004) 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 (2004), 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 administración de costos debido a la gran inversión económica que representa un plan de esta magnitud, la etapa de planificación, como principal área de conocimiento aplicada en este tipo de proyectos, ya que brinda el sentido de proactividad 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 RIESGOS, PMI / EDS

Riesgo

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 2. (Infocentre, 2007)

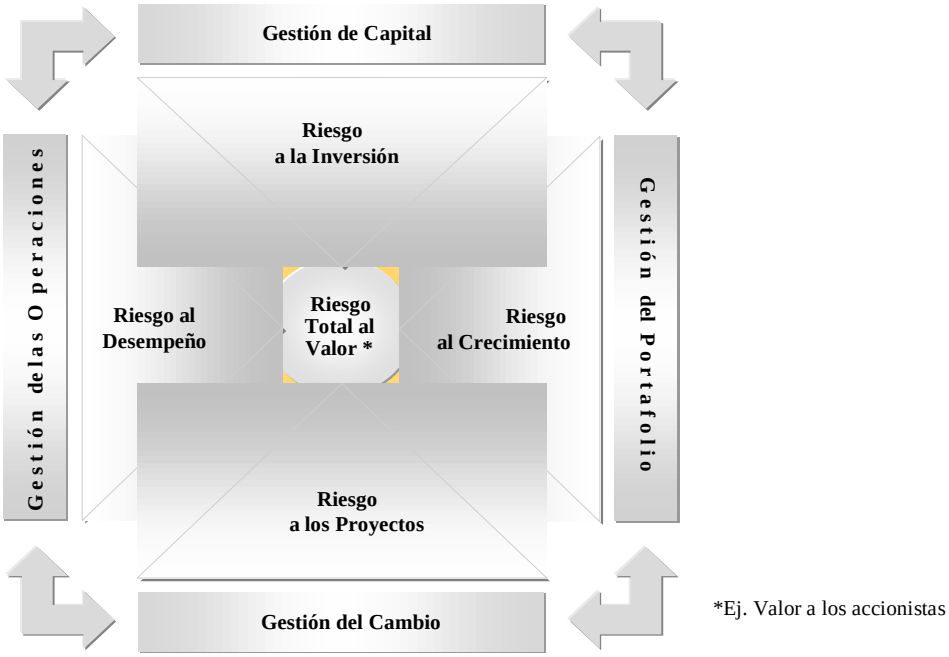


Figura 2. Multi-Dimensionalidad del Riesgo, (Infocentre, 2007)

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 taxonomía de EDS contiene, entre otros, 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 ” (Infocentre, 2007)

La metodología ABCD de EDS complementa esta definición. La Figura 3 muestra los elementos que componen el proceso de administración de riesgos.

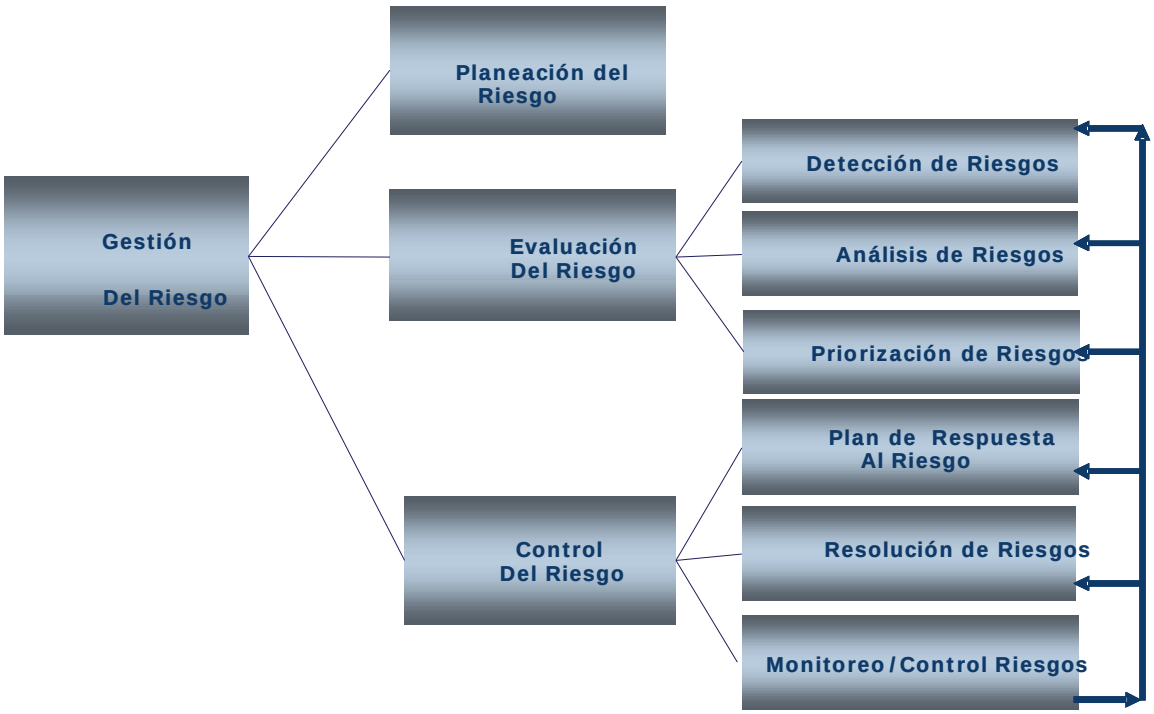


Figura 3. Proceso de Administración de Riesgos, (Infocentre, 2007)

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, pequeña 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 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 planeación. Cada elemento importante que surge al planear una serie de futuros eventos pueden ser capturados 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 (planeamiento). 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 planeación 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

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.

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*" (asuntos pendientes de resolver), 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 planeación, ya sea al inicio o si se requiere re-planear en algún punto del ciclo de vida del proyecto, también surgen 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 escalación

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 ROJO, AMARILLO y VERDE. 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 el Cuadro 4:

Cuadro 4. Clasificaciones por criticidad, (Infocentre, 2007)

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

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 a resolverse en 5 días es más importante que un "*issue*" AMARILLO con una resolución en 2 semanas.

Cerrando los "issues"

Los *issues* se cierran al:

- Obtener una respuesta satisfactoria, o
- Un evento (ej. Un cambio en la política) que resuelve o elimina el "issue", o
- 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 objetivo 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”. 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 de seguimiento al estatus de los supuestos o buscando nuevos supuestos.

Los supuestos pueden ser explícitos y se registran en muchas áreas, 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 de 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 de el 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 4.

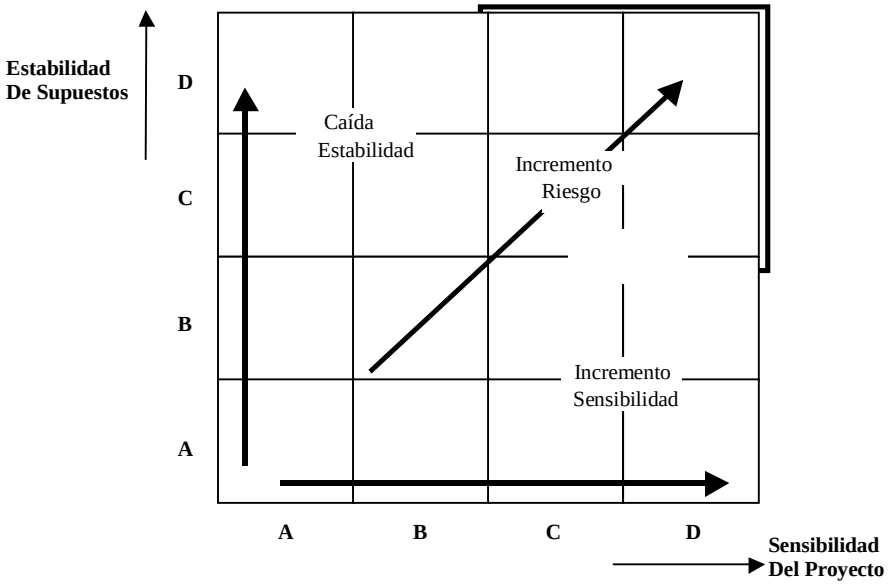


Figura 4. Diagrama de Sensibilidad/Estabilidad (Infocentre, 2007)

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 verdaderos o falsos, si son verdaderos se convierten en hechos. En el caso de los supuestos 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
- Controlabilidad
- 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

Controlabilidad

La controlabilidad es una métrica de **confianza** de que el riesgo será administrado. La clasificación de controlabilidad 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. Es un número entre 0 y 1, usualmente expresado en forma de porcentaje.

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 re-evaluada.

La probabilidad es utilizada en el cálculo de la Exposición al Riesgo (o riesgo factorado).

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 Enero 12, 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 en Diciembre 1 (seis semanas antes de la necesidad), y la aprobación debe estar para Noviembre 18"

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 la controlabilidad. 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 debe 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 muestra 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

Donde 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 para 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. Como mínimo se debe calcular el costo de esos planes de contingencia.

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 Riesgos

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 relativamente 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.

La controlabilidad está representada 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, esto 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. El gráfico es solo una foto de las clasificaciones ya que estas se mueven en el tiempo y no da detalle de los riesgos.

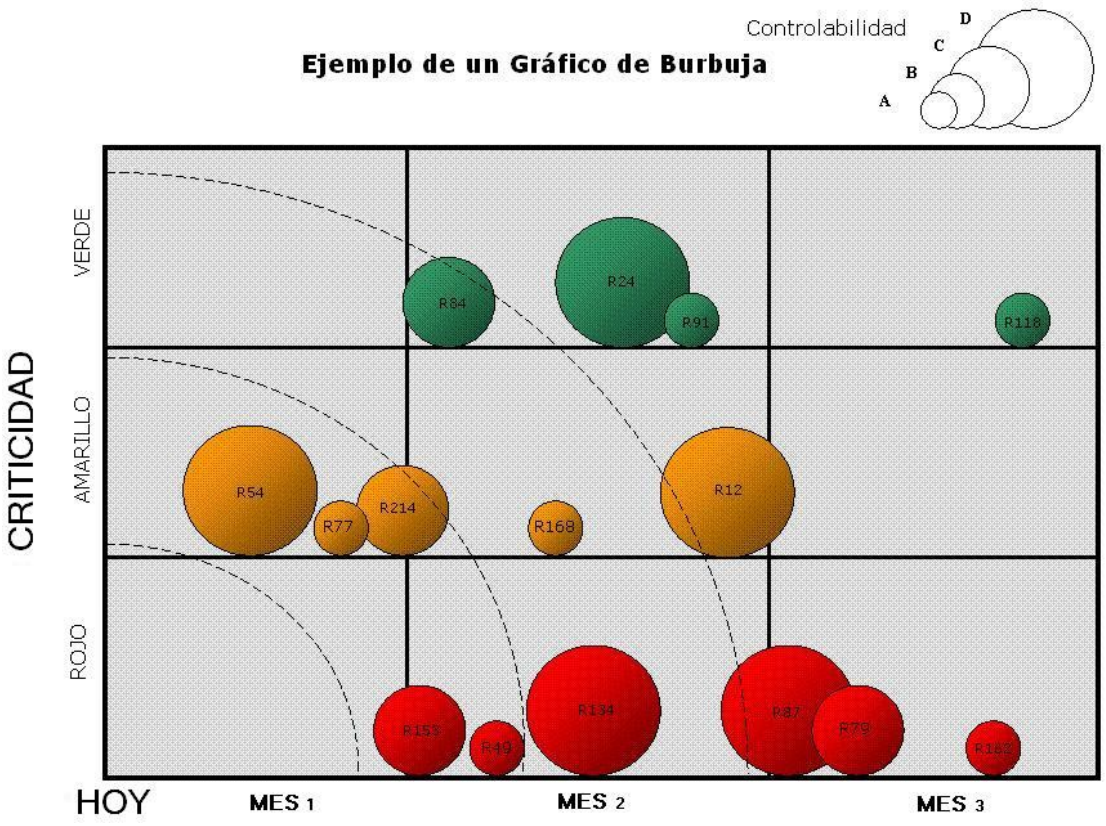


Figura 5. Diagrama de burbuja con tamaño de burbuja = Controlabilidad (Infocentre, 2007)

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)
- La controlabilidad (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 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 Riesgos

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, des-sensibilizar el riesgo al re-diseñar o re-planear.

Esas opciones están resumidas en la Figura 6.

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

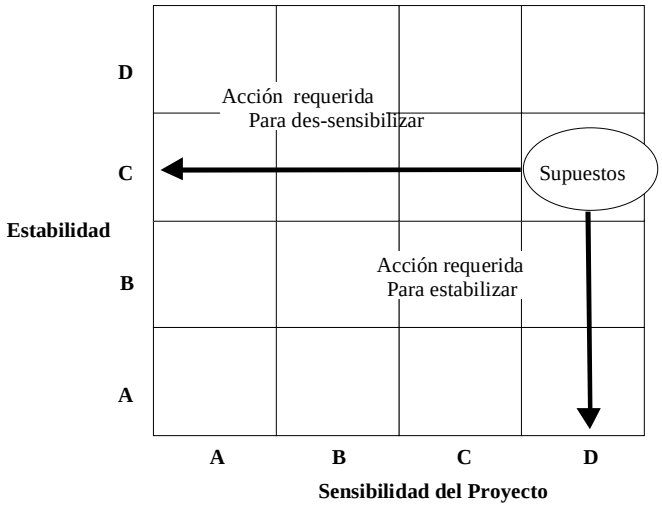


Figura 6. Objetivos básicos de las acciones reductoras de riesgo (Infocentre, 2007)

Enfoques estratégicos – “Manejadores”

Para ayudar a encontrar estrategias que mitiguen los riesgos de un portafolio de riesgos grande, por ejemplo, excesos del riesgo #25, 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.

A manera de ejemplo, el gráfico de Manejadores de Riesgo del Cuadro 5 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.

Cuadro 5. Gráfico de Manejadores de Riesgo (Infocentre, 2007)

	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**

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 a el 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 des-sensibilizar 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.
- Re-calendarizar módulos y actividades
- Re-estructurar la estructura de trabajo.
- Re-acomodo 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” 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.
- 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 “senior” de la organización.

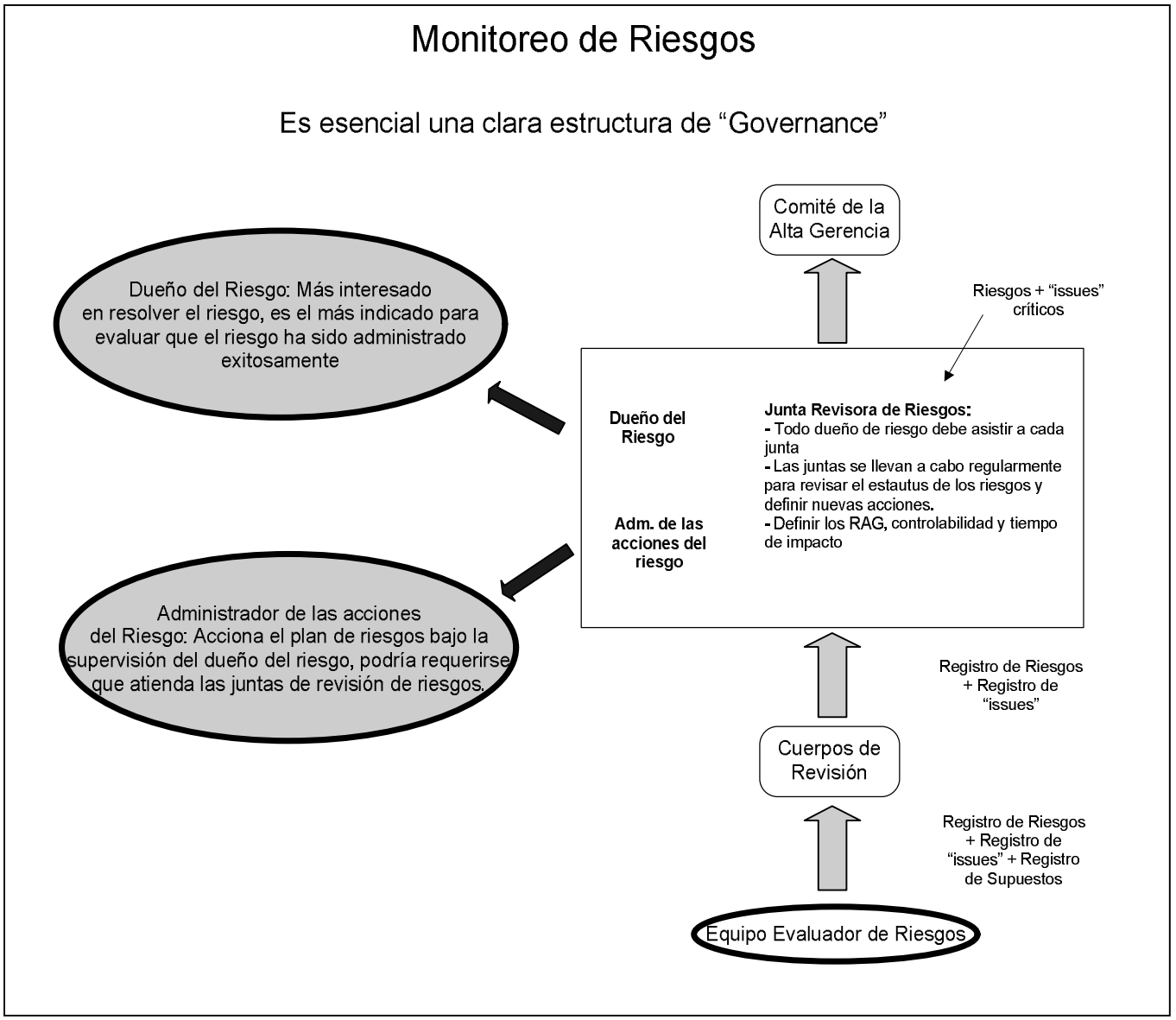


Figura 7. Junta de Revisión de Riesgos (JRR) (Infocentre, 2007)

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 controlabilidad
- 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 (ITIL)

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 (Bajada, 2007):

- 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 “senior” 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 Cambios (SkillSoft, 2007)

- **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 (ITIL)

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 (SkillSoft, 2007):

- 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 o 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 planeación financiera.

3 - MARCO METODOLÓGICO

Con respecto a la metodología empleada en este proyecto, la investigación inicia como Exploratoria y termina como Descriptiva con un enfoque Cualitativo.

Inicia como Exploratoria, dado que el tema es relativamente desconocido y la bibliografía existente es escasa, principalmente si lo que se busca son investigaciones y bibliografía relacionada directamente con centros de cómputo de alta disponibilidad. Por lo tanto, 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.

Finaliza como descriptiva, ya que una vez revisados los libros relacionados con la recuperación de sistemas en caso de desastre, en los que se validaron los principios de este tema y las recomendaciones sobre temas como las comunicaciones y análisis de riesgos, se procede a describir los aspectos que deben tomarse en cuenta al crear un plan de recuperación por desastre, es decir a crear una guía, fundamentada en la teoría encontrada, aplicada de acuerdo a la información extraída de las entrevistas a los expertos de cada área del departamento de Tecnología de una empresa procesadora de tarjetas de crédito.

La investigación tiene un enfoque cualitativo dado que se proporciona una gran cantidad de información valiosa pero posee un limitado grado de precisión, es decir, la guía sugerida nace del análisis subjetivo de la teoría encontrada por parte del autor de este trabajo con respecto a la información recopilada en las entrevistas a los expertos de la compañía procesadora de tarjeta de crédito, contribuyendo a identificar los factores importantes que deben ser tomados en cuenta en la formulación de un plan de recuperación en caso de desastre.

Los instrumentos a utilizar son los siguientes:

- Entrevistas a los expertos de cada área de la organización.
- Inventarios de hardware y software existente en la organización.
- Observación de los procesos seguidos en el Centro de Datos de una procesadora de tarjeta de crédito.

La metodología se aplicacará 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: un análisis 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 y provea 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 (Burtles, 2007):

- *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 por sus siglas en inglés). Es el tiempo transcurrido desde que el desastre ocurre hasta que se recuperan los procesos impactados.

- *Objetivo de punto de recuperación* (RPO por sus siglas en inglés). Punto en el tiempo al cual los datos deben estar restaurados para reiniciar la operación. Es la base sobre la cual se desarrolla la estrategia de proyección de datos.

La información obtenida durante la fase de adquisición necesita ser cuidadosamente examinada y analizada para identificar procesos y sistemas críticos, interdependencias y tiempos meta 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:

Cuadro 6. Niveles de criticidad (Burtles, 2007)

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

El siguiente cuestionario también debe realizarse a los expertos para apoyar la definición de la criticidad de los sistemas de información de la compañía, contestando:

a. Significativamente, Moderadamente, Indirectamente, No del todo, Desconocido.

   - ¿En qué grado se requiere de X sistema de información para ejecutar las funciones esenciales de la organización?

- ¿En qué nivel apoya el sistema de información X al plan de continuidad del negocio?
- ¿En qué grado se vería afectada la función normal de la compañía si se pierde o degrada el funcionamiento del sistema de información X?
- ¿En qué grado afecta el sistema de información X a los clientes?
- ¿En qué grado afecta el sistema de información X a la conectividad interna o externa (intranet) ?
- ¿Los socios y aliados comerciales requieren la disponibilidad de este sistema de información?
- ¿Qué rol juega el sistema de información X como proveedor de medios para mantener el negocio?
- ¿En caso de pérdida del sistema de información X cómo se reduciría la capacidad para mantener el negocio?
- ¿En qué grado soporta la misión de otras entidades de negocio?

b. Indispensable, Apoyo, Indirectamente, No del todo, Desconocido

- ¿Qué papel juega el sistema de información X en cuanto al apoyo a las operaciones de negocio y capacidades de la organización como un todo?
- ¿Está el sistema de información X directamente asociado con una función de la compañía específicamente identificada en el plan financiero?

c. Internacionalmente, Nacionalmente, Regionalmente, Localmente, Desconocido

- ¿En qué escala afecta al negocio el sistema de información X?

d. SI, NO, Desconocido

- ¿Existe algún otro sistema similar al sistema de información X que pueda sustituirlo?
- ¿El sistema de información X protege datos financieros sensibles?
- ¿El sistema de información X soporta grandes segmentos de la compañía?
- ¿La degradación del sistema de información X afectaría a otros activos de la compañía?

e. Colapso económico, Trastorno significativo, Mínimo, Ninguno, Desconocido

- ¿Qué tipo de trastorno económico puede causarle al negocio la pérdida o degradación del sistema de información X?

f. Grande, Mediano, Pequeño, Ninguno, Desconocido

- ¿Cuál es el tamaño del área de la compañía que es soportada por este sistema?

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 (Wallace, 2004):

- 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
- Cuadros y 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 DE 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 de tarjeta de crédito, 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, Autorizaciones……. 600 GB
- Servidor XYX, Tarjeta crédito……...2200 GB

Medio: DVD

- Servidor XYS, Troquelación……3 GB

Periodicidad: SEMANAL

Medio: CINTA

- Servidor XYXZ, Datawarehouse……...2300 GB
- Servidor XYXX, Tarjeta crédito…….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 un cuadro 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.

Cuadro 7. Respaldos incrementales vs Replicación de Datos (Infocentre, 2007)

ESQUEMA	RTO-RPO	DUPLICI-DAD DE DATOS	DESINCRO-NIZACIÓN DE DATOS	PÉRDIDA DE INFORMA-CIÓN POR CINTAS CORRUPTAS	ANCHO DE BANDA REQUERI-DO
Actualización por respaldos incrementa-les	Alta probabilidad de que se incrementen 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).	4.5 Mbps (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	4.5 Mbps (aprox.),

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 de 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. (PMI, 2004)

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, 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

Cuadro 8. Ejemplo de una Matriz de Comunicaciones (Infocentre, 2007)

Tipo (1)	**Propósito (2)**	**Responsable (3)**	**Distribución (4)**	**Medio (5)**	**Frecuencia (6)**	**Consideraciónes 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 • Aprobar y tomar decisiones	Luis Morera / 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.	• Resolver los asuntos relacionados a los recursos del proyecto • Seguimiento al cronograma • Aprobar y tomar decisiones	Director del proyecto	•Gerente de 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 AM	Se debe generar una minuta de la reunión la cual será guardada en la carpeta del proyecto.

Tipo (1)	Propósito (2)	Responsa-ble (3)	Distribu-ción (4)	Medio (5)	Frecuen-cia (6)	Considera-ciónes especiales (7)
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 AM	Informal
Boletines por Correo Electrónico	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 el web site, sección de noticias.

Distribución de la Información. 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 el Cuadro 8.

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 todos 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 – IMPLEMENTACIÓN DEL PLAN EN EL GRUPO FINANCIERO

4.1 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.

4.1.1 Comité Ejecutivo del Proyecto. Estará conformado de acuerdo a los requerimientos estratégicos del Banco, 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. Será responsable de tomar las decisiones que tengan que ver con cambios fuertes en el alcance del proyecto y en el esquema de contratación. El cuadro 9 muestra un ejemplo de un posible Comité Ejecutivo.

Cuadro 9. Comité Ejecutivo

PUESTO	NOMBRE	DEPARTAMENTO
Gerente-Empresa XYZ	Juan Pérez	Gerencia
Gerente Tecnología	Carlos Rodríguez	Tecnología
Gerente Desarrollo	María Rojas	Desarrollo
Director PMO	Jorge Salazar	Administración Proyectos

NOTA: En caso de existir relaciones con proveedores externos se recomienda tener un representante de los mismos en el Comité Ejecutivo.

4.1.2 Comité Operativo. Estará conformado de acuerdo a los requerimientos de seguimiento y control del proyecto desde una perspectiva táctica/operativa. En él participan representantes del Comité Ejecutivo, el Director del Proyecto, Asesores del Proyecto y los representantes de cada producto a recuperar en el sitio alterno. Además se podrán incorporar aquellos funcionarios que en determinado momento sean requeridos. Su función principal será la de controlar el avance del proyecto y la calidad de las entregas. Los gerentes funcionales participarán por demanda o requerimiento para tomar decisiones funcionales asociadas a su área de trabajo.

El Cuadro 10 muestra un ejemplo de un Comité Operativo.

Cuadro 10. Comité Operativo

PUESTO	NOMBRE	DEPARTAMENTO
Gerente-Empresa XYZ	Juan Pérez	Gerencia
Gerente Infraestructura	Carlos Rodríguez	Infraestructura
Gerente Desarrollo	María Rojas	Desarrollo
Director PMO	Jorge Salazar	Administración Proyectos
Director del Proyecto	Luis Morera	Administración Proyectos
Arquitecto DRP	Luisa Vindas	Desarrollo
Administrador de Base de Datos	Ana López	Bases de Datos
Supervisor del Centro de Datos	Andrés Rojas	Centro de Datos
Experto en intercambio con las Marcas VISA y Master Card	Diego Quirós	Intercambio

PUESTO	NOMBRE	DEPARTAMENTO
Experto en Autorizaciones	Mario Rojas	Desarrollo
Experto en aplicaciones Front-End	Silvia Salas	Desarrollo
Asegurador de Calidad	Gabriel Díaz	Control de Calidad
Usuario Experto	Juan Carlos Mora	Servicio al Cliente
Diseñador de pruebas (“*tester*”)	Rosa Vargas	Control de Calidad

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

4.1.3.1 Patrocinador

Roles

- Cliente interno. Es el receptor interno de los resultados del proyecto. También financia el proyecto.
- Figura de autoridad. El patrocinador tendrá la palabra final en decisiones que afecten las restricciones de costo, cronograma y rendimiento.

Responsabilidades

- Proveer y asegurar los recursos para el proyecto.
- Definir o aprobar el alcance del proyecto.
- Aprobar cambios en los objetivos del proyecto como resultado de cambios en el alcance

- Tomar las decisiones al final de cada fase. Ejemplo, autorización del proyecto, aprobaciones, aceptaciones, entre otros.
- Interpretar o formular las políticas existentes o nuevas.
- Recibir el estado del proyecto periódicamente por parte del director del proyecto.
- Promover el proyecto y su alineamiento con los objetivos de la compañía.

4.1.3.2 Director del Proyecto

Roles

- Comunicador. Debe asegurarse que todas las partes se encuentran informadas. Debe darle seguimiento y apoyarse en la matriz de comunicaciones.
- Organizador. Establece la estructura organizacional del proyecto. Debe negociar con los gerentes funcionales y patrocinadores.
- Planificador. Debe asegurarse que se esté creando un plan integral que sea suficiente para cumplir con los objetivos del proyecto.
- Catalizador. Debe hacer que el plan del proyecto se cumpla.

Responsabilidades

- Identificar las responsabilidades de las áreas
- Comunicarse con los gerentes funcionales
- Comunicarse con los comités
- Comunicarse con los patrocinadores clientes e involucrados.

- Establecer la estructura organizacional del proyecto
- Tomar el liderazgo en la conformación del equipo del proyecto
- Liderar el equipo para desarrollar el plan del proyecto
- Preparar la documentación del proyecto
- Reportar en forma periódica los "*issues*", pendientes y estado del proyecto
- Organizar las juntas de seguimiento

4.1.3.3 Gerentes Funcionales de Infraestructura y Desarrollo

Roles

- Figura de autoridad. Deben tomar las decisiones que le atañen a sus respectivos departamentos principalmente en conflictos relacionados con recursos (humano, infraestructura, etc.)
- Solucionadores de conflictos. Principales facilitadores en la resolución de conflictos.

Responsabilidades

- Atender la invitación a las juntas que se les convoque.
- Proveer los recursos necesarios según el plan autorizado del proyecto.

4.1.3.4 Arquitecto y expertos de cada área

Roles

- Los líderes técnicos o expertos de las áreas de autorizaciones, "*core"* del sistema, intercambio con las marcas y aplicaciones "*front-end"* sirven como soporte clave al director del proyecto cuando el conocimiento técnico sea un factor relevante. Proveen información clave y experiencia en el diseño e

implementación de múltiples aspectos y su integración clave con el producto o servicio final.

- Los arquitectos son los creadores de los modelos de la solución. Deben analizar las distintas opciones de la solución y hacer las recomendaciones del caso.

- Tanto los líderes técnicos como el arquitecto tienen un rol de "*couching"* con el resto del equipo del proyecto.

Responsabilidades

- Crear y documentar definiciones técnicas y direccionarlas de manera que puedan ser entendidas por todos los miembros del equipo.

- Asistir al director del proyecto con la identificación de las áreas técnicas y en la creación del plan del proyecto. El líder técnico será el autor de las áreas del plan del proyecto que se relacionan con descripciones de productos y funciones, confiabilidad en requerimientos, aspectos técnicos, verificación y validación.

- Comunicar y resolver cambios técnicos del producto dentro de las restricciones de costo, tiempo y desempeño.

- Entender, usar e impulsar el uso de herramientas apropiadas.

4.1.3.5 Administrador de las bases de datos

Roles

- Tiene el mismo rol de un líder técnico pero circunscrito al área de base de datos.

Responsabilidades

- Proveer las diferentes opciones de replicación, respaldo y restauración de datos al sitio alterno con las respectivas recomendaciones durante la fase de diseño de la solución.
- Proveer los datos que se requieran para construir el laboratorio de pruebas según el cronograma del proyecto.
- Proveer a tiempo y de forma eficiente los datos que requieran los diferentes equipos para ejecutar sus actividades.

4.1.3.6 Supervisor del Centro de Datos

Roles

- Como administrador del centro de datos conoce las tareas operativas que se realizan el mismo, incluyendo, periodicidad de las actividades, herramientas utilizadas y su localización, dependencias y responsables de ejecutarlas.

Responsabilidades

- Facilitar la información requerida por los equipos encargados de generar los planes de recuperación que involucren máquinas, procesos o aplicaciones del centro de datos.

4.1.3.6 Asegurador de la calidad

Roles

- **Auditor**. Debe velar porque se siga y respete la metodología usada en la organización para desarrollar el proyecto.

- **Asistente.** Es la “mano derecha” del director del proyecto apoyando la gestión de administración del proyecto evaluando continuamente la calidad del proceso.

- **Consultor.** Dado que estará validando que se cumplan los criterios de calidad definidos para este proyecto en cada uno.de sus módulos, deberá participar como consultor sobre el impacto que podría tener un cambio externo o interno al proyecto.

Responsabilidades

- Generar informes de las revisiones de calidad que realice.

- Generar alertas cuando no se siga la metodología de la organización.

- Velar porque se siga el respectivo proceso de administración de cambios dentro del proyecto.

- Apoyar y auditar el proceso de administración de riesgos generando los respectivos informes.

4.1.3.7 “*Tester*” y Usuario Experto

Roles

- Durante la etapa de pruebas, el *“tester”* debe cumplir el rol de persona técnica que es externo a los cambios en las aplicaciones, sistemas y procesos a probar, de manera que no sea el desarrollador de los cambios el que defina y realice las pruebas (juez y parte).

- El usuario experto tiene un rol similar al del *“tester”* pero su papel se limita a probar el correcto funcionamiento de las aplicaciones finales, el “tester” prueba integralmente.

- Ambos personas tienen un rol comunicador con respecto al avance de la etapa de pruebas.

Responsabilidades

- Definir la estrategia de pruebas de cada módulo que es parte del proyecto DRP.
- Ejecutar las pruebas
- Crear un informe con el resultado de las pruebas y enviarlo al Comité Ejecutivo.
- Comunicar cualquier anomalía que surja durante la etapa de pruebas.

4.1.4 Matriz de Responsabilidades

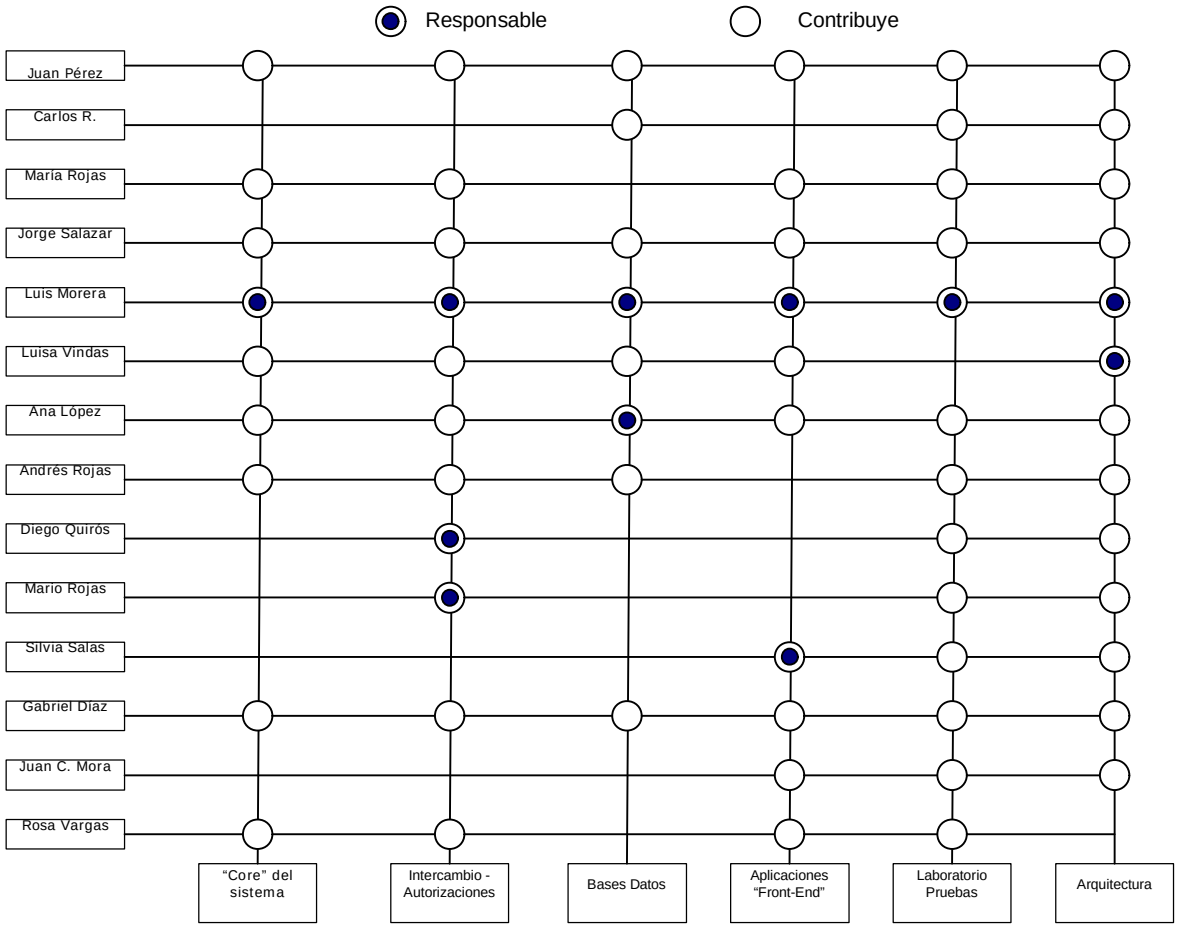


Figura 8. Ejemplo de una matriz de responsabilidades

4.2 Distribución de las actividades en el tiempo

Cuadro 11. Propuesta de Cronograma

ACTIVIDAD	DURACIÓN	INICIO	FIN
Desarrollo de planes por área	**24.5 Días**	**02/06/08**	**30/06/08**
Centro Datos Procesadora	**15 Días**	**02/06/08**	**19/06/08**
Junta de expertos para definir procesos del Centro de Datos a incluir en DRP	8 horas	02/06/08	02/06/08
Documentación de la junta de expertos	8 horas	03/06/08	03/06/08
Levantado de inventario de máquinas y aplicaciones	40 horas	04/06/08	10/06/08
Recolección de Instaladores	40 horas	11/06/08	17/06/08
Recolección de requerimientos previos a la instalación	24 horas	18/06/08	20/06/08
Intercambio/Autorizaciones (Emisión/Adquirencia VISA-MasterCard)	**9,5 Días**	**03/06/08**	**13/06/08**
Junta con expertos de negocio para definir procesos a incluir en DRP	4 horas	04/06/08	04/06/08
Documentación de la junta de expertos	8 horas	04/06/08	05/06/08
Levantado de inventario de equipos y aplicaciones	24 horas	05/06/08	10/06/08
Recolección de Instaladores	24 horas	10/06/08	13/06/08
Recolección de requerimientos previos a la instalación	16 horas	13/06/08	17/06/08
Bases Datos	**10 Días**	**05/06/08**	**19/06/08**
Junta de expertos para definir requerimiento de datos en sitio alterno	16 horas	05/06/08	09/06/08
Documentación de la junta de expertos	8 horas	9/06/08	10/06/08
Diseño de esquema de replicación de datos al sitio alterno	24 horas	10/06/08	13/06/08
Análisis de Factibilidad	24 horas	13/06/08	18/06/08
Definición de esquema final de replicación de datos al sitio alterno	8 horas	18/06/08	19/06/08
Aplicaciones Front-End	**18 Días**	**10/06/08**	**4/07/08**
Junta con expertos de negocios para definir aplicaciones clave a contemplar en el DRP	8 horas	10/06/08	11/06/08
Documentación de la junta de expertos	8 horas	11/06/08	12/06/08

ACTIVIDAD	DURACIÓN	INICIO	FIN
Inventario de Máquinas y Aplicaciones	24 horas	12/06/08	17/06/08
Recolección de Instaladores	80 horas	17/06/08	1/07/08
Recolección de requerimientos previos a la instalación	24 horas	1/07/08	4/07/08
Creación de laboratorio para pruebas	**36 Días**	**12/06/08**	**01/08/08**
Adquisición de equipos para pruebas de laboratorio	40 horas	12/06/08	19/06/08
Instalación de la Red	40 horas	19/06/08	26/06/08
Instalación y configuración de hardware y software en paralelo con la creación de los TAP	80 horas	4/07/08	18/07/08
Ejecución de Pruebas de aplicaciones del Centro de Datos actualizando los procedimientos	80 horas	18/07/08	1/08/08
Ejecución de Pruebas de aplicaciones de Intercambio actualizando los procedimientos	80 horas	18/07/08	1/08/08
Ejecución de Pruebas de aplicaciones Front-End actualizando los procedimientos	80 horas	18/07/08	1/08/08
Certificación de Procedimientos en sitio alterno	**48,5 Días**	**02/06/08**	**07/08/08**
Adquisición de equipos para el sitio alterno	40 horas	02/06/08	06/06/08
Instalación y configuración de equipos en el sitio alterno	40 horas	09/06/08	13/06/08
Pruebas de replicación de datos al sitio alterno	16 horas	16/06/08	17/06/08
Implementación de los procedimientos del centro de datos	16 horas	01/08/08	5/08/08
Pruebas de funcionalidad de las aplicaciones del centro de datos	8 horas	5/08/08	6/08/08
Implementación de los procedimientos de Intercambio	16 horas	1/08/08	5/08/08
Pruebas de funcionalidad de las aplicaciones de Intercambio	8 horas	5/08/08	6/08/08
Implementación del los procedimientos de aplicaciones Front- End	16 horas	1/08/08	5/08/08
Pruebas de funcionalidad de las aplicaciones Front-End	8 horas	6/08/08	7/08/08
Firma de certificación de procesos	0 horas	7/08/08	7/08/08
Plan de Mantenimiento	**1 Día**	**02/06/08**	**02/06/08**
Modificaciones al proceso de Administración de Cambios	8 horas	02/06/08	02/06/08
Liberación de la Política del Plan de Mantenimiento	0 horas	02/06/08	02/06/08
Plan de Simulación	**13 Días**	**02/06/08**	**18/06/08**

ACTIVIDAD	DURACIÓN	INICIO	FIN
Junta con expertos de negocio y sistemas para definir la estrategia de las simulaciones	16 horas	02/06/08	03/06/08
Diseño del plan de simulacros	80 horas	04/06/08	17/06/08
Junta de aceptación del plan	8 horas	18/06/08	18/06/08
Liberación de la Política del Plan de Simulación	0 horas	18/06/08	18/06/08
Cierre	**1 Día**	**07/08/08**	**08/08/08**
Desarrollar sesión de lecciones aprendidas	8 horas	07/08/08	08/08/08
Firmar cierre del proyecto	0 horas	08/08/08	08/08/08

4.3 Gestión de Riesgos

4.3.1 Análisis de *"Issues"* y Supuestos

NOTA: El supuesto consiste en la afirmación del "issue". Por ejemplo, el "issue"

- ¿Se cuenta con el código fuente de todas las aplicaciones a respaldar? – corresponde al supuesto - Se cuenta con el código fuente de todas las aplicaciones a respaldar.

Sensibilidad.

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

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

Estabilidad:

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

a. Hay mucha confianza de que el supuesto esté estable
b. Bastante confiable

c. Incómodo
d. Muy incómodo (es muy probable que el supuesto resulte ser incorrecto)

Cuadro 12. Análisis de “Issues”

“ISSUE”	CRITICI-DAD	IMPACTO (si no se atiende)	SENSIBI-LIDAD	ESTA-BiLIDAD
1) ¿Cómo me aseguro que los expertos en las aplicaciones del centro de datos estarán disponibles el 2 de Junio? 2) ¿Cómo me aseguro que los expertos en Intercambio/Autorizaciones estarán disponibles el 4 de Junio? 3) ¿Cómo me aseguro que los expertos en bases de datos estarán disponibles el 5 de Junio? 4) ¿Cómo me aseguro que los expertos en las aplicaciones “*Front-End*” estarán disponibles el 10 de Junio?	AMARILLO	• Se atrasa el cronograma. • Podrían quedar aplicaciones clave fuera del DRP o con riesgos desconocidos.	B	A
5) ¿Se cuenta con el código fuente de todas las aplicaciones a respaldar?	ROJO	• Podrían quedar fuera del plan aplicaciones clave para el buen funcionamiento del negocio • Se atrasa el cronograma si se debe reprogramar la aplicación o sistema	D	C

"ISSUE"	CRITICI-DAD	IMPACTO (si no se atiende)	SENSIBI-LIDAD	ESTA-BiLIDAD
6) ¿Se tienen todas las licencias de los productos utilizados? 7) ¿Se pueden usar estas licencias en el sitio alterno?	AMARILLO	• Si se deben comprar licencias adicionales el costo del proyecto puede aumentar	B	B
8) ¿El presupuesto destinado a la compra de máquinas se tiene disponible?	AMARILLO	• Se atrasa la creación del laboratorio • Se atrasa la creación del sitio alterno	C	B
9) ¿El proveedor de las máquinas puede entregar el producto en una semana luego de hacer el pedido?	AMARILLO	• Se atrasa la creación del laboratorio • Se atrasa la creación del sitio alterno	C	B
10) ¿Se cuenta con un sitio en la organización para implementar el laboratorio?	AMARILLO	• Se atrasa la creación del laboratorio	D	B
11) ¿Se cuenta con suficiente personal para atender el día a día del negocio y los requerimientos del proyecto?	ROJO	• Se atrasa el plan	C	C
12) ¿La comunicación entre la organización y el sitio alterno es menor a 3 segundos?	AMARILLO	• Lentitud en el monitoreo del sitio alterno y traslado de información (si se requiere	C	B

"ISSUE"	CRITICI-DAD	IMPACTO (si no se atiende)	SENSIBI-LIDAD	ESTA-BiLIDAD
13) ¿Se cuenta con un medio manual o automático para enviar los respaldos de las bases de datos al sitio alterno?	ROJO	• Factor principal para implementar el plan	D	A
14) ¿Se pueden implementar las aplicaciones VISA/Master Card en el sitio alterno? 15) ¿Se requiere gestionar algo directamente en las marcas?	ROJO	• Aplicaciones principales del negocio de tarjeta de crédito	D	A
16) ¿Se cuenta con personal dedicado a darle mantenimiento al hardware/software implementado en el sitio alterno?	ROJO	• Las actividades de Intercam-bio/Autoriza-ciones pueden quedar incompletas	C	B
17) ¿Se cuenta con personal en el sitio alterno para realizar tareas operativas (carga de cintas)?	ROJO	• El plan pierde efectividad y vigencia	B	B
18) ¿El personal clave que debe viajar al sitio alterno requiere algún tipo de visa o permiso para ingresar?	AMARILLO	• Se atrasa la creación del sitio alterno	B	B

4.3.2 Clasificación de '*Issues*'/Supuestos

- Supuestos no cruciales para el proyecto con altas probabilidades de que sean verdaderos.

  1 – 2 – 3 – 4 – 6 – 7 – 17- 18

- Supuestos que deben ser revisados con los expertos de forma regular ya que corresponden a riesgos potenciales.

  8 – 9 – 10 – 12 – 13 – 14 – 15 – 16

- Riesgos que requieren acciones para mantenerlos bajo control.

  5 – 11

Cuadro 13. Categorización de riesgos

RIESGO	CRITICIDAD	CONTROLABILI-DAD	RESPONSABLE	DISPARADOR /ACCIÓN
5) SUPUESTO Se cuenta con el código fuente de todas las aplicaciones a respaldar IMPACTO • Podrían quedar fuera del plan aplicaciones clave para el buen funcionamiento del negocio • Se atrasa el cronograma si se debe reprogramar la aplicación o sistema	ROJO	C	María Rojas/Gerente de Desarrollo	DISPARADOR Al realizar la actividad "Recolección de Instaladores" se valida que faltan instaladores. ACCIÓN Definir un equipo que busque los instaladores. Si no se encuentran se debe revalidar la criticidad de la aplicación que falta y definir si se debe reprogramar e informar del impacto.
8) SUPUESTO El presupuesto destinado a la compra de máquinas se tiene disponible IMPACTO • Se atrasa la creación del laboratorio • Se atrasa la creación del sitio alterno	AMARILLO	B	Juan Pérez/ CIO-Empresa Grupo financiero	DISPARADOR Fondos económicos insuficientes para compra de máquinas. ACCION Modificar el plan de acuerdo al atraso e informar al respecto

RIESGO	CRITICIDAD	CONTROLABILI-DAD	RESPONSABLE	DISPARADOR /ACCIÓN
9) SUPUESTO El proveedor de las máquinas puede entregar el producto en una semana luego de hacer el pedido IMPACTO • Se atrasa la creación del laboratorio • Se atrasa la creación del sitio alterno	VERDE	B	Carlos Rodríguez / Gerente Infraestructura	DISPARADOR Tres días antes del envío del equipo no se tiene confirmación del proveedor ACCION Realizar contratos con multas por incumplimiento. Aplicar multas, modificar el plan de acuerdo al atraso, informar al respecto
10) SUPUESTO Se cuenta con un sitio en la organización para implementar el laboratorio IMPACTO • Se atrasa la creación del laboratorio	AMARILLO	B	Juan Pérez/ CIO-Empresa Grupo financiero	DISPARADOR Dos semanas antes para implementar el laboratorio no se tiene definido el sitio para el mismo. ACCION Buscar un sitio alterno ya sea alquilado o en alguna de las oficinas del Grupo Financiero. Validar impacto en el

				plan e informar al respecto.
RIESGO	**CRITICIDAD**	**CONTROLABILI-DAD**	**RESPONSABLE**	**DISPARADOR /ACCIÓN**
11) SUPUESTO Se cuenta con suficiente personal para atender el día a día del negocio y los requerimientos del proyecto IMPACTO Se atrasa el plan en la cantidad de días con que no se cuente con el personal	ROJO	C	Luis Morera / Director del Proyecto	DISPARADOR Una semana antes de cada actividad no se tiene confirmación de la disponibilidad de los recursos asignados a la tarea. ACCION Contratar una empresa proveedora de personal calificado antes de iniciar el proyecto y utilizarlo en caso de que sea necesario. Calcular impacto por curva de aprendizaje e informar al respecto.
12) SUPUESTO La comunicación entre la organización y el sitio alterno es menor a 3 segundos IMPACTO Lentitud en el monitoreo del sitio	AMARILLO	B	Carlos Rodríguez / Gerente Infraestructura	DISPARADOR Al realizar pruebas no se obtienen las métricas necesarias. ACCIÓN Contratar enlace

alterno y traslado de información (si se requiere)				satelital.
RIESGO	**CRITICIDAD**	**CONTROLABILI-DAD**	**RESPONSABLE**	**DISPARADOR /ACCIÓN**
13) SUPUESTO Se cuenta con un medio manual o automático para enviar los respaldos de las bases de datos al sitio alterno IMPACTO Factor principal para implementar el plan	ROJO	B	Luis Morera / Director del Proyecto	DISPARADOR Antes de iniciar el proyecto no se puede obtener un contrato "Courier" para enviar las cintas al sitio alterno. ACCION Contratar líneas de comunicación con un ancho de banda mayor y colocar servidores espejo en ambos sitios. Validar costos y comunicar el impacto.
14) SUPUESTO Se pueden implementar las aplicaciones VISA/Master Card en el sitio alterno IMPACTO Aplicaciones principales del negocio de tarjeta de crédito	ROJO	B	María Rojas / Gerente Desarrollo	DISPARADOR Las marcas comunican que los procesos solo se pueden realizar en el sitio actual. ACCION Re-contratar servicio en el sitio alterno

RIESGO	CRITICIDAD	CONTROLABILI-DAD	RESPONSABLE	DISPARADOR /ACCIÓN
15) SUPUESTO Si se requiere gestionar algo directamente en las marcas se tiene la colaboración de las mismas IMPACTO Las actividades de Intercambio/Autori-zaciones pueden quedar incompletas	AMARILLO	C	Diego Quirós / Intercambio	DISPARADOR No se puede localizar un experto en las oficinas de las marcas. ACCION Contratar el servicio en las marcas.
16) SUPUESTO Se cuenta con personal dedicado a darle mantenimiento al hardware/software implementado en el sitio alterno IMPACTO El plan pierde efectividad y vigencia	AMARILLO	B	Luis Morera / Director del Proyecto	DISPARADOR En el contrato de arrendamiento del sitio alterno no se brinda el servicio. ACCION Contratar el servicio con la empresa administradora del sitio remoto

4.4 Costos aproximados

Para desarrollar el plan de costos, lo primero que se debe hacer es una estimación del costo de los recursos necesarios para desarrollar el plan de recuperación. Para esto se recomienda tomar en cuenta lo siguiente:

Entradas para determinar los recursos:

- Activos organizacionales como conocimiento del equipo del proyecto, documentos de lecciones aprendidas, archivos de otros proyectos relacionados con los principales módulos de la organización.
- Documento de alcance del proyecto
- Documento de Estructura del Desglose de Trabajo (EDT).

Herramientas para determinar el costo de los recursos:

- Estimación por analogía: Se recomienda esta técnica ya que es por medio del juicio de expertos e información de proyectos anteriores en módulos específicos, que se va a determinar, tanto los recursos a tomar en cuenta en el plan de recuperación, como el costo asociado a éstos.

Salidas del proceso de estimación de costos:

El siguiente cuadro de costos muestra un ejemplo de lo que se puede esperar con base en el proceso de determinación de recursos y su costo asociado. Este cuadro se desarrolló bajo los siguientes supuestos:

- El sitio alterno tiene servicios de teléfono, impresora, parqueo, internet y está localizado en Arizona, Estados Unidos.
- El sitio actual y el sitio remoto tienen escritorios, *“racks”* (lugar donde se alojan los servidores) y sillas.

- El sitio actual y el sitio remoto tienen el cableado estructurado requerido.
- El sitio actual y el sitio remoto tienen UPS, planta eléctrica e inversores o reguladores de picos.
- No se requiere contratar ningún servicio de capacitación.
- El laboratorio y el sitio alterno se requieren simultáneamente, es decir, no se puede utilizar el material del laboratorio en el sitio alterno.

Cuadro 14. Costos aproximados

TIPO	DESCRIPCIÓN	CARACTERÍSTICAS	COSTO APROXIMADO
Hardware Laboratorio	4 Computadoras personales	Core 2 Duo, 2.33 GHz, 1 GB Memoria DDR, Disco Duro de 80 GB	$ 900,00 c\u $3.600,00 total
	7 Servidores para base de datos, correo, y otros.	HP ProLiant DL380 G5 High Performance - Quad-Core Xeon E5345 2.33 GHz. Memoria: 4 GB (installed) / 32 GB (max) - DDR II SDRAM - Advanced ECC - 667 MHz - PC2-5300	$12.000,00 c\u $84.000,00 total
	• 2 Switches	Cisco 4500	$60.000,00 c\u $120.000,00 total
	• 1 Enrutador	Cisco 2850, 2 puertos	$10.000,00 c\u $20.000,00 total
	• 1 Modem Satelital	Incluido en el costo del contrato de enlace satelital	No aplica

	• 1 Modem para Línea Dedicada	Incluido en el costo del contrato de enlace satelital	No aplica
	Costo Total del Hardware del laboratorio……..……$ 237,600.00		
Hardware Sitio Remoto	• 4 Computadoras personales • 7 Servidores de base de datos • 2 Switches • 1 Enrutador • 1 Modem Satelital • 1 Modem para Línea Dedicada	*Idem anterior*	*Idem anterior*
	Costo Total del Hardware del sitio alterno…….$ 237,600.00		
Software Laboratorio	• 4 Licencias de office	• Office 2007	$150 c\u, total $600
	• 5 Licencias Sybase Server	• ASE Small Business Edition 15.0.2 for Windows	$7,000 c\u, Total $ 35,000
	• 4 Licencias de cliente Sybase	• Networked Seat	$195 c\u, total $780
	• 2 Licencias de SQLServer,	• SQLServer 2005	$10.000 c\u Total $20.000

	• 7 Licencias de Windows 2003 Server	• Enterprise Edition	$ 4.000 c\u Total $28,000
	Costo Total del Software del laboratorio…….$ 84,380.00		
Software Sitio Remoto	• 4 Licencias de office • 5 Licencias Sybase Server • 4 Licencias de cliente Sybase • 2 Licencias de SQLServer, • 7 Licencias de Windows 2003 Server	*Idem anterior*	*Idem anterior*
	Costo Total del Software del sitio remoto……$ 84,380.00		
Recurso Humano (Tiempo Completo)	• 4 Desarrolladores • 1 *"Tester"* • 1 QA • 2 Administradores de Bases de Datos • 2 Especialistas en Infraestructura • 1 Especialista en Comunicaciones • 1 Director de Proyectos	No aplica	4 Especialistas calculados en $2,500 c\u durante 3 meses. Total: $30,000 8 Analistas calculados en $1,500 c\u durante 3 meses. Total: $36,000
	Costo Total del recurso humano……$ 66,000		

<table>
<tr><td>Contratos

(Anual)</td><td>Contrato de Servicios con el sitio alterno</td><td>Incluye servidores de tipo “Servicio Administrado” que implica que las aplicaciones se mantienen instaladas.</td><td>$600,000 Anuales</td></tr>
<tr><td colspan="4">Costo Total por contrato con el sitio alterno……$ 600,000</td></tr>
<tr><td>Logística</td><td rowspan="4">Transporte y viáticos durante una semana en Arizona, Estados Unidos, para siete personas encargados de implementar el sitio alterno</td><td>• Boletos Aéreos</td><td>• $700 c\u, total $4900</td></tr>
<tr><td>• Transporte interno</td><td>• $1,000 total</td></tr>
<tr><td>• Hospedaje</td><td>• $1,050 todos por día

Total $7,350</td></tr>
<tr><td>• Alimentación</td><td>• $385 todos por día

Total $2,695</td></tr>
<tr><td colspan="4">Costo Total de la logística para implementar el sitio alterno… $ 15,945</td></tr>
<tr><td>Comunicaciones</td><td>Contrato de enlace satelital</td><td>E1 (2 MBits/s)</td><td>$300.000 Anuales</td></tr>
<tr><td colspan="4">Costo Total por las comunicaciones con el sitio alterno……..$ 300,000</td></tr>
</table>

Por lo tanto,

Costo total aproximado de implementar el laboratorio y el sitio alterno	$725,905
Costos fijos anuales por contratos con el proveedor de las comunicaciones y el sitio alterno	$900,000 anuales

Los restantes procesos del área de Gestión de Costos, a saber, preparación del presupuesto de costos y el control de los costos, no se toman en cuenta en esta guía dado que son parte de la puesta en práctica del proyecto de recuperación en caso de desastre, utilizando o no esta guía.

5 – 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. Se tomó como base una empresa de tecnología que brinda el servicio de procesamiento de datos para organizaciones financieras, específicamente en el campo de tarjetas de crédito.

El plan abarcó la recuperación de aplicaciones, sistemas y procesos, 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 procesadora de tarjeta de crédito. 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 que provee el marco de trabajo ITIL.

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 Centro de Datos, 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. Por ejemplo, la operación diaria en Costa Rica y el sitio alterno en Estados Unidos.
- 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.

6 - BIBLIOGRAFÍA

- Bajada , Stephen. **ITIL Foundations**. GTS Learning Group, 2007. p.irr

- Burtles, Jim. **Principles and Practice of Business Continuity—Tools and Techniques**. Rothstein Associates Inc., Publisher. Brookfield, Connecticut USA, 2007. p.irr

- Hernández Sampieri, R. – Fernández Collado, C. – Lucio, P., **Metodología de la Investigación**. Cuarta Edición, McGraw Hill, México, 2006. p.irr

- Hiatt, Charlotte. **A Primer for Disaster Recovery Planning in an IT Environment**. Published in the United States of America. Idea Group Publishing, 2000. p.irr

- Ianna, Frank. **Disaster Recovery for Business; Disaster Recovery Journal,** Estados Unidos, 1997. p.irr

- infocentre.eds.com/risk_management/, Intranet Corporativa de la empresa Electronic Data Systems (EDS). Estados Unidos, 2007. Extraído el 03 de Diciembre, 2007.

- P.M.I (Project Management Institute), **Guía de los Fundamentos de la Dirección de Proyectos, PMBOK Guide**. Tercera Edición, Estados Unidos, 2004. p.irr

- Robertson, Guy. **People, Paper, Data: Disaster Planning for Libraries.** Estados Unidos, 1997. p.irr

- Schreider, Tari (**1998. "Using the Internet to Develop An Effective Disaster Recovery Plan;" The 9th Annual Corporate Continuity Planning Seminar and Exhibition, San Diego, CA, March 15-18**), Estados Unidos 1998.

- SkillSoft Corporation. **Managing Infrastructure using ITIL**, 2007

- Toigo, Jon William. **Disaster Recovery Planning: Managing Risk and Catastrophe in IS.** Yourdon Press, Prentice-Hall, Inc., USA, Englewood Cliffs, New Jersey, 1989. p.irr

- Wallace, Michael y Webber, Lawrence**. The Disaster Recovery Handbook—A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets**. Estados Unidos, AMACOM, a division of American Management Association, 1601 Broadway, New York, NY 10019, 2004. p.irr

- Weil, Steven – Northcutt, Stephen – Edmead, Mark. **Disaster Recovery and Business Continuity Step-by-Step**. SANS Institute, 2004. p.irr

- Wold, Geoffrey H. and Shriver, Robert F. **Risk Analysis Techniques; Disaster Recovery Journal,** Estados Unidos, 1997. p.irr

- Wold, Geoffrey H. **Some Techniques for Business Impact Analysis**, Disaster Recovery Journal, 1996. p.irr

- www.VISAOnLine.com, sitio web privado para las empresas procesadoras de tarjeta de crédito. Estados Unidos, 2007. Extraído el 25 de Noviembre, 2007.

ANEXOS

ANEXO No.1

ACTA DEL PROYECTO

ANEXO No.2

ESTRUCTURA DETALLADA DE TRABAJO (EDT)

ANEXO No.3

CRONOGRAMA DEL PROYECTO