UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA
DE SISTEMAS – PLANEACIÓN

ESTRATEGIA PARA IMPLANTAR UN PLAN DE RECUPERACIÓN ANTE DESASTRES EN LA COMISIÓN NACIONAL DE SEGUROS Y FIANZAS: UN ESTUDIO DE CASO

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN INGENIERÍA

PRESENTA:
MIGUEL FRANCO MARTÍNEZ

TUTOR PRINCIPAL
DR. JAVIER SUAREZ ROCHA
FACULTAD DE INGENIERÍA

MÉXICO, D. F. MAYO 2013

JURADO ASIGNADO:

Presidente:	**Dr. José Jesús Acosta Flores**
Secretario:	**M. I. Arturo Fuentes Zenón**
Vocal:	**Dr. Javier Suárez Rocha**
1 er. Suplente:	**M.I. Francisca Irene Soler Anguiano**
2 d o. Suplente:	**M. I. Mariano Antonio García Martínez**

Lugar o lugares donde se realizó la tesis: COMISIÓN NACIONAL DE SEGUROS Y FIANZAS

TUTOR DE TESIS:

DR. JAVIER SUÁREZ ROCHA

FIRMA

AGRADECIMIENTOS

A mis Padres y Hermanos

Por el cariño y apoyo que siempre me han brindado.

A mi Esposa y a mis Hijos

Por su confianza y paciencia

A mis Sobrinos

A mis Amigos

Al Dr. Javier Suárez Rocha

Por su apoyo para el desarrollo de este trabajo.

A mis Maestros y Compañeros del Posgrado de la Facultad de Ingeniería.

A mis Compañeros de la Comisión Nacional de Seguros y Fianzas

TABLA DE CONTENIDO

RESUMEN

La realización de las actividades sustantivas en la Comisión Nacional de Seguros y Fianzas depende, en gran medida, del funcionamiento de los sistemas informáticos; por lo que, en caso de ocurrir una interrupción en los servicios que estos brindan, la dependencia ve comprometida su operación.

Para enfrentar esta problemática la Comisión requiere elaborar una estrategia a través de la cual sea posible responder ante un incidente que pueda interrumpir su operación y reanudarla en un tiempo aceptable, de tal forma que pueda controlar el impacto resultante en términos de credibilidad e imagen principalmente.

Para dar respuesta a esta necesidad se hace uso de dos teorías validadas:

Primera, la elaboración de un Plan de Recuperación ante Desastres (por sus siglas en inglés DRP) que permite garantizar la disponibilidad de los servicios informáticos que se proveen al exterior; así como la operación de los procesos internos críticos a un nivel aceptable en caso de desastre, de tal forma que se logre una recuperación efectiva y se mitiguen los efectos causados.

Segunda, el Enfoque de Sistemas que permite conceptualizar al objeto de estudio como un sistema, ayudando a evitar los errores comunes que se presentan en la implantación de un DRP.

ABSTRACT

The completion of the substantive activities in the Comisión Nacional de Seguros y Fianzas depends largely on the operation of information systems, so that in the event of an interruption in the services they provide, the organization is committed to operate.

To address this problem requires the Commission to develop a strategy through which it is possible to respond to an incident which may interrupt and resume operation in a reasonable period of time, so that it can control the resulting impact in terms of credibility and image mainly.

To respond to this need is using two validated theories:

First, the development of a Disaster Recovery Plan (DRP) which ensures the availability of IT services that are provided to the outside, as well as the operation of the critical internal processes to an acceptable level in the event disaster, so as to achieve an effective recovery and the effects are mitigated.

Second, the systems approach that allows conceptualizing the object of study as a system, helping to avoid common errors that occur in the implementation of a DRP.

INTRODUCCIÓN

La Gestión de Continuidad del Negocio (por sus siglas en inglés BCM), es un proceso de gestión holístico que identifica los impactos potenciales que amenazan a una organización y proporciona un marco para la construcción de un plan de recuperación, con la capacidad para una respuesta efectiva que salvaguarde los intereses de sus stakeholders clave, reputación, marca y actividades de creación de valor. Mediante éste las organizaciones buscan garantizar su permanencia, aún ante la presencia de eventos que ocasionen interrupciones en su operación, derivados del riesgo operacional. Se basa en las mejores prácticas aceptadas internacionalmente por instituciones reconocidas en el mercado como son el Instituto de Recuperación ante Desastres en Estados Unidos y el Instituto de Continuidad del Negocio en el Reino Unido.

Recuperación ante Desastres es el proceso que una organización utiliza para restablecer el acceso a su software, datos y hardware necesarios para reanudar las funciones críticas del negocio, después de un desastre ya sea natural o causado por personas; lo cual, permite mantener el compromiso de continuidad al cliente.

El riesgo operacional no es un riesgo nuevo; de hecho, es un riesgo inherente a cualquier negocio y no es exclusivo de la actividad financiera. Sin embargo, la preocupación por éste ha crecido considerablemente en los últimos años, tanto por parte de las entidades financieras como por parte de los supervisores. Además, se tiene la percepción de que ha sido un riesgo creciente en la última década, debido, entre otros factores, a la mayor dependencia de las entidades en los procesos informáticos, al desarrollo del comercio electrónico y a la aparición de nuevas técnicas de mitigación de riesgos. En definitiva, nos encontramos ante un sistema financiero con una complejidad cada vez mayor, que da lugar a que estos eventos de riesgo operacional sean más probables y que, además, en caso de que ocurran, tengan un mayor impacto.

La realización de las actividades sustantivas en la Comisión Nacional de Seguros y Fianzas (CNSF) depende, en gran medida, del funcionamiento de los sistemas informáticos; por lo que, en caso de ocurrir una interrupción en los servicios que estos brindan, la dependencia ve comprometida su operación. Así mismo, no cuenta con un plan de recuperación ante desastres que le permita garantizar que los servicios informáticos que provee al exterior así como los procesos internos críticos operen a un nivel aceptable en caso de desastre, de tal forma que se logre una recuperación efectiva y se mitiguen los efectos causados.

Para enfrentar esta problemática la CNSF busca una estrategia a través de la cual sea posible responder ante un incidente que pueda interrumpir la operación y reanudarla en un tiempo aceptable, de tal forma que pueda controlar el impacto resultante, en términos de credibilidad e imagen principalmente.

El concepto de sistema ha llegado a desempeñar un papel fundamental en la ciencia contemporánea. Esta preocupación se refleja entre los responsables de la gestión, para los que el enfoque de sistemas a problemas es fundamental y para los cuales las organizaciones, un tipo especial de sistema, son el principal objeto de estudio.

El Enfoque de Sistemas permite conceptualizar un objeto de estudio como un sistema, su aplicación en la estrategia ayudará a evitar los errores comunes que se presentan en la implantación de un Plan de Recuperación ante Desastres (por sus siglas en inglés DRP). Su carácter hace que éste sea muy efectivo en la mayoría de tipos de problemas que involucran

cuestiones complejas, que dependen en gran medida del pasado o de las acciones de los demás y/o que se derivan de la coordinación ineficaz entre los implicados.

CAPÍTULO 1. FORMULACIÓN DE LA PROBLEMÁTICA

En los últimos años se ha visto cómo la preocupación por el riesgo operacional, que hasta hace poco tiempo era considerado un riesgo secundario en el sector financiero, ha ido creciendo progresivamente. Por una parte, las entidades y los supervisores perciben que la exposición a este riesgo se ha intensificado a medida que el sector ha ido evolucionando (Nieto). Factores decisivos en esta tendencia han sido la mejora de las tecnologías, el desarrollo de nuevas técnicas de mitigación de riesgos y la creciente globalización y complejidad del sistema financiero. Por otra parte, esta industria se ha visto cada vez más interesada en la medición de este riesgo, motivada por la necesidad de mejorar su eficiencia y racionalizar la asignación de capital entre las diferentes unidades de negocio.

Así mismo, los sistemas informáticos se han convertido en elementos críticos para el funcionamiento de estas organizaciones y por lo tanto, resulta prioritario contar con los elementos necesarios para limitar su pérdida así como su recuperación.

Los desastres, imprevisibles por naturaleza, pueden ocurrir en cualquier lugar y en cualquier momento con poca o ninguna advertencia. Recuperarse de estos puede ser estresante, costoso y consumir mucho tiempo, especialmente para aquellos que no se han tomado el tiempo para pensar en el futuro y prepararse para esa posibilidad; sin embargo, los que se han preparado y realizado planes de recuperación sobreviven, comparativamente, con pérdidas mínimas y/o disrupción de la productividad.

Los desastres pueden adoptar diferentes formas. Algunos principalmente afectan personas, por ejemplo, el daño de un disco duro; mientras que otros tienen un mayor tamaño e impacto colectivo. Entre estos últimos podemos citar cortes de energía, inundaciones, incendios, tormentas, fallas de equipo, sabotaje, terrorismo e incluso epidemias. Cada uno de estos puede, por lo menos, causar a corto plazo interrupciones en el funcionamiento normal del negocio; pero, la recuperación del impacto de muchos de los desastres mencionados puede tomar más tiempo, especialmente si las organizaciones no han hecho preparativos con anticipación.

La mayoría reconoce a estos problemas potenciales como posibilidades. Desafortunadamente, la aleatoriedad de algunos de estos desastres propicia en las organizaciones una sensación de falsa seguridad: "No es probable que suceda aquí". Si las organizaciones se han preparado para enfrentarlos, el proceso de recuperación ante desastres no será estresante, por el contrario, se simplificará. Al ocurrir una catástrofe, las organizaciones que aplican su plan de recuperación ante desastres a menudo presentan una mínima o ninguna pérdida de datos, hardware o ingresos. Esto, a su vez permite mantener la confianza de sus clientes e inversionistas.

No hace muchos años, cuando una empresa deseaba encontrar la manera de prepararse contra los desastres y asegurar la continuidad del negocio, la mayor parte de su tiempo, dinero y esfuerzo se utilizaba en formas en que un desastre podría (se esperaba) evitarse por completo. Por ejemplo, el uso de líneas de datos redundantes.

Mientras que un pequeño porcentaje de corporativos consideraron a la recuperación ante desastres como una forma de mantener la continuidad del negocio, la mayor parte se centró en evitarlos. Sin embargo, en los últimos años ese paradigma ha cambiado y un nuevo tipo de preparación ante desastres ha sustituido ese tipo de pensamiento. Evitar es una gran idea en teoría, pero no siempre puede ser reproducida en la vida real.

Los acontecimientos del 11 de septiembre han puesto claramente de manifiesto las deficiencias y lo inadecuado de la idea de los planes que buscan evitar el desastre. La urgente necesidad de recuperar la continuidad del negocio después del desastre y la incapacidad de muchas organizaciones para poder acceder a las funciones críticas de negocio de forma normal, fueron una llamada de atención para reevaluar los planes que habían puesto en marcha para mitigar estos eventos. Estos hechos permitieron a muchas organizaciones considerar el alto precio pagado por su vulnerabilidad inconsciente. Tratar de evitar los desastres es un buen punto para empezar, pero ahora las organizaciones se han dado cuenta que también deben prepararse para circunstancias inevitables.

La Planeación de Recuperación ante Desastres es el factor que hace la diferencia crítica entre las organizaciones que pueden manejar crisis con éxito con un costo y esfuerzo mínimo y máxima velocidad y, aquellas que ocupan incalculables períodos de tiempo de sus proveedores a cualquier costo y están obligadas a tomar decisiones desesperadas para su recuperación.

El objetivo principal de cualquier plan de recuperación ante desastres es ayudar a la organización a mantener la continuidad del negocio, minimizar el daño y evitar la pérdida. La mejor forma de garantizar la fiabilidad del plan es su práctica de manera regular. Tener a las personas adecuadas practicando lo que harían para ayudar a recuperar la función de negocios en caso de que ocurra un desastre. También se deben de programar revisiones periódicas y actualizaciones de los planes de recuperación. Algunas organizaciones encuentran útil hacer esto una vez al mes, a fin de que el plan se mantenga al corriente y refleje las necesidades de hoy de la organización, y no sólo los datos, software, etc., que había tiempo atrás.

De acuerdo con (Dávila, 2005) para elaborar el Plan de Recuperación ante Desastres se entrevista a la gente de tecnología y se le pide información de la infraestructura correspondiente (datos, hardware y software), así como a los usuarios finales respecto a las aplicaciones. Sin embargo, debido al poco tiempo que brindan los entrevistados y al poco entendimiento de parte del entrevistador se termina por hacer un plan de alto nivel, sin mucho detalle, inclusive validado por los primeros.

Las dificultades que esperan a aquellos que desarrollan planes de continuidad del negocio son numerosas (DRI, 2009). Cuando se está desarrollando un Plan de Recuperación ante Desastres se tiene que ajustar a las necesidades de la organización, ya que si se emplea el plan de alguna otra, basado en condiciones y requerimientos que la organización no tiene, entonces puede resultar en desastres de otro tipo.

La mejor forma de evitar esto es determinar las necesidades de la organización y en función a esto la respuesta más apropiada. Así mismo, es necesario detallarlos a fin de presupuestar correctamente los costos asociados y evitar dolores de cabeza al personal de la organización en tiempos de desastre.

Más aún, si bien los conceptos de continuidad del negocio y recuperación ante desastres se originaron a partir de tecnologías de la información, la planeación conceptual sólo para infraestructura de TI deja a la organización abierta a una posible catástrofe. Por ejemplo, si existen programas para gestionar las operaciones críticas fuera del departamento de TI y no se consideran durante las etapas de planeación, entonces al momento de ocurrir un desastre no se incluirá su recuperación.

La realización de las actividades sustantivas en la Comisión Nacional de Seguros y Fianzas depende, en gran medida, del funcionamiento de los sistemas informáticos; por lo que, en caso de ocurrir una interrupción en los servicios que estos brindan, la dependencia ve comprometida su operación.

Así mismo, la CNSF no cuenta con un plan de recuperación ante desastres que le permita garantizar que los servicios informáticos que provee al exterior así como los procesos internos críticos operen a un nivel aceptable en caso de desastre, de tal forma que se logre una recuperación efectiva y se mitiguen los efectos causados.

Para enfrentar esta problemática la CNSF requiere elaborar una estrategia a través del cual sea posible responder ante un incidente que pueda interrumpir la operación y reanudarla en un tiempo aceptable, de tal forma que pueda controlar el impacto resultante, en términos de credibilidad e imagen principalmente.

Este tipo de planes está enfocado principalmente hacia tecnologías de la información, por lo que su elaboración es responsabilidad del personal de la Dirección de Soporte; el cual, en apego a sus funciones establecidas, hasta este momento únicamente a determinado las normas y procedimientos de respaldo y recuperación de información, así como adquirido un software que le permitirá realizar el análisis de impacto al negocio, el análisis del riesgo operacional, definir estrategias de mitigación de desastres (incluido el procedimiento de recuperación) y finalmente documentar el plan de recuperación ante desastres de TI; sin embargo, el éxito de éste depende de la estrategia que se siga para su implantación, por lo que el problema a resolver se centra en la definición adecuada de ésta así como de su validación.

Concluyendo, podemos decir que el problema que se tiene en la CNSF es la falta de un plan de recuperación ante desastres y de una estrategia para su implantación de forma exitosa, por lo que, es necesaria la elaboración de:

Una Estrategia para Implantar un Plan de Recuperación ante Desastres en la Comisión Nacional de Seguros y Fianzas

En la figura 1 se presenta el mapa conceptual que representa de manera general la problemática que enfrenta la CNSF, así como la forma en que deberá resolverse el problema asociado.

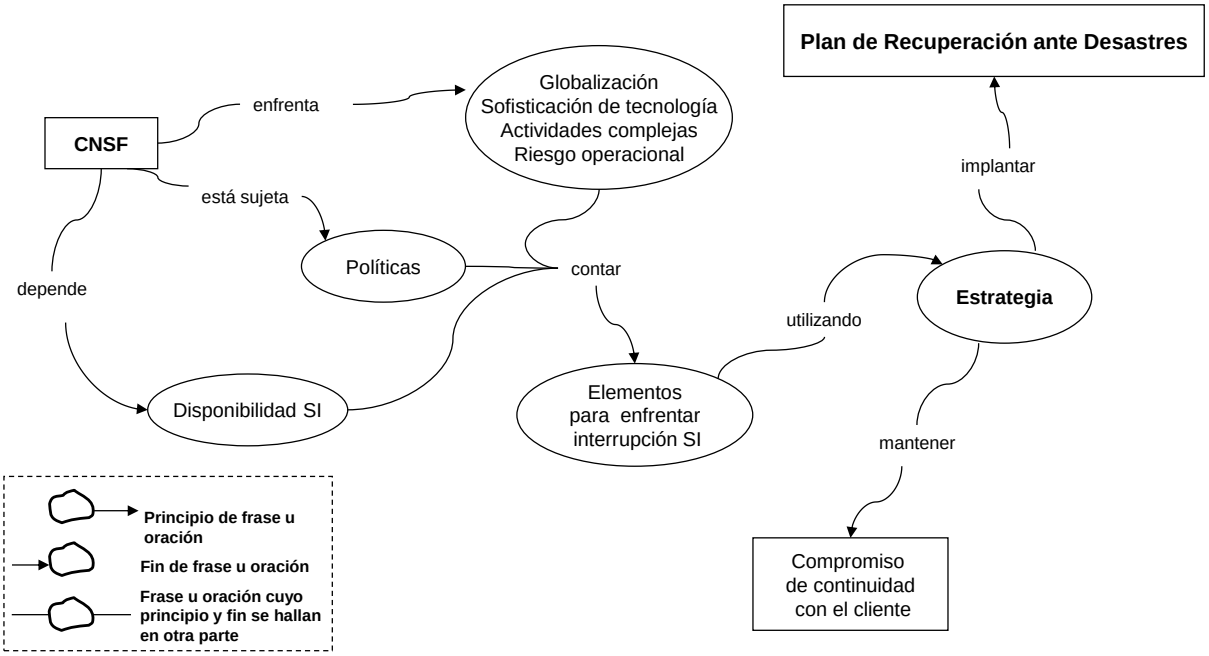


Figura 1. Mapa conceptual de la formulación de la problemática en la CNSF

Objetivo General

Elaborar una estrategia para implantar un Plan de Recuperación ante Desastres en la Comisión Nacional de Seguros y Fianzas.

Objetivos Particulares

A continuación se listan los objetivos particulares que se quieren alcanzar con la realización de este trabajo; mismos que, se jerarquizan en la figura 2.

- Establecer los conceptos de sistemas necesarios para el desarrollo de la Estrategia.
- Realizar el análisis de impactos al negocio.
- Realizar la evaluación de riesgos.
- Evaluar y documentar la estrategia que se utilizará para llevar a cabo la recuperación ante un evento de desastre, basadas en prioridades, tiempo e impacto.
- Desarrollar un estudio de caso para retroalimentar el trabajo de investigación y mejorar la estrategia propuesta.

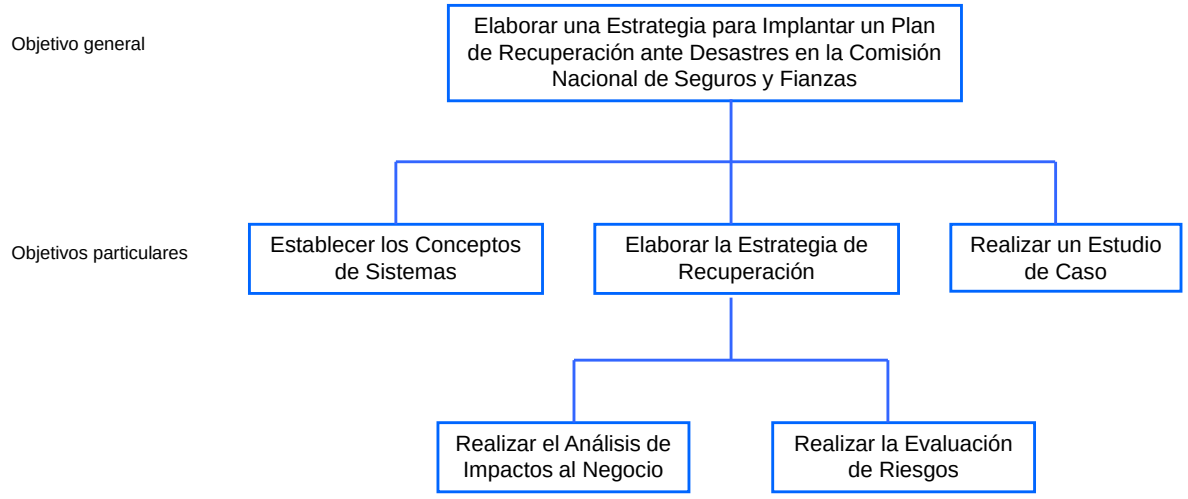


Figura 2. Árbol de objetivos

Supuestos

- Una Estrategia para Implantar un Plan de Recuperación ante Desastres en la Comisión Nacional de Seguros y Fianzas permitirá una respuesta rápida ante una declaración de desastre, logrando una recuperación efectiva y mitigando los efectos causados por éste mediante la adecuada planeación y control.
- De esta forma se garantizará que los servicios de Sistemas Informáticos que provee la Dirección General de Informática (DGI) al exterior y los procesos internos críticos operen a un nivel aceptable.

Justificación

En los últimos años, la CNSF ha incrementado su Infraestructura Tecnológica en lo relativo a recursos de cómputo y de Sistemas Informáticos con la finalidad de impulsar el desarrollo de los sectores asegurador y afianzador, así como profundizar en la modernización del marco de regulación y supervisión de dichos sectores[1]. Por tanto, se han convertido en activos críticos para su funcionamiento y, resulta prioritario contar con los elementos necesarios para limitar su pérdida así como su recuperación.

Las Direcciones de Soporte y de Sistemas, ambas dependientes de la Dirección General de Informática, son las responsables de evaluar y seleccionar las tecnologías de información más convenientes, para adquirirlas, integrarlas y manejarlas en la CNSF.

La Dirección de Soporte tiene como función determinar las normas y procedimientos de respaldo, para asegurar la continuidad en la operación de los sistemas, en caso de alguna falla. Así como de facilitar la recuperación de información en caso de contingencia, minimizando la pérdida de información debida a algún siniestro.

La Planeación de la Continuidad del Negocio es una parte esencial del funcionamiento de cualquier organización moderna que considera a sus clientes como elemento fundamental para su operación. Con tantos desastres potenciales que pueden ocurrir en una organización en cualquier momento, parece poco prudente no tomar medidas para prepararse y tratar de prevenir los efectos devastadores de estas catástrofes.

El primer paso para el establecimiento de un plan de continuidad del negocio es la creación del plan de recuperación ante desastres, el cual, como se mencionó anteriormente, es un proceso de recuperación que cubre los datos, el hardware y el software crítico; esto es, está enfocado principalmente a Tecnología de la Información.

La forma tradicional en la que se elabora un DRP, en ocasiones, da como resultado planes de alto nivel, sin mucho detalle, inclusive validados por los responsables de los procesos de negocio y de aplicaciones de la empresa en la que se realicen.

Varias son las causas que originan este resultado, destacándose las siguientes:

- Empleo de planes de otras organizaciones, basados en condiciones y requerimientos ajenos.
- Planes no ajustados a las necesidades de la organización, que impiden establecer la respuesta más adecuada en caso de desastre.
- Planes dirigidos sólo hacia las áreas de TI, que impiden considerar tanto activos informáticos como personal que gestiona operaciones críticas fuera de éstas.
- No se estable una responsabilidad conjunta entre el personal directivo, de TI y los propietarios de los procesos de negocios.

[1] Objetivos principales de las modificaciones a la Ley General de Instituciones y Sociedades Mutualistas de Seguros y a la Ley Federal de Instituciones de Fianzas, publicadas en el Diario Oficial de la Federación el 16 de enero de 2002.

- No se legitima la implantación del DRP.

Existen múltiples beneficios de la Planeación de la Continuidad del Negocio en una organización. No sólo los datos, hardware, software, etc., estarán mejor protegidos, las personas que componen la organización serán mejor salvaguardadas en caso de que ocurra un desastre. Además, los empleados serán informados y habrán ensayado las acciones a tomar para inmediatamente iniciar el proceso de recuperación y garantizar la continuidad del negocio.

De este modo, poniendo en práctica los planes de continuidad del negocio, la organización ahora puede prepararse para la mayoría de los desastres potenciales, ayudar a asegurar que será capaz de mantener la continuidad de sus prácticas de negocios y reducir o incluso cuando sea posible eliminar su efecto.

Además de los beneficios mencionados, las siguientes también son ventajas de la Planeación de la Continuidad del Negocio:

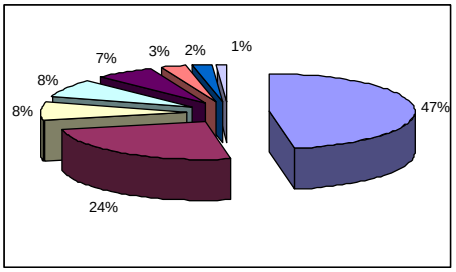
- Si no lo es ya, la organización muy pronto estará obligada a incorporar algún tipo de planeación de BCM dentro de sus políticas ya sea por estándar corporativo o legislación gubernamental.
- Las compañías de seguros pueden reducir las primas correspondientes a los seguros contratados.
- El proceso de evaluación de debilidades potenciales y planeación de cómo hacer frente a lo que podría salir mal, a menudo ofrece a la dirección la oportunidad de obtener una mejor comprensión de sus negocios y, en última instancia, ayudar a la organización a identificar maneras de fortalecer cualquier deficiencia. Con frecuencia, el valor más grande e inmediato del proceso de Planeación de Continuidad del Negocio es la conciencia que se gana de los detalles del negocio y no necesariamente la racionalización de la forma de manejar los desastres, se crea conciencia de formas útiles para mejorar una organización, a veces incluso en zonas que anteriormente no habían sido consideradas.
- Hará a la organización más sólida, fortaleciéndola no sólo contra los grandes problemas, sino también ayudándola a hacer más pequeños los problemas que pudieran causar interrupciones en la continuidad, a través de una planeación detallada.
- Mostrará a los inversionistas que se toma en serio los negocios, que se está preparado y se desea mantener la productividad a pesar de dificultades. Esta preparación también mostrará al personal que se tiene en mente sus empleos y bienestar.
- Informar a los clientes que se tiene un plan de continuidad del negocio, que se han tomado medidas para garantizar la continuidad de la productividad para que se puedan mantener los compromisos con ellos, les informa que se considera la prestación de un servicio de calidad como alta prioridad lo cual se convierte en confianza en el negocio.
- Ayuda a proteger la imagen, marca y reputación de la organización. Ser bien conocida como una empresa confiable es siempre bueno para los negocios.
- Puede reducir significativamente las pérdidas, inclusive si la organización se ve afectada por un desastre.

Por su parte, el Enfoque de Sistemas puede ser aplicado en el estudio de las organizaciones planteando una visión inter, multi y transdisciplinaria que ayudará a analizar y desarrollar a la empresa de manera integral permitiendo identificar y comprender con mayor claridad y profundidad los problemas organizacionales, sus múltiples causas y consecuencias. Así mismo, viendo a la organización como un ente integrado, conformada por partes que se interrelacionan entre sí a través de una estructura que se desenvuelve en un entorno determinado, se estará en capacidad de poder detectar con la amplitud requerida tanto la problemática, como los procesos de cambio que de manera integral, es decir a nivel humano, de recursos y procesos, serían necesarios de implantar para tener un crecimiento y desarrollo sostenibles y en términos viables en un tiempo determinado.

Impacto de desastres naturales o causados por personas

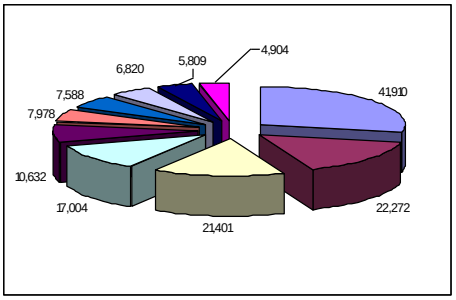
A fin de justificar con datos estadísticos la necesidad de contar con un DRP en la CNSF, a continuación se presentan una serie de gráficas que ilustran el impacto de desastres naturales o causados por personas sobre negocios de Estados Unidos de América.

Causas de desastres mayores en Estados Unidos de América en el período 1986-2005 (Hartwig, 2007).



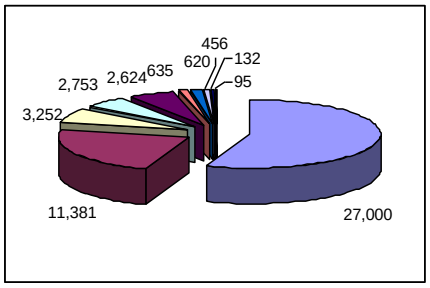
- Huracanes y tormentas tropicales
- Tornados
- Tormentas invernales
- Terrorismo
- Terremotos y otros acontecimientos geológicos
- Viento, granizo o inundaciones
- Incendios
- Trastornos civiles, daños causados por agua y servicios públicos

Las diez catástrofes más costosas en Estados Unidos de América, pérdida en millones de USD (III, 2007).



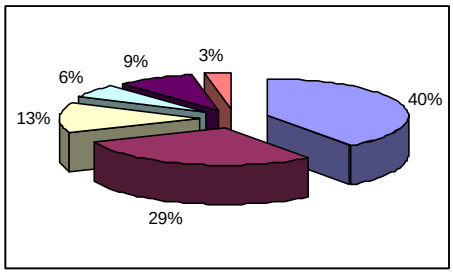
- Huracán Katrina
- Huracán Andrew
- Ataques al World Trade Center y al Pentágono
- Terremoto en Northridge, CA
- Huracán Wilma
- Huracán Charley
- Huracán Iván
- Huracán Hugo
- Huracán Rita
- Huracán Frances

Los diez terremotos más costosos en Estados Unidos de América, pérdida en millones de USD (III, 2007)



- Northridge, CA
- Bahía de San Francisco; Loma Prieta, CA
- Alaska y la costa oeste de Estados Unidos
- San Fernando, CA
- Washington, Oregon
- Sur de California, principalmente en Los Ángeles-Pasadena-Whittier
- Long Beach, CA
- Kern County, CA
- Sur de California; Landers-Joshua Tree-Big Bear
- Costa Norte de California; Petrolia-Eureka

Causas de pérdida de datos en computadoras personales (SLS, 2000)



- Falla de hardware
- Error humano
- Corrupción de software
- Virus en computadoras
- Robo
- Destrucción de hardware

Atentados 9/11

Como ejemplo puntual del impacto de un desastre tenemos los atentados terroristas del 11 de septiembre de 2001 a las Torres Gemelas del World Trade Center de Nueva York, figura 3; los cuales, causaron estragos en vidas, destruyeron edificios y desestabilizaron seriamente la economía estadounidense. Perjudicaron los negocios. La bolsa cesó operaciones. En Europa los mercados permanecieron abiertos, pero con descensos superiores al 6%.

Fig 3. Atentados del 9/11 al Wolrd Trade Center de Nueva York

Los ataques tuvieron un impacto significativo en el mercado estadounidense y mundial. La Reserva Federal redujo temporalmente sus contactos con bancos por la falta del equipo perdido en el distrito financiero de Nueva York. En horas se recuperó el control sobre el suministro de dinero, con la consecuente liquidez para los bancos. Los índices bursátiles New York Stock Exchange (NYSE), American Stock Exchange y NASDAQ no abrieron el 11 de septiembre y permanecieron cerrados hasta el 17 de ese mismo mes. Los sistemas del NYSE no fueron dañados por el ataque, pero los daños en las líneas telefónicas del sistema financiero del World Trade Center impidieron que funcionaran.

Cuando los mercados reabrieron el 17 de septiembre de 2001, tras el mayor paro desde la Gran Depresión, el índice Dow Jones Industrial Average cayó 684 puntos (7.1%), hasta 8,920, en su mayor caída en un solo día. Al final de la semana, el Dow Jones había perdido 1,369.7 puntos (14.3%), su mayor caída en una semana. Desde entonces Wall Street permanece protegido contra un atentado terrorista.

Alcance

La elaboración tradicional de un Plan de Recuperación ante Desastres limita su estudio al departamento de Tecnología de la Información; en este caso, aplicaría únicamente a la Dirección General de Informática (DGI). Por lo que se considerarían tanto los procesos de los que es responsable, como aquellos, en los que no siéndolo mantiene el resguardo de los activos (datos, aplicaciones y/o hardware) que los soportan. Así mismo, contemplaría los recursos humanos responsables de los mismos. Sin embargo, con el fin de considerar todos los procesos críticos (sustantivos y de apoyo) de la CNSF se considerará a los departamentos de Operación Institucional, Jurídico y Administrativo. Adicionalmente, es importante mencionar que el proyecto cuenta con el apoyo de la Alta Gerencia para su desarrollo.

La estrategia propuesta para implantar un DRP en la CNSF considerará el Enfoque de Sistemas para realizarlo de manera exitosa.

La selección de los procesos y del personal se determina en función del papel que desempeñan en la consecución de los objetivos operativos y estratégicos de la Comisión.

La estrategia de recuperación brindará una propuesta de infraestructura tecnológica mínima necesaria, así como una relación del personal y proveedores indispensables para dar continuidad a la operación de TI en un site alterno.

En la figura 4 se presenta el mapa conceptual de los elementos generales contemplados en la estrategia para implantar un DRP en la CNSF.

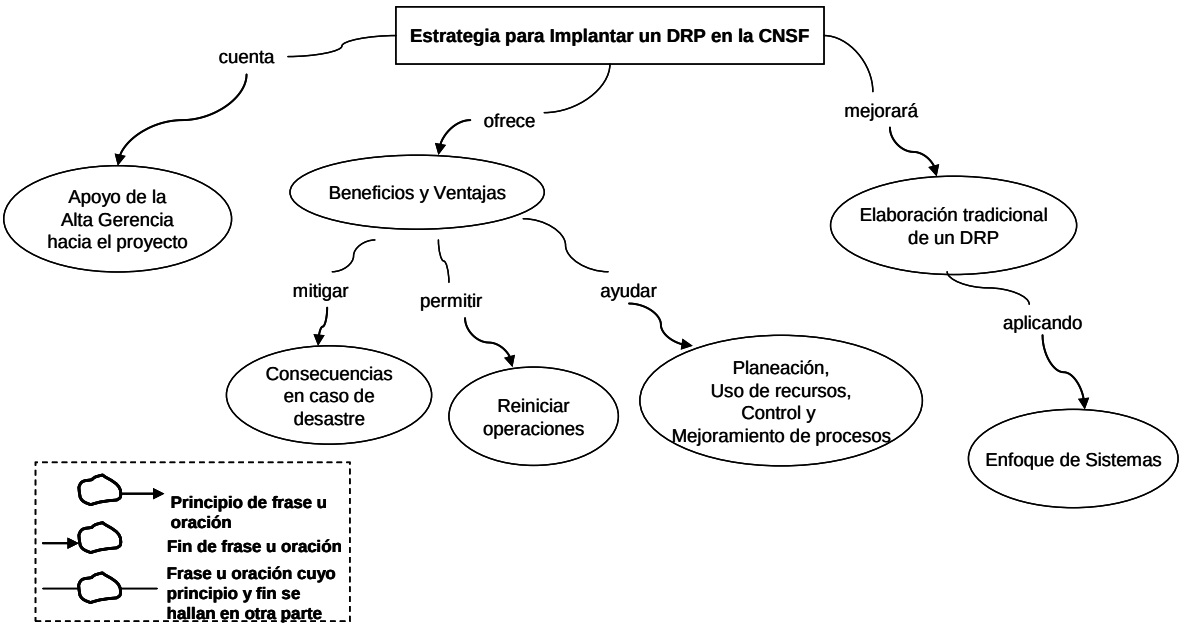


Figura 4. Mapa conceptual de la estrategia para implantar un DRP en la CNSF

CAPÍTULO 2. MARCO CONCEPTUAL DE REFERENCIA

2.1 Estándares Internacionales

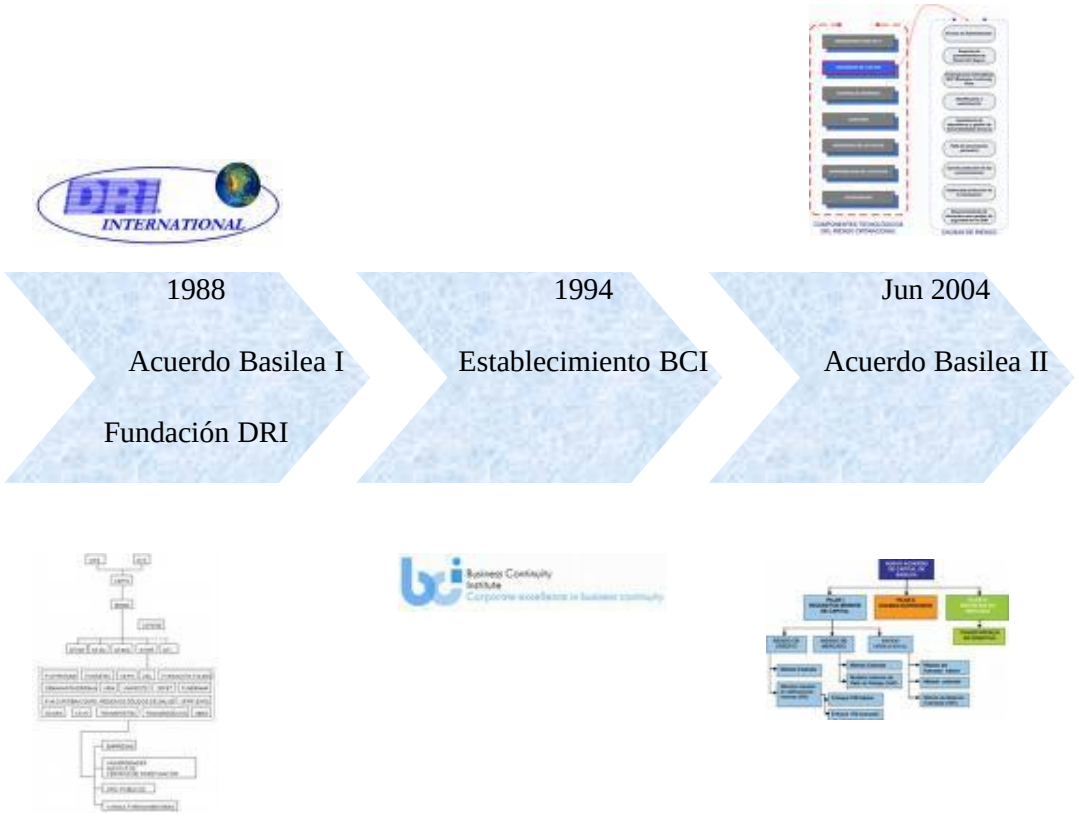


Figura 5. Evolución de los estándares internacionales

Basilea I

En 1988, el Comité de Basilea[2] publicó el primero de los Acuerdos, un conjunto de recomendaciones alrededor de una idea principal: establecer un techo para el valor de los créditos que puede conceder una entidad bancaria en función de su capital propio, que se fijó en 12.5 veces el valor de éste último.

Este acuerdo era una recomendación: cada uno de los países signatarios, así como cualquier otro país, quedaba libre de incorporarlo en su ordenamiento regulatorio con las modificaciones que considerase oportunas. Entró en vigor en más de cien países.

[2] Integrado por los gobernadores de los bancos centrales de Alemania, Bélgica, Canadá, España, USA, Francia, Italia, Japón, Luxemburgo, Holanda, el Reino Unido, Suecia y Suiza.

DRI International

El Instituto Internacional de Recuperación de Desastres (por sus siglas en inglés DRI International) es un organismo sin fines de lucro fundado en 1988 con el fin de desarrollar una base de conocimientos en la planeación de contingencias y el manejo de riesgos. Administra los principales programas de educación y certificación de la industria para aquellos comprometidos con la práctica de la planeación y administración de la Continuidad del Negocio. Tiene como objetivo principal promover un conocimiento común de la planeación de la Continuidad del Negocio / Recuperación ante Desastres mediante la educación, asistencia y publicación del recurso estándar.

Instituto de Continuidad del Negocio

El Instituto de Continuidad del Negocio (por sus siglas en inglés BCI) se creó en 1994 para permitir que cada uno de sus miembros obtuviera orientación y soporte de compañeros profesionales de continuidad del negocio. El Instituto actualmente cuenta con más de 4,000 miembros en más de 85 países.

En 2007 se dio el lanzamiento de Asociación BCI permitiendo a las organizaciones trabajar estrechamente con este instituto para realizar su misión general:

Promover el arte y la ciencia de la gestión de continuidad del negocio a nivel mundial.

El papel más amplio del BCI y de la Asociación BCI es promover los más altos estándares de competencia profesional y ética comercial en el suministro y el mantenimiento de la continuidad de las actividades de planeación y servicios.

Basilea II

Basilea II es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, publicado inicialmente en Junio de 2004, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

En los últimos años, la industria financiera ha sufrido sustanciales pérdidas por fallos operacionales, bajo un escenario de continuos avances tecnológicos y mayor complejidad de la operativa bancaria y de los mercados financieros. El Comité de Basilea, no ajeno a esta situación, en junio de 2004, publicó un Nuevo Acuerdo de Capital en el que incluía requerimientos por riesgo operacional.

El Acuerdo de Basilea II, con respecto a los riesgos financieros en general y al riesgo operacional en particular, no se encamina meramente hacia la búsqueda del cumplimiento de una regla o unos estándares de medición; implícitamente el Nuevo Acuerdo pretende un avance y un mayor rigor en la gestión y control de riesgo y capital en las entidades financieras. Así, el Acuerdo de Basilea II contribuye a evitar que nos sigamos sorprendiendo de lo que sabemos que va a pasar y a estar preparados para lo esperado e inesperado (Caruana, 2005).

2.2 Conceptos de Gestión de Continuidad del Negocio

Gestión de Continuidad del Negocio (por sus siglas en inglés *BCM*) es un proceso de gestión holístico que identifica los impactos potenciales que amenazan a una organización y proporciona un marco para la construcción de un plan de recuperación con la capacidad para una respuesta efectiva que salvaguarde los intereses de sus stakeholders clave, reputación, marca y actividades de creación de valor.

El objetivo principal de la Gestión de Continuidad del Negocio es permitir a los ejecutivos continuar manejando las operaciones del negocio bajo condiciones adversas, mediante la introducción de estrategias de recuperación adecuada, objetivos de recuperación, continuidad del negocio, consideraciones de gestión de riesgos operacionales y planes de gestión de crisis.

El modelo de Gestión de Continuidad del Negocio, se basa en las mejores prácticas aceptadas internacionalmente por instituciones reconocidas en el mercado como son el Instituto de Recuperación ante Desastres en Estados Unidos y el Instituto de Continuidad del Negocio en el Reino Unido.

2.2.1 Planeación de Continuidad del Negocio

Planeación de Continuidad del Negocio (por sus siglas en inglés *BCP*) es la forma en que una organización se prepara para recuperarse ante un desastre. Se trata de un acuerdo hecho entre la dirección y el personal clave acerca de las medidas que se adoptarán para ayudar a la organización a recuperarse en caso de que ocurra un desastre. Estos programas preparan para enfrentar múltiples problemas. Tiene como objetivo crear planes detallados para exponer claramente las acciones que una organización o un miembro en particular tomará para ayudar a recuperar/restaurar cualquiera de sus operaciones críticas que puedan haber sido ya sea total o parcialmente interrumpidas durante o después de un desastre (y que se producen dentro de un determinado período de tiempo).

En términos concretos, un Plan de Continuidad del Negocio es la forma en que una organización se protege contra futuros desastres que pudieran dañar su salud a largo plazo o el cumplimiento de su misión principal. Estos planes deben tener en cuenta los desastres que pueden ocurrir en diversos niveles geográficos ya sea locales o regionales, así como catástrofes a nivel nacional como incendios, terremotos o pandemias. Así mismo, las estrategias para su desarrollo deben evolucionar y ajustarse a los nuevos posibles desastres que requieren de recuperación, incluyendo desde virus tecnológicos hasta ataques terroristas. El objetivo final es ayudar a acelerar la recuperación de las funciones críticas de una organización y la mano de obra después de algún tipo de desastre. Este tipo de planeación

avanzada puede ayudar a una organización a minimizar la cantidad de pérdidas y el tiempo de inactividad así como crear su mejor y más rápida oportunidad para recuperarse después de un desastre.

La alta Gerencia tiene un rol activo en la continuidad de negocio y será responsable de ciertos planes como el de manejo de crisis. También tiene la responsabilidad de normar lo referente al antes, durante y después de la contingencia y asignar para ello los recursos necesarios sin pensar necesariamente en el retorno de inversión (por sus siglas en inglés ROI), valor que no se puede calcular y no existe hasta que ocurra la contingencia. Sin embargo, es conveniente mencionar que en lo que respecta a continuidad del negocio, el apoyo político no es suficiente, todos los empleados son igualmente responsables.

Contar con plan estratégico permite tener un horizonte claro de a dónde vamos y entender que el logro de la excelencia en continuidad del negocio no es inmediato sino progresivo.

2.2.2 Plan de Recuperación ante Desastres

Recuperación ante Desastres es el proceso que una organización utiliza para recuperar el acceso a su software, datos y/o hardware necesarios para reanudar las funciones críticas del negocio después de un desastre ya sea natural o causado por personas; sin embargo, no se puede olvidar el elemento vital de la mano de obra que compone una gran parte de cualquier organización. El incendio de un edificio podría afectar principalmente el almacenamiento de datos vitales, mientras que una epidemia es más probable que tenga un efecto en el personal. Ambos tipos de desastres deben considerarse, de tal forma que las organizaciones deben incluir en sus DRP's cómo van a hacer frente a la repentina e inesperada pérdida de personal clave, así como la manera de recuperar sus datos.

Así mismo, un DRP ayuda en la Planeación, el uso de recursos, el control y mejoramiento de procesos. Los elementos anteriores se muestran de manera gráfica en la figura 6 a través de un mapa conceptual.

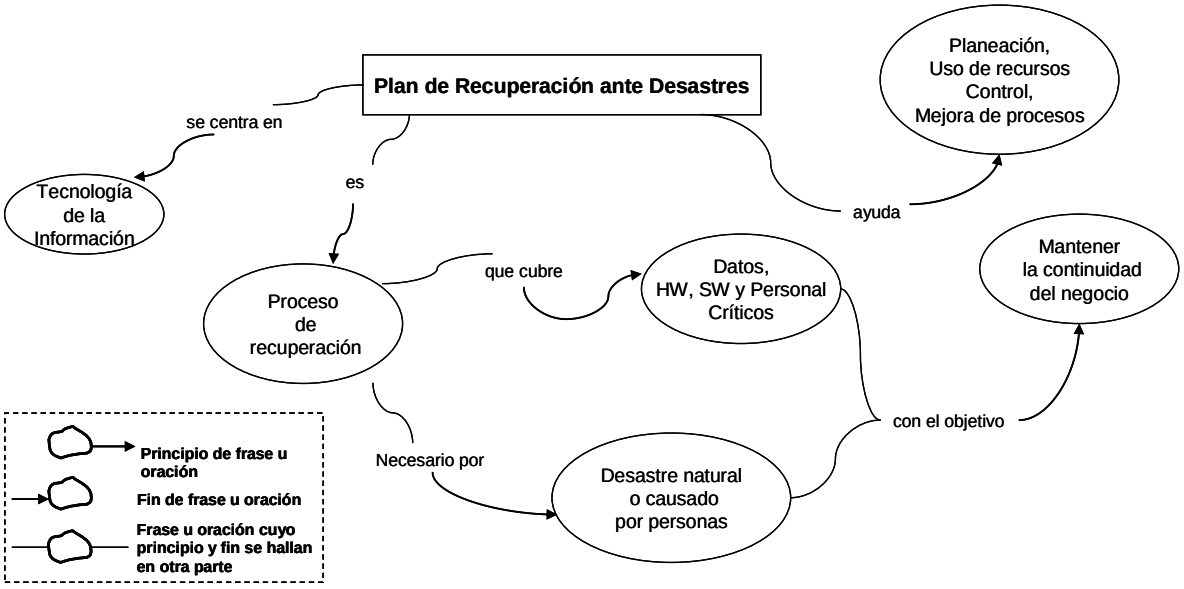


Figura 6. Mapa conceptual de un plan de recuperación ante desastres

Es de vital importancia que sean cuidadosamente establecidos, detallados y documentados para evitar dolores de cabeza al personal de la organización en tiempos de desastre (DRI, 2009). Así mismo deben practicarse con regularidad a fin de que los actores principales estén familiarizados con las acciones específicas que deben hacer en caso de que ocurra un desastre mejorando el tiempo de recuperación y reduciendo al mínimo el tiempo en que las funciones normales de negocio se ven interrumpidas. También deben ser adaptables y actualizarse periódicamente; por ejemplo, si nuevo personal, una sucursal, hardware o software se agregan a la organización, entonces deben incorporarse rápidamente al plan.

En los planes de recuperación ante desastres, los sistemas TI se consideran como apoyo a los procesos comerciales. Para poner en marcha sus sistemas informáticos las organizaciones necesitan entrenar regularmente a sus ingenieros de informática. También, debe prestarse especial atención para la formación de los nuevos empleados que tendrán un papel decisivo en este proceso.

Se debe tener presente que no todos los riesgos de desastres pueden ser eliminados por completo, pero si es posible tomar medidas preventivas y correctivas enfocadas a evitarlos o a reducir lo más posible su probabilidad de ocurrencia, así como minimizar los efectos del desastre en caso de que este ocurra. Para lograrlo es necesario estudiar y controlar en la medida deque sea posible las causas y efectos que se pudieran presentar.

¿Qué constituye un Desastre?

Un desastre es un evento súbito, imprevisto y perjudicial que crea una incapacidad para que una organización proporcione las funciones críticas de negocio por un período indeterminado de tiempo, resultando en un gran daño o pérdida para ésta.

En la figura 7 se presentan dos fotografías de desastres naturales: terremoto e inundación.

Figura 7. Desastres naturales

2.2.3 Riesgo Operacional

El riesgo operacional no es un riesgo nuevo; de hecho, es un riesgo inherente a cualquier negocio y no es exclusivo de la actividad financiera. Sin embargo, la preocupación por éste ha crecido considerablemente en los últimos años, tanto por parte de las entidades financieras como por parte de los supervisores.

Además, se tiene la percepción de que ha sido un riesgo creciente en la última década, debido, entre otros factores, a la mayor dependencia de las entidades en los procesos informáticos, al desarrollo del comercio electrónico y a la aparición de nuevas técnicas de mitigación de riesgos. En definitiva, nos encontramos ante un sistema financiero con una complejidad cada vez mayor, que da lugar a que estos eventos de riesgo operacional sean más probables y que, además, en caso de que ocurran, tengan un mayor impacto.

Como respuesta, a la preocupación por el riesgo operacional, las entidades financieras han ido incrementando paulatinamente los recursos asignados a este riesgo, pasando de la simple mejora de los sistemas de control al desarrollo de modelos de medición y gestión del riesgo operacional que intentan obtener una estimación razonable del impacto de futuras pérdidas.

El Comité de Basilea ha venido a recoger la preocupación y la importancia que los supervisores otorgan a este riesgo, al haber introducido en el Nuevo Acuerdo de Capital de Basilea unas exigencias de capital explícitas por riesgo operacional.

Basilea II define el riesgo operacional como el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo de reputación.

2.3 Elaboración de un Plan de Recuperación ante Desastres

Existen varias opciones disponibles a utilizar por las organizaciones una vez que deciden empezar a crear su plan de recuperación ante desastres. La primera y más accesible fuente son los conocimientos y la experiencia que tienen los gerentes. Para las organizaciones que no cuentan con este tipo de experiencia en casa, existen una serie de opciones externas, como consultores entrenados y software especialmente diseñado.

Una buena práctica utilizada por los responsables de las organizaciones es usar una plantilla de plan de recuperación ante desastres. Aunque las plantillas no pueden cubrir todas las necesidades específicas de cada organización, son un buen elemento para comenzar la preparación ya que ayudan a que el proceso de preparación sea más simple y sencillo. Así mismo, ofrecen orientación e incluso pueden revelar aspectos que podrían, de otra forma, ser olvidados.

Un plan de recuperación ante desastres es uno de los documentos más importantes (si no, el más importante) que tiene una organización. Este es el documento que toda la organización requiere para capacitación, orientación y protocolo en caso de una crisis, especialmente una que podría causar disrupciones mayores en sus funciones del día a día, o podría tener un marcado afecto en su capacidad para mantener la productividad. Este documento ayudará a la organización a recuperarse más rápidamente e incluso puede ayudarla a evitar la pérdida de ingresos.

Incluso, considerándolo importante, muchas organizaciones se ven tentadas a posponer la creación de su plan de recuperación ante desastres, porque el proceso puede sentirse un poco abrumador. Por esta razón, algunas organizaciones, como el Disaster Recovery proporcionan plantillas para ayudar en la creación de este tipo de planes. Usándolas se aprovecha la información de algunos de los más experimentados expertos de la industria de TI, misma que puede integrarse con la experiencia y los conocimientos del personal propio.

Cada negocio y sus necesidades específicas son únicos. Un plan de recuperación ante desastres general no es adecuado para todos.

En la actualidad, se cuenta con software de fácil uso e inclusive con acceso a través de Internet que sirve no sólo para documentar, sino que también permite planear y gestionar todas las interrupciones y las situaciones de recuperación ante desastres. Ayuda a realizar el análisis de vulnerabilidades, recomendar estrategias y permite el desarrollo de la continuidad del negocio y planes de recuperación ante desastres. También incluye la notificación de emergencia y gestión de la documentación.

2.3.1 Iniciando un Plan de Recuperación ante Desastres

El proceso de creación puede parecer abrumador al principio, pero este esfuerzo podría un día salvar a la organización. Los desastres pueden adoptar muchas formas y tamaños y pueden ocurrir en cualquier momento. A la sombra de los compromisos diarios hacer un plan de recuperación ante desastres puede parecer engorroso y no prioritario. Pero cuando un desastre ocurre, el proceso no esperará hasta que sea demasiado tarde, inmediatamente se convierte en una prioridad absoluta.

El primer paso en planeación de recuperación ante desastres es concientizarse de la necesidad de este tipo de preparación. Las organizaciones que valoran sus negocios necesitan establecer y mantener un sistema eficaz de planes de recuperación ante desastres. Cuando estos planes se necesiten, pueden minimizar las interrupciones en el funcionamiento normal de la operación del negocio y limitar el alcance de los daños e interrupciones en la productividad.

La responsabilidad de configurar estos planes corresponde al personal directivo. Ellos deben organizar y mantener un esquema claro de qué acciones quieren que se tomen y qué empleados necesitan desempeñar algún papel en el proceso de recuperación ante desastres.

Los planes de recuperación ante desastres deben ser conocidos y ensayados por todos los que tendrán un papel en el proceso de recuperación. Todos los directivos y el personal deben estar concientes del plan de recuperación ante desastres y de lo que se requiere de ellos en caso de que uno de estos ocurra.

Existen varios elementos fundamentales que deben incluirse en cualquier plan de recuperación, tales como: el protocolo de respuesta ante la emergencia, los procedimientos para realizar respaldos de los datos, el software, etc., así como las líneas detalladas para personal que debe participar en el proceso de recuperación y qué medidas concretas se deben adoptar con el fin de que la organización regrese a su funcionamiento normal, con la menor cantidad de gastos y en el menor lapso de tiempo posible.

Cuando una organización está lista para empezar a crear su plan de recuperación ante desastres, debe realizar al menos las siguientes actividades:

- Fijar metas para el plan; por ejemplo, ¿Qué debería de cumplir? y ¿En qué plazos de tiempo?
- Crear una lista exacta y actualizada del personal de cada uno de sus departamentos.
- Hacer una lista de todas las aplicaciones esenciales, el personal esencial para operarlas y determinar con qué frecuencia la información debe ser respalda.
- Realizar un inventario físico de todos los elementos necesarios para gestionar la red (LAN o WAN).
- Tomar nota de los procedimientos involucrados en el respaldo se sus servicios de información.
- Realizar un esquema detallado de todos los procedimientos de recuperación ante desastres que deben hacerse.

Hacer un plan de recuperación requerirá de esfuerzo, pero puede simplificarse con el apoyo de folletos explicativos y de plantillas. Estas abarcan una serie de temas importantes que las organizaciones deben tener en cuenta al crearlo. Así mismo, puede emplearse el software de gestión de continuidad del negocio.

2.3.2 Análisis de Impactos al Negocio

Análisis de Impactos al Negocio (por sus siglas en inglés BIA) es un proceso para determinar las aplicaciones críticas del negocio.

Aplicación crítica = f (criticad del proceso que la soporta)

La criticidad está en función de los conceptos de Recuperación, Impacto e Interrelación (EMC^2, 2008); los cuales, se evalúan a través de una asignación proporcional ponderada por el grado de importancia de cada uno de estos, de acuerdo a la estrategia funcional y operativa de la Organización.

Tiers de aplicación

Los tiers de aplicación son los grupos más significativos de aplicaciones. La categoría en la que se ubican está en función de su importancia para la operación de los procesos de negocio.

Estos tiers son la base para el establecimiento de los Acuerdos de Nivel de Servicio (por sus siglas en inglés SLA´s) entre las áreas de tecnología y los procesos de negocio sobre las características de disponibilidad de la información que requieren para operar y que es obtenida a través de las aplicaciones de TI que soportan los procesos.

Los criterios utilizados para la definición de los tiers de aplicación son el tiempo objetivo de recuperación (por sus siglas en inglés RTO), que establece el tiempo que transcurrirá entre la caída de la aplicación y su recuperación, y el punto objetivo de recuperación (por sus siglas en inglés RPO), que define el grado de actualización de la información con que será recuperada la aplicación, como se muestra en la figura 8.

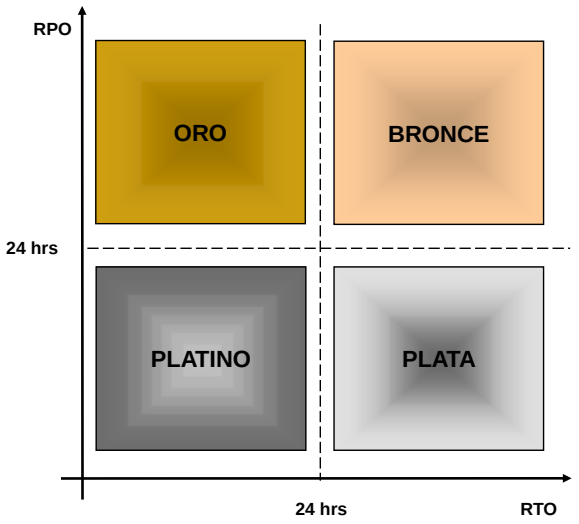


Figura 8. Tiers de aplicación

Mediante esta categorización de aplicaciones, es posible determinar cuáles tienen mayores exigencias, en características de disponibilidad y respaldo, hacia la estrategia de DRP que se establezca.

Además, este análisis permite determinar los activos que las soportan, como lo son el Hardware y las telecomunicaciones; así como otros elementos críticos de operación: herramientas y registros vitales.

Finalmente, proporciona información clave a la dirección para tomar decisiones estratégicas relacionadas con la recuperación y la continuidad del negocio.

2.3.3 Evaluación de Riesgos

Con el fin de crear el plan más efectivo para recuperarse después de un desastre, una organización debe considerar, en primer lugar y tanto como sea posible, de los desastres potenciales cuáles les podrían ocurrir y cómo cada uno de estos podría impactar la continuidad del negocio y, a continuación averiguar cómo se ocupará de cada crisis en caso de producirse.

Para hacer sus esfuerzos más eficaces, los ejecutivos y los miembros de la junta directiva deben considerar todos los posibles escenarios cuando se analizan los riesgos potenciales a los que la organización podría hacer frente. Esto significa que todos los posibles riesgos deben contemplarse, desde los peligros mundanos como fallas del suministro eléctrico, hasta eventos extremadamente peligrosos como actos de guerra o ataques terroristas. Como el objetivo de un plan de recuperación ante desastres es definir qué acciones se tomarán en caso de que una organización experimente un desastre, estas crisis no sólo deben ser contempladas, sus posibles impactos deben ser evaluados y determinar qué medidas se adoptarán para superar el impacto, así como si el plan de recuperación ante desastres es realmente efectivo y práctico.

Desafortunadamente, las evaluaciones de recuperación ante desastres a veces pueden llegar a ser muy complejas. A continuación, se incluye una breve lista de algunos de los acontecimientos disruptivos que podrían tener un efecto en las operaciones normales y que deben tenerse en cuenta al preparar un plan de recuperación ante desastres.

- Daño de disco duro,
- Incendios de edificios,
- Inundaciones,
- Fallas en el suministro eléctrico,
- Fallas en Internet,
- Fallas en líneas de datos,
- Terremotos,
- Ataques terroristas,
- Actos de guerra,
- Epidemias y
- Fallas en el transporte debido a condiciones meteorológicas, huelgas o algún otro acontecimiento.

Estos dos últimos podrían causar una repentina y significativa disminución del personal, incluidos aquellos empleados que mantienen posiciones de vital importancia.

Es importante tener en cuenta que esta lista de posibles desastres está lejos de ser exhaustiva y no incluye muchos de los eventos especiales relativos a una organización en particular. Por ejemplo, si fuera una pequeña empresa, eventos menores pueden tener un mayor impacto en el personal, particularmente en quien cuenta con los conocimientos necesarios para llevar a cabo determinadas tareas.

2.3.4 Estrategia de Recuperación

En esta etapa se determina la estrategia de disponibilidad y recuperación que será proveída por el área de Tecnología de Información, la cual, estará en función de los criterios de recuperación (RTO y RPO) identificados por las áreas críticas de la Organización. Así mismo, se realiza una propuesta de los elementos necesarios para llevar a cabo tal recuperación.

Los tiers de aplicación, definidos durante el Análisis de Impactos al Negocio, permiten definir qué aplicaciones deben ser recuperadas en la menor ventana posible de tiempo, conservando la mayor cantidad de la información que se encontraba en la aplicación en el momento de la interrupción.

Las aplicaciones de la primera categoría o aplicaciones Platino, en términos de estrategias de respaldo, son las que requieren de una estrategia de mayor disponibilidad, con recuperación en el menor tiempo, lo que en términos prácticos debería constituir una baja caída, con un esquema que garantice un respaldo externo para todos los datos correspondientes.

Las aplicaciones de la segunda categoría u Oro, comparten la característica de mayor disponibilidad, pero su esquema de respaldo admite una mayor pérdida de datos, ajustándose al último respaldo efectuado; sin embargo, por tener características exigentes en lo relativo a los tiempos de recuperación, es necesario contar con este respaldo disponible para su restauración inmediata.

Las aplicaciones Plata requieren de un esquema de respaldo que garantice una baja pérdida de datos; sin embargo estas aplicaciones soportan procesos, que por sus características particulares, admiten una recuperación diferida de las aplicaciones de esta categoría. Por tanto estas aplicaciones aunque forman parte de la estrategia de mayor respaldo, sus requerimientos de recuperación serán establecidos en un tercer nivel de prioridad.

Las aplicaciones Bronce serán las aplicaciones de último nivel, por tanto tienen tiempos diferidos de recuperación y una restauración desde el último respaldo. Estos respaldos no requieren estar disponibles de forma inmediata, pero si estar resguardados de forma externa a las instalaciones principales de la Empresa.

Los tiers de aplicación establecidos en el BIA definen la prioridad de la recuperación más no directamente la secuencia de la misma. Son la base del diseño de la estrategia, pero la secuencia final de recuperación la establece la viabilidad técnica de la misma.

Las actividades necesarias para el desarrollo de un DRP de forma tradicional así como algunas de sus ventajas se muestran en la figura 9.

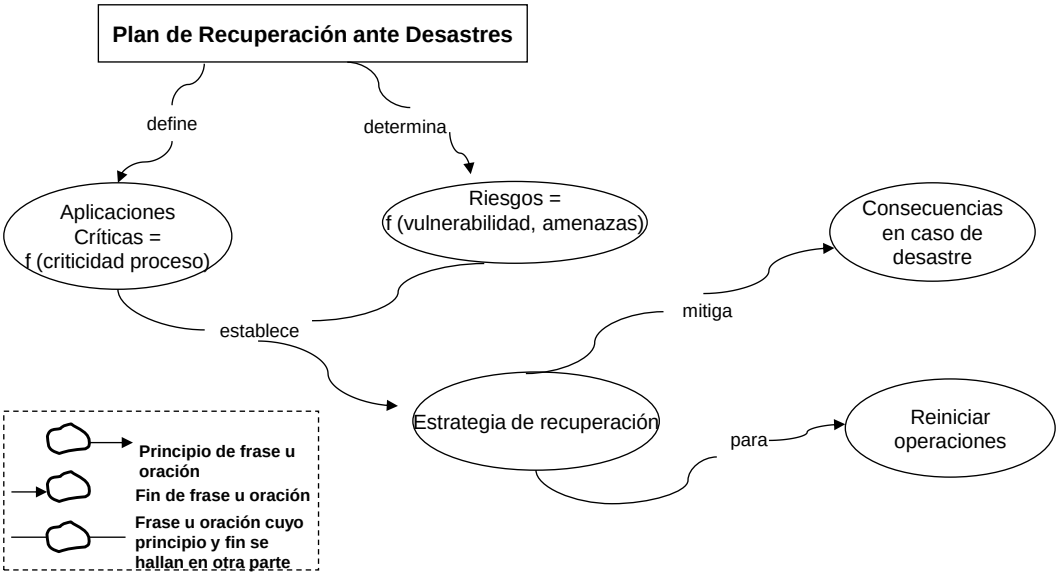


Figura 9. Mapa conceptual de la elaboración tradicional de un DRP

Compañías de Software de Gestión de Continuidad del Negocio

Lo importante a la hora de seleccionar y adquirir un software no es que sólo sirva para documentar, sino sobre todo que sirva para ayudar a la gestión de continuidad del negocio manteniendo todos los procedimientos actualizados al día, ya que de no estarlo se corre el riesgo de perder la empresa u organización. Y es que resulta complicado hacer gestión de continuidad del negocio a "mano" que a la larga es más costoso y sobre todo más riesgoso que utilizar un software.

En la tabla 1 se presentan ejemplos de compañías de software de gestión de continuidad del negocio.

Strohl Systems http://strohlsystems.com	En 1988 compró todos los derechos del software Livin Disaster Recovery Planning System (LDRPS®) y desde entonces se ha dedicado al diseño, desarrollo, comercialización y al soporte del software de continuidad del negocio, incluidos los servicios. En 1994, Strohl libera un nuevo producto de software, BIA Professional®, el primer programa de análisis de impacto del negocio basado en Windows.
Evergreen http://www.evergreen-data.com	Ha estado proporcionando soluciones de gestión de continuidad del negocio (BCM) en todo el mundo desde 1998. El software empleado para tal efecto es Mitigator.
SunGard http://www.sungard.com	SunGard se formó en 1982 como una división de Sun Oil Company. Ofrece servicios de recuperación ante desastres, de gestión de TI, de consultoría de disponibilidad de información y software de gestión de continuidad del negocio.
RecoveryPlanner.com http://www.recoveryplanner.com	Fundada en 1999 por expertos en la continuidad del negocio, recuperación ante desastres y gestión de crisis, ofrece servicios de planeación de continuidad del negocio y de recuperación ante desastres, apoyados en su software RPX.
CSCI **http://www.csc-inc1.com**	Proveedor desde 1977 de servicios de tecnología de la información para empresas de gobierno y comerciales. Algunas de sus soluciones incluyen: • Análisis de impactos al negocio. • Planeación e implementación de recuperación en caso de desastres

Tabla 1. Ejemplos de compañías de software de gestión de continuidad del negocio

2.4 Conceptos de Sistemas

A continuación se presentan los conceptos de sistemas, necesarios para definir e implantar la estrategia.

2.4.1 Teoría General de Sistemas

En tanto que anteriormente la ciencia trataba de explicar los fenómenos observables reduciéndolos al juego de unidades elementales, investigables e independientes una de otra, en la ciencia reciente aparecen actitudes que se ocupan de lo que un tanto vagamente se llama "totalidad", es decir, problemas de organización, fenómenos que no se pueden descomponer en acontecimientos locales, interacciones dinámicas manifiestas en la diferencia de conducta de partes aisladas o en una configuración superior, etc.; en una palabra, "sistemas" de varios órdenes, no comprensibles por investigación de sus respectivas partes aisladas. Concepciones y problemas de tal naturaleza han aparecido en todas las ramas de la ciencia, sin importar que el objeto de estudio sean cosas inanimadas, organismos vivientes o fenómenos sociales. Esta correspondencia es más llamativa en vista de que cada ciencia siguió su curso independiente, casi sin contacto con las demás y basándose todas en hechos diferentes y filosofías contradictorias. Esto indica un cambio general en la actitud y las concepciones científicas (Bertalanffy, 1968).

No sólo se parecen aspectos y puntos de vista generales en diferentes ciencias; con frecuencia hallamos leyes formalmente idénticas o isomorfas en diferentes campos. En muchos casos, leyes isomorfas valen para determinadas clases o subclases de "sistemas", sin importar la naturaleza de las entidades envueltas. Parece que existen leyes generales de sistemas aplicables a cualquier sistema de determinado tipo, sin importar las propiedades particulares del sistema ni de los elementos participantes.

Estas consideraciones conducen a proponer una nueva disciplina científica, que llamamos teoría general de los sistemas. Su tema es la formulación de principios válidos para "sistemas" en general, sea cual fuere la naturaleza de sus elementos componentes y las relaciones o "fuerzas" reinantes entre ellos.

De esta suerte, la teoría general de los sistemas es una ciencia general de la "totalidad", concepto tenido hasta hace poco por vago, nebuloso y semimetafísico.

De buenas a primeras, da la impresión de que la definición de sistemas como "conjuntos de elementos en interacción" fuera tan general y vaga que no hubiera gran cosa que aprender de ésta.

Sistemas cerrados y abiertos: limitaciones de la física ordinaria

La física ordinaria sólo se ocupa de sistemas cerrados, de sistemas que se consideran aislados del medio circundante. Ejemplos de estos son la fisicoquímica y la termodinámica. Sin embargo, encontramos sistemas que, por su misma naturaleza y definición, no son sistemas cerrados. Todo organismo viviente es ante todo un sistema abierto.

No ha sido sino hasta años recientes cuando se ha presenciado una expansión de la física orientada a la inclusión de sistemas abiertos. Esta teoría ha aclarado muchos fenómenos oscuros en física y biología, y ha conducido a importantes conclusiones generales, dos de las cuales se presentan a continuación:

La primera es el principio de equifinalidad. En cualquier sistema cerrado, el estado final está inequívocamente determinado por las condiciones iniciales; si éstas o el proceso se alteran, el estado final cambiará también. No ocurre lo mismo en los sistemas abiertos; en estos puede alcanzarse el mismo estado final partiendo de diferentes condiciones iniciales y por diferentes caminos.

Sobre la base de la teoría de los sistemas abiertos, la aparente contradicción entre entropía y evolución desaparece. En todos los procesos irreversibles la entropía debe aumentar. Por tanto, el cambio de entropía en sistemas cerrados es siempre positivo; hay continua destrucción de orden. En los sistemas abiertos, sin embargo, no sólo tenemos producción de entropía debida a procesos irreversibles, sino también entrada de entropía que bien puede ser negativa.

Información y entropía

Otra vía que está vinculada de cerca a la teoría de los sistemas es la teoría de la comunicación. La noción general en ésta es la de información. Una manera de medirla es en términos de decisiones. Esta medida de la información resulta ser similar a la de la entropía, o más a la de la entropía negativa. La entropía es una medida del desorden, de ahí que la entropía negativa o información sea una medida del orden o de la organización.

Otro concepto de la teoría de la comunicación y el control es el de retroalimentación, el mantenimiento homeostático de un estado característico o la búsqueda de una meta, basada en cadenas causales circulares y en mecanismos que devuelven información acerca de desviaciones con respecto al estado por mantener o la meta por alcanzar. La figura 10 representa un esquema sencillo de retroalimentación

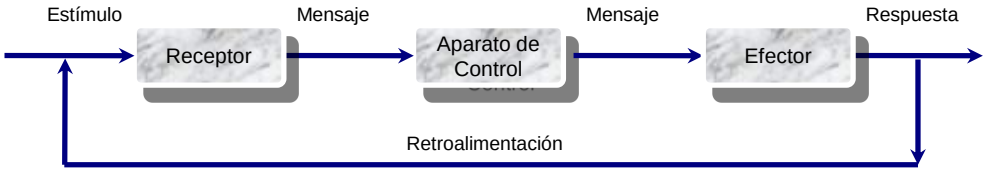


Figura 10. Esquema de retroalimentación

Los dispositivos de retroalimentación se emplean mucho en la tecnología para estabilizar determinada acción o la dirección de acciones hacia determinada meta: las desviaciones se retroalimentan, como información, hasta que se alcanza la meta o el blanco.

La teoría de la cibernética aspira a mostrar que mecanismos de naturaleza retroalimentadora fundamentan el comportamiento teleológico o intencionado en las máquinas construidas por el hombre, así como en los organismos vivos y en los sistemas sociales.

Causalidad y teleología

Desde el punto de vista mecanicista, nacido de la física clásica del siglo XIX, la única meta de la ciencia parecía ser analítica: la división de la realidad en unidades cada vez menores y el

aislamiento de líneas causales separadas. Así, la realidad física era descompuesta en puntos de masa o átomos, el organismo vivo en células, el comportamiento en reflejos, la percepción en sensaciones puntuales, etc.

Puede tomarse como característica de la ciencia moderna el que este esquema de unidades aislables actuantes según causalidad unidireccional haya resultado insuficiente. De ahí la aparición, en todos los campos de la ciencia, de nociones como las de totalidad, holismo, organismo, *Gestalt,* etc., que vienen a significar todas que, en última instancia, debemos pensar en términos de sistemas de elementos en interacción mutua.

Análogamente, las nociones de teleología y directividad parecían caer fuera del alcance de la ciencia y ser escenario de misteriosos agentes sobrenaturales o antropomorfos, o bien, tratarse de un seudo problema, intrínsecamente ajeno a la ciencia, mera proyección mal puesta de la mente del observador en una naturaleza gobernada por leyes sin propósito. Con todo, tales aspectos existen, y no puede concebirse un organismo vivo, no se diga el comportamiento y la sociedad humanos, sin tener en cuenta lo que, variada y bastante vagamente, se llama adaptabilidad, intencionalidad, persecución de metas y cosas semejantes.

Característico del presente punto de vista es que estos aspectos sean tomados en serio, como problemas legítimos para la ciencia; y también estamos en condiciones de procurar modelos que simulen tal comportamiento.

Ya se han mencionado dos ejemplos de estos modelos de comportamiento adaptativo. Uno es la equifinalidad y el otro, la retroalimentación.

El concepto teleológico debe considerarse como una forma de comportamiento definible en términos científicos y cuyas condiciones necesarias y mecanismos posibles pueden ser indicados.

¿Qué es Organización?

El concepto de organización también era ajeno al mundo mecanicista. Las cosas son distintas en la física moderna. Un átomo, un cristal o una molécula son organizaciones. En biología, los organismos son, por definición, cosas organizadas.

Características de la organización, trátese de un organismo vivo o de una sociedad, son nociones como las de totalidad, crecimiento, diferenciación, orden jerárquico, dominancia, control, competencia, etc.

Es posible definir tales nociones dentro del modelo matemático de un sistema: más aun, en ciertos aspectos pueden deducirse teorías detalladas que derivan los casos especiales a partir de supuestos generales. Sin embargo, hay muchos aspectos de organizaciones que no se prestan con facilidad a interpretación cuantitativa.

2.4.2 Enfoque de Sistemas

Sistema

Un sistema es un conjunto de elementos interrelacionados de cualquier tipo, figura 11, que tiene las siguientes tres propiedades (Ackoff, 1973):

1. Las propiedades o el comportamiento de cada elemento del conjunto tiene un efecto sobre las propiedades o el comportamiento del conjunto como un todo.

2. Las propiedades y el comportamiento de cada elemento y la forma en que estos afectan al todo dependen de las propiedades y el comportamiento de al menos otro elemento en el conjunto. Por lo tanto, ningún elemento tiene un efecto independiente sobre el todo.

3. Cada subgrupo posible de elementos en el conjunto tiene las dos primeras propiedades. Cada uno tiene un efecto, y ninguno puede tener un efecto independiente, sobre el todo. Por lo tanto, los elementos no pueden ser organizados dentro de subgrupos independientes.

Debido a estas tres propiedades, un conjunto de elementos que forma un sistema siempre tiene algunas características, o puede mostrar algún comportamiento, que ninguno de sus elementos o subgrupos puede. Además, la afiliación en el conjunto, aumenta o disminuye la capacidad de cada elemento, pero no se dejan intactos.

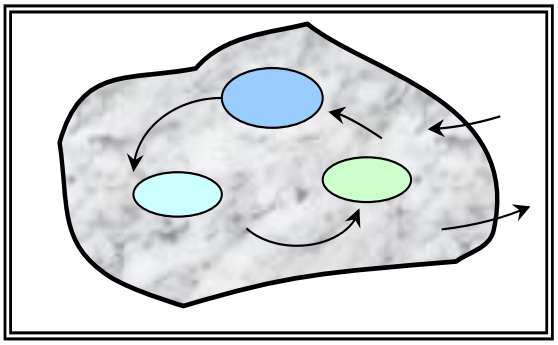


Figura 11. Esquema general de un sistema

Por lo tanto, un sistema es más que la suma de sus partes; es un todo indivisible. Pierde sus propiedades esenciales cuando sus elementos son separados. Los elementos de un sistema pueden ser sistemas por sí mismos y cada sistema puede ser elemento de un sistema más grande.

En el pensamiento analítico, la explicación del todo se deriva de las explicaciones de sus elementos. En contraparte, en el pensamiento sintético, algo a ser explicado es visto como parte de un sistema mayor y se explica en términos de su rol en éste.

El desempeño de un sistema depende de cómo se relaciona con su medio ambiente, del sistema mayor del cual forma parte y de los otros sistemas en ese medio ambiente.

El pensamiento analítico se da de fuera hacia adentro; mientras que, el pensamiento sintético de dentro hacia fuera. No puede negarse el valor del primero, pero mediante el pensamiento sintético se puede comprender lo que no podemos obtener a través del análisis, en particular de fenómenos colectivos.

Enfoque de sistemas

Cuando el pensamiento sintético se aplica a los problemas, se llama *Enfoque de Sistemas* (Ackoff, 1973). Esto es, permite conceptualizar un objeto de estudio como un sistema.

Ejemplos de áreas en las que el enfoque de sistemas ha demostrado su valor son:

- Problemas complejos que involucran ayudar a muchos actores a ver el "panorama general" y no sólo su parte.
- Problemas recurrentes que se han agravado debido a los intentos pasados de solucionarlos.
- Cuestiones en las que una acción afecta (o se ve afectada por) el medio ambiente en torno a ésta, ya sea el medio natural o el competitivo.
- Problemas cuyas soluciones no son evidentes.

El procedimiento de conceptualización de sistemas consiste de dos formas parciales y complementarias de construcción de un sistema: por composición y por descomposición (Gelman y García, 1989). El concepto *sistema general* se determina como un constructo que se obtiene con la composición de ambas representaciones.

Construcción por composición

Este procedimiento principia con los intentos iniciales de definir al sistema, que corresponden a las primeras etapas de elaboración del concepto, cuando se empieza a comprender que el conjunto de elementos seleccionados se encuentra organizado e interconectado en cierta totalidad gobernada por leyes comunes. En una siguiente etapa se intenta construir el concepto al deducir las propiedades del sistema mediante el estudio de sus componentes básicas, su comportamiento y las relaciones que los vinculan. Con este procedimiento, que parte del elemento y busca llegar al sistema, se corre el riesgo de no comprender la naturaleza integral del mismo, esto es, de aquellos aspectos estipulados, por el papel que juega, en un sistema mayor denominado *suprasistema*. En este tipo de construcciones, el conjunto de elementos, los vínculos e interrelaciones, constituyen una de las nociones parciales del sistema, como se muestra en la figura 12:

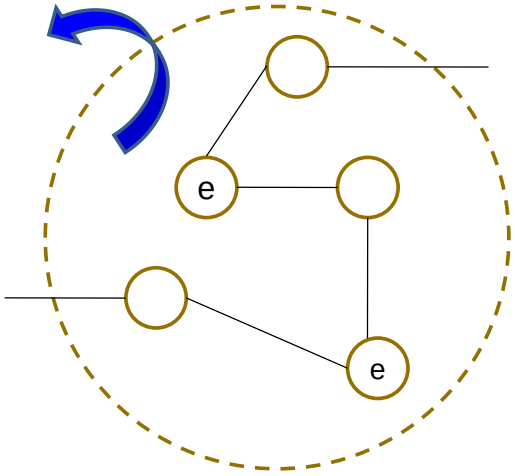


Figura 12. Construcción de un sistema por composición

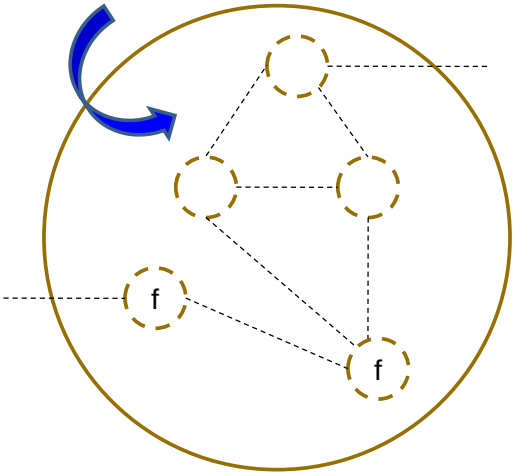


Figura 13 Construcción de un sistema por descomposición

Construcción por descomposición

Este tipo de procedimiento se aproxima más al espíritu sistémico; corresponde a un movimiento cognoscitivo opuesto al de construcción anterior. Esto es, se parte del sistema hacia sus componentes, lo que constituye una forma típica de enfoque integral, que consiste en desmembrar un sistema en subsistemas, cuyas funciones y propiedades aseguren las del sistema en su conjunto, mediante una organización adecuada.

Esta construcción se realiza tomando en cuenta la estructura externa y la interna del sistema en consideración. La primera se establece por medio del papel que el sistema juega en el suprasistema, al definir los objetivos y funciones totales y determinar otros sistemas al mismo nivel. La estructura interna del sistema, en particular su estructura funcional, se obtiene al considerar un sistema como un agregado hipotético de subsistemas interconectados, de tal forma, que asegure su funcionamiento, como se muestra en la figura 13.

2.4.3 El Método de los Sistemas

Conceptos de sistema

Al hablar de sistema nos referimos a la forma o manera como un elemento o conjunto de elementos realiza una función con un objetivo determinado (Ochoa, 1997).

Existen sistemas naturales y sistemas humanos. Los sistemas naturales son producto de diversos aspectos de la naturaleza: la lluvia, las estaciones del año, el sistema planetario solar, etc. En estos sistemas el hombre, a través de las disciplinas científicas, describe y explica los fenómenos, puede llegar a pronosticar su comportamiento aplicando como instrumento el método científico e incluso puede llegar a alterarlos para satisfacer sus necesidades.

Los sistemas humanos son aquellos diseñados por el hombre: el sistema de drenaje profundo, el sistema alimentario mexicano, el sistema de transporte, el sistema educativo, el sistema socio-político, etc. En estos sistemas el hombre, a través de los sistemistas, hombres con mentalidad sistémica, no sólo describe y explica los fenómenos, cabe la posibilidad de alterar y predecir su comportamiento. Esta última cualidad establece la diferencia entre los sistemas naturales y humanos.

Los sistemas humanos pueden ser subclasificados en: sociales y productivos, cuya similitud radica en el hecho de que participan elementos humanos y la diferencia es que los elementos físicos son componentes de mayor trascendencia en los sistemas productivos.

El objetivo general de los sistemas productivos es satisfacer necesidades materiales del hombre; en todos existen elementos (espacio físico, mobiliario, tecnología) que de alguna manera cumplen una función (producir), orientada hacia un objetivo (satisfacer necesidades materiales humanas).

Se define sistema productivo, en términos generales, como la forma o manera de cómo un conjunto de elementos humanos, físicos y mecánicos, interrelacionados y estructurados, desempeñan la función de producir bienes o servicios para satisfacer las necesidades de la sociedad.

En este contexto, un problema es la contradicción entre un estado real y un estado deseado de las cosas (puede tratarse de la destrucción o moderación de algo existente pero

indeseado, o bien la adquisición o logro de algo ausente pero deseado), es decir, cuando existe una contradicción entre nuestros objetivos y la realidad presente.

Es posible proceder a una subclasificación mayor de los sistemas productivos, en la que se considere, por un lado la estructura ya definida y por el otro, la secuencia que siguen en el tiempo, para poder asociar tipos de problemas.

Con estas condiciones, un sistema productivo primero se crea; entonces, el primer tipo de problema que se presenta es el de crear el sistema, que aún no existe.

Posteriormente, cuando el sistema existe se inician una serie de condiciones que llevan a la aparición de problemas de diversa índole; los de operación, que pueden ser: de corrección o mejoramiento y de operación; y problemas de magnitud del sistema existente: de expansión y de contracción.

Por último, un proceso es un conjunto de fases de un fenómeno o bien la sucesión o secuencia de operaciones concatenadas; estructurar es ordenar las partes de un todo. De este modo, al hablar del Método de los sistemas se está haciendo referencia a un Proceso estructurado de solución de problemas de sistemas productivos.

Considerando tipo de sistemas y tipo de problemas, se presenta en la figura 14 un resumen de estos, en dónde la línea punteada señala el área de aplicación preferencial del proceso:

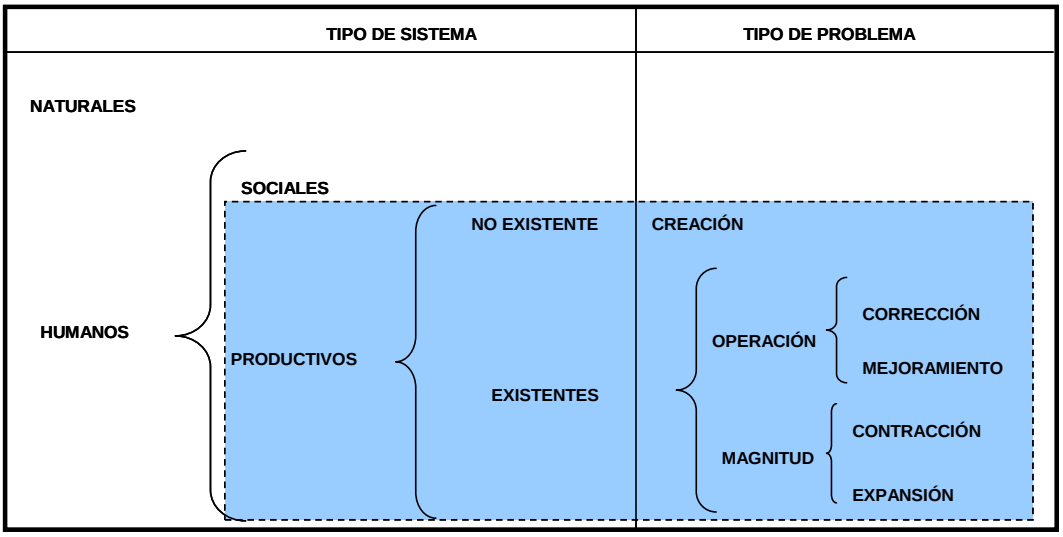


Figura 14. Tipos de sistemas y de problemas

Necesidad de un Método Sistémico

Indiscutiblemente estamos viviendo una época en la que nuestra sociedad se conduce de manera caótica. Las equivocaciones en la conducción saltan a la vista, vivimos en un mundo donde los actores permanecen inconformes e intranquilos.

Se observa en las ciencias básicas (física y química) avances que han permitido un conocimiento y dominio amplio de sus objetivos de estudio. Así también en las disciplinas técnicas, cuyo prototipo es la ingeniería, que mediante sus diversas ramificaciones han originado grandes cambios en nuestra forma de vida. En las ciencias naturales (biología y medicina) sus logros son también ampliamente reconocidos. El último grupo en esta simple clasificación lo constituyen las disciplinas económico-sociales, limitadas en su propósito para conocer y entender la realidad, predecirla o modificarla.

De lo anterior surgen algunos comentarios. Al observar los grupos en una escala cuyos extremos fueran las ciencias básicas y las disciplinas económico-sociales, el componente humano se incrementa considerablemente. Como consecuencia de este componente humano, el método de investigación utilizado denota una característica diferenciadora: mientras que las ciencias básicas se han apoyado sustancialmente en el método científico, éste no ha funcionado como debería en algunas disciplinas técnicas y menos en las económicas o sociales. El método científico formula teorías o modelos, los verifica mediante la información de sistemas existentes; de no corresponder se vuelven a formular teorías o modelos; de suceder lo contrario los utiliza para predecir nuevas observaciones y volver a verificar con nuevos datos, refinando así el modelo iterativamente hasta que pueda preverse con confianza el comportamiento del sistema, con el margen del error esperado, dada la imprecisión de las observaciones.

Al trasladar este método al estudio de los sistemas en los que intervienen con mayor proporción el hombre, se olvida que vive en constante creación, autorreflexión y modificación de su conducta, lo que origina que los modelos elaborados con el método científico no se puedan corroborar o corregir por lo repetitivo de los fenómenos.

Esta situación ha generado el enfoque de sistemas, que parte de la condición de que cualquier problema debe analizarse asociado al concepto de sistema. Consiste en una forma de pensar y de razonar en la que se abarca el todo (sistema), sin olvidarse de sus partes (subsistemas), y en el que consideran las interacciones entre estas partes y el sistema, y entre el sistema y su medio ambiente; parte del criterio de que siempre existen varias alternativas y cursos de acción para escoger los que conduzcan a un sistema satisfactorio.

Asociado al enfoque de sistemas existen diversas metodologías como el proceso estructurado de solución de problemas de sistemas productivos.

Un viraje en la solución de problemas

Los pilares del método científico (reduccionismo y causalidad) conducen a un pensamiento determinista, es decir, la ciencia no necesita conceptos teleológicos, el mundo puede ser visto como una máquina o mecanismo cuyo comportamiento está determinado por su propia estructura, lo que se conoce como mecanicismo. Así, en la escala de valores del científico, la verdad se ubica en lo más alto.

Al contrario con el método de la ciencia, el concepto de verdad cambia por el de utilidad, por ello el modo de resolver los problemas es pragmático. El enfoque analítico de la ciencia es

sustituido por un enfoque sintético, que es la razón del enfoque de sistemas; consecuentemente, el método dominante es la síntesis, que explica los fenómenos de manera integral, en su totalidad y no en partes aisladas.

El reduccionismo es sustituido por el expansionismo y el determinismo por la teleológia. Con el reduccionismo se niega la posibilidad de explicar el todo, el sistema, a partir de sus elementos últimos (sin considerar sus interrelaciones). Con la teleología se da al sistema y a sus componentes la posibilidad de fijar objetivos y elegir caminos alternativos para lograrlos; en resumen al objeto de estudio (sistema), se le da un carácter de totalidad que en sí mismo no puede ser explicado sólo por las causas, sino por los objetivos que éste persigue.

2.4.3.1 Modelo de un Sistema Productivo

Un sistema productivo es un conjunto de elementos interrelacionados y estructurados que llevan a cabo un proceso de transformación con un objetivo determinado, la manera de cómo se lleva a cabo éste queda descrito por los siguientes componentes:

- Los elementos que intervienen en el proceso de transformación, ya sea en forma activa o pasiva.
- Los elementos que no intervienen en el proceso.
- Los elementos que se ven afectados directa o indirectamente por el proceso de transformación.
- Las relaciones y su tipo entre los elementos que intervienen.
- El proceso utilizado para desarrollar dicha transformación.
- La eficiencia y efectividad con que el sistema desarrolla el proceso de trasformación.

Para lograr un primer acercamiento al modelo general de un sistema productivo se emplea un concepto de uso común, conocido como caja negra, mismo que se ilustra en la figura 15.

Cualquier sistema productivo se caracteriza por ser una estructura que mediante flujos de entrada produce flujos de salida.

Figura 15. Modelo de la caja negra

Entre los flujos de entrada, sin pretender jerarquizarlos, destacan los recursos financieros proporcionados por los propietarios del sistema o diversas instituciones.

Todo sistema productivo requiere del flujo permanente de bienes o servicios producidos por otros sistemas, o por la naturaleza, como en los procesos de extracción. Los encargados de proporcionar insumos al sistema son los proveedores, que proporcionan una gama de requerimientos, que van desde refacciones, mobiliario, materia prima, etc., hasta tecnología e información.

Los bienes o servicios producidos por el sistema conforman las mercancías que han de ser comercializadas y vendidas a los usuarios, los que retribuyen al sistema el costo invertido en su elaboración, más un incremento, generando así los ingresos. Esta retribución monetaria es considerada como otra fuente de entrada al sistema.

El último factor relevante que incide en el sistema tiene un carácter especial, consiste en el efecto de los competidores hacia el sistema, que puede ser caracterizado como otro flujo de entrada, manifestado en el mercado de bienes y servicios; así se podría hablar del impacto por la reacción del sistema en su ambiente.

Con respecto a los componentes que configuran los flujos de salida del sistema, se puede decir que un sistema productivo se interconecta con el exterior por los bienes o servicios que produce, razón de ser del sistema. Así el producto final del sistema llegará a los usuarios y consumidores, que son de dos tipos: el primero es aquél que utiliza la mercancía como insumo para su producción, el sistema al que el nuestro sirve como proveedor, encadenándose las relaciones sectoriales con el nombre de relaciones intersectoriales hacia delante; el segundo tipo de usuarios es al que el producto del sistema sirve como consumo final (no necesariamente es ropa o alimentos, sino que puede ser maquinaria, refacciones, construcción, etc., según el sistema en estudio).

Del sistema hacia el exterior, se dirigen unidades monetarias como pago a los proveedores por los insumos proporcionados al sistema, bienes o servicios del sistema productivo del proveedor. Esto provoca una concatenación sectorial, pero en sentido inverso, lo que se conoce como relaciones intersectoriales hacia atrás.

Una tercer salida son los desechos; no importantes para algunos sistemas, pero muy significativos para otros; por ejemplo las fábrica de cemento Portland o cualquier sistema de alcantarillado, por su repercusión en el ambiente.

Los sistemas productivos se dan en un espacio físico con una planta e instalaciones; no existe alguno que sea idealización e intangible. En la planta laboran los ejecutivos, los administrativos y los obreros (mano de obra directa), que llevan a cabo las funciones del sistema. Para ejecutar estas funciones se requieren recursos naturales, que se transforman en productos finales por medio de maquinaria, equipo y una tecnología acorde.

Todo sistema productivo tiene una estructura con las relaciones que deben darse entre las jerarquías, funciones y obligaciones individuales para su eficiente operación, es decir, una organización respaldada y complementada por información.

Estos elementos señalados proporcionan una acotación del entorno de primer orden, como puede observarse en la figura 16, que representa el modelo general de un sistema productivo.

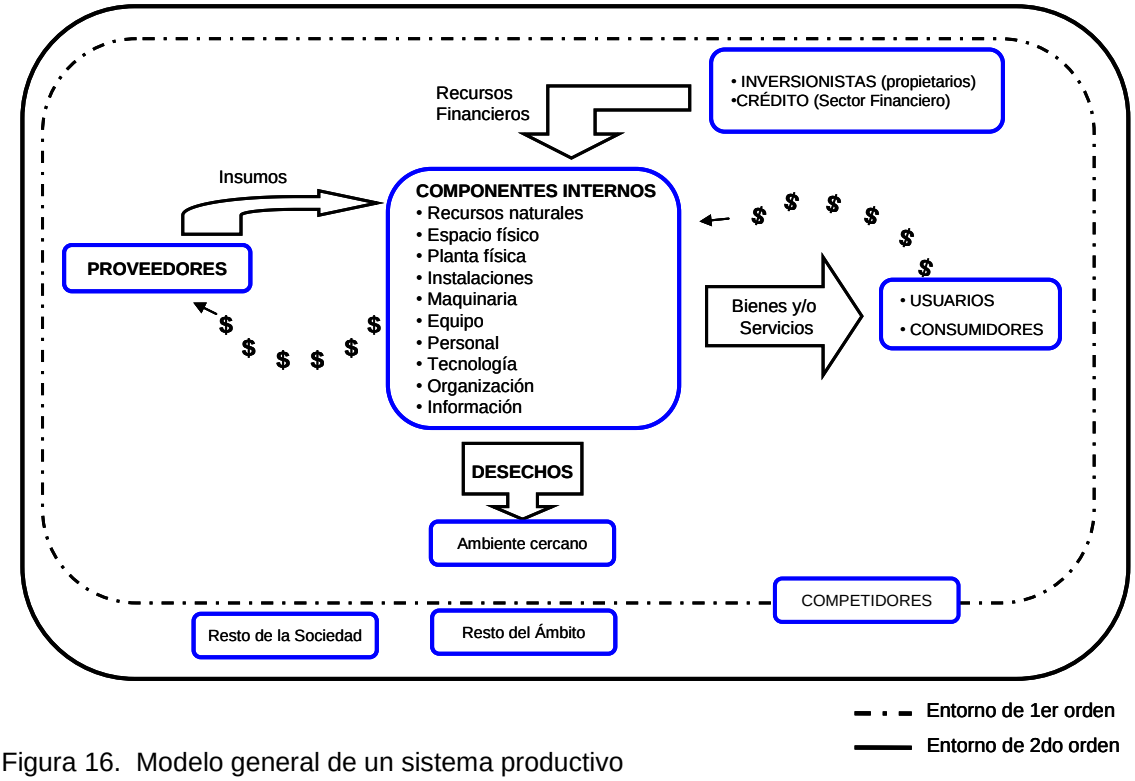


Figura 16. Modelo general de un sistema productivo

Este entorno se caracteriza por ser la envolvente de las interacciones más fuertes e importantes del sistema con el medio en que se encuentra; el entorno de segundo orden sería la envolvente de las más débiles o secundarias, como las interacciones entre el sistema y el resto de la sociedad. En dicho esquema se ubica a los competidores con un componente en el entorno de primer orden y otro en el segundo, con lo que se intenta representar la poca importancia que tienen en algunas ocasiones y la gran relevancia en otras.

El proceso estructurado debe corresponder a la naturaleza del problema; así, los problemas de mejoramiento y corrección guardan una gran similitud, ya que el sistema no requiere cambios cuantitativos relevantes, sino variaciones, reajustes o reorganización de sus elementos. Los problemas de expansión, contracción y creación de sistemas implican cambios cuantitativos importantes, que pueden generar un nuevo sistema.

Al considerar dos tipos de problema (tomando en cuenta que un problema de corrección es igual a uno de mejoramiento) necesariamente se requieren dos procesos de solución para todo tipo de problemas en un sistema productivo.

El método sistémico para resolver problemas operacionales, (método operacional) sirve para abordar problemas de mejoramiento y corrección; en cambio el método sistémico para resolver problemas de creación o modificación de sistemas (método de planeación) se utiliza en los casos de creación, expansión o contracción de sistemas.

Un proceso es un conjunto de fases de un fenómeno, o la secuencia de operaciones concatenadas; estructurar es ordenar las partes de un todo. Entonces, al hablar de un “proceso estructurado de solución de problemas” se hace referencia a una secuencia

ordenada de fases u operaciones concatenadas que disminuyen o anulan la diferencia entre un estado real de la cosas y una situación deseada.

La evolución de un sistema productivo va desde que nace la inquietud de crearlo y se obtienen los recursos para realizarlo, hasta que surgen y se solucionan los problemas en el sistema ya operando.

2.4.3.2 El Método Operacional

El objetivo es llegar a controlar el sistema. Se requiere ubicarlo para poder definir el marco de su análisis; separar sus componentes, que pueden ser evaluados ex-post, y sus resultados determinan la existencia de problemas que serán definidos con el propósito de diagnosticar el estado actual del sistema e identificar las opciones de corrección; estas se evalúan ex-ante para seleccionar la mejor, implantarla y controlar nuevamente el sistema, figura 17.

1) Ubicación del sistema

   Incluye tres niveles: ubicación temporal, sectorial y espacial. El primero se refiere al período para el cual se planeó el sistema, indicando el tiempo transcurrido y por transcurrir en este horizonte de planeación; en el segundo se señala si es del primero, segundo o tercer nivel de agregación sectorial; por último, en el tercero se indica si es puntual, regional, nacional, etc., el ámbito de acción del sistema en el espacio geográfico.

2) Análisis del sistema existente

   Se desagregan los componentes para conocer los elementos específicos del sistema; la orientación del análisis está dada en la elaboración de diseños alternativos.

   La razón de este análisis es detectar fallas, desajustes, incongruencias, y mientras haya esto, la importancia para cada subsistema es distinta, resaltan las áreas en las que la problemática es más evidente, pero no hay que olvidar las restantes ni perder el sentido de totalidad, básica para el sistema.

   El resultado de esta fase son elementos que caracterizan algún componente del sistema, con una medida de comportamiento que muestre los resultados de su desarrollo en un periodo dado; por ejemplo, eficiencia en una línea de producción, volumen de ventas (en unidades de producción o monetarias), costos unitarios de producción, tiempos de entrega de proveedores, inasistencia del personal, retrasos en financiamiento, contenido de contaminantes en los desechos, etc.

3) Evaluación ex-post de los resultados del sistema

   Evaluar ex-post es juzgar los resultados del sistema; es afirmar e informar si el sistema marcha bien o no, con respecto a los objetivos planteados. Esta evaluación resulta eficiente si el análisis lo fue; esto es, si la separación de los elementos del sistema y la asignación de parámetros de medición de su comportamiento se relacionan con objetivos originales, de esta manera será fácil demostrar si éstos han sido cumplidos y en qué medida.

   Para que la comparación sea objetiva es recomendable hacerla con el mismo sistema, sobre todo cuando no se tienen claros los objetivos; esto es, si no existen, deben buscarse en series históricas del sistema o en indicadores sobre el estado del mismo y con ellos comparar su funcionamiento.

Si no se logra lo anterior, podrían utilizase indicadores de otros sistemas productivos nacionales en caso de falla, otra opción sería considerar la desagregación sectorial o bien sistemas existentes en otros países. Una última opción, sería realizar estimaciones.

Como ejemplos de esta fase tenemos: la eficiencia en la línea de producción es más baja de lo que se esperaba; dados los objetivos y las condiciones de mercado prevalecientes, el volumen de ventas es adecuado; los costos de producción comparados con sistemas similares, son altos; y el retraso de la producción es debido al pésimo suministro de materias primas.

Como podrá observarse, los componentes-problemas o las áreas-problemas deben quedar bien definidos como aquellas en las que no exista dificultad alguna.

4) Diagnóstico del comportamiento del sistema

   El diagnóstico es determinar el estado del sistema actual, es plantear causas por las cuales se encuentra así y definir las relaciones que guardan las partes del mismo.

   Detectados los problemas, se identifican las cadenas causa-efecto y se llega hasta las últimas causa-origen, no precisamente porque se consideren los males a combatir, sino porque ello determina las limitaciones o alcances de la siguiente fase.

5) Identificación de opciones de mejoramiento.

   Realizando el diagnóstico del sistema, la fase de identificación de opciones resulta sencilla.

   De lo anterior surge un método importante: deben identificarse como mínimo tantos cursos de acción como causas se incluyen en la cadena, es decir, se reconoce que una causa es a su vez efecto de otra, entonces, la ausencia de una causa provocará no solo la desaparición de su efecto, sino además la de los subsecuentes.

   Entre más cadenas de causa-efecto existan, mayor será el número de opciones de corrección o mejoramiento, porque se pueden visualizar combinaciones de rompimientos de cadenas, lo que debe considerar los costos combinados, teniendo presente al sistema como un todo.

6) Evaluación ex-ante de opciones

   En esta fase se evalúan las opciones obtenidas en la anterior, se emite un juicio generado de la comparación de los posibles resultados que se obtendrán con cada opción considerando los objetivos o marcos de comparación establecidos.

7) Selección

   La mejor opción de mejoramiento o corrección consiste en valorar la evaluación ex-ante. Es una fase en donde se toma la decisión de implantar la mejor opción.

8) Implantación de la opción seleccionada

   Con un nuevo elemento o mecanismo operativo, se transforman las condiciones en cada uno de sus elementos, en la medida en que estén interconectados. Esta fase se lleva a cabo con el mínimo de alteraciones.

9) Control.

Para algunos autores está fase es de mayor importancia. El sistema productivo dinámico es susceptible de producir cambios internos que lo desvíen de lo deseado y se creen problemas. El control permite minimizar o anular, de ser posible, esta situación latente en los sistemas.

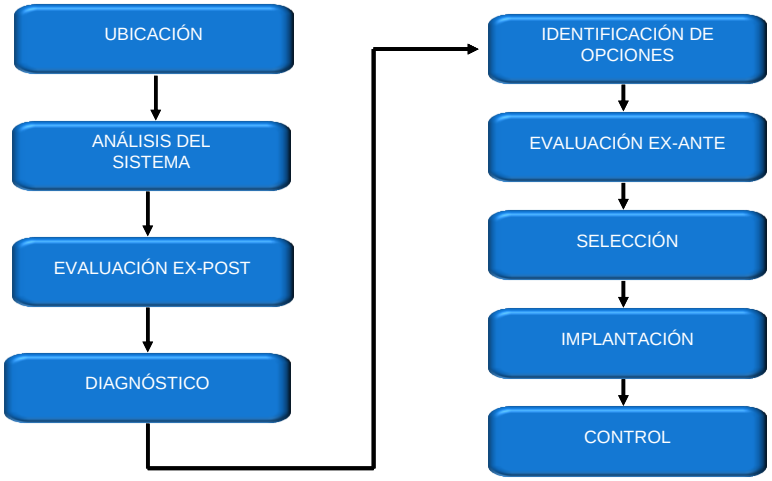


Figura 17. Proceso de solución de problemas de sistemas productivos existentes

2.4.4 Mapas Conceptuales

Dado que un sistema es una totalidad caracterizada por las relaciones entre sus componentes, estáticos o dinámicos, concretos o abstractos, muchas conexiones son más fácilmente "dibujables" que descritas en prosa, ya que, mirando un mapa, por ejemplo, podemos considerarlo como un todo y nuestra mente pueden procesar simultáneamente diferentes partes de éste.

Los diagramas son resúmenes automáticos, así, los mapas son muy importantes en cualquier aplicación de conceptos de sistemas; son un medio para visualizar ideas, conceptos y relaciones jerárquicas entre los mismos.

Un mapa conceptual es una representación gráfica, esquemática y fluida, donde se presentan los conceptos relacionados y organizados jerárquicamente, figura 18. También representan una simplificación de algún sistema de actividad humana.

Su elaboración favorece la organización de las ideas; no es sólo plasmar un conocimiento que se representa gráficamente, sino que anima a establecer relaciones que no se habían planteado en un principio; los significados son en buena parte personales, y la representación esquemática y fluida del mapa estimula la creatividad en las relaciones que establecen.

Sus características son las siguientes:

- Son inclusivos.- existen conceptos generales que se enlazan con otros conceptos menores y por lo tanto más específicos.
- Son jerárquicos.- existe una relación de subordinación entre el concepto clave y los conceptos que se enlazan con éste.
- Son subjetivos: puesto que cada persona tiene una manera distinta de establecer las relaciones que existen entre los conceptos de un mapa conceptual.
- Son integradores u holísticos.- un mapa conceptual representa los conocimientos como un todo, graficando en éste, la mayor parte de las relaciones conceptuales que un individuo puede realizar.

- Son sintetizadores.- en tanto permiten esquematizar las relaciones conceptuales que un individuo puede realizar, dirigiendo su atención a los aspectos más relevantes y de mayor significado para él.
- Son interrelacionadores.- cada una de sus partes está vinculada al resto, por lo cual la activación de cualquiera de sus partes puede activar las otras.

El desarrollo de mapas conceptuales está dirigido hacia la elaboración de un conjunto de símbolos propios o específicos, y hacia la definición de reglas generales y de un conjunto de criterios que permitan formularlos consistentemente.

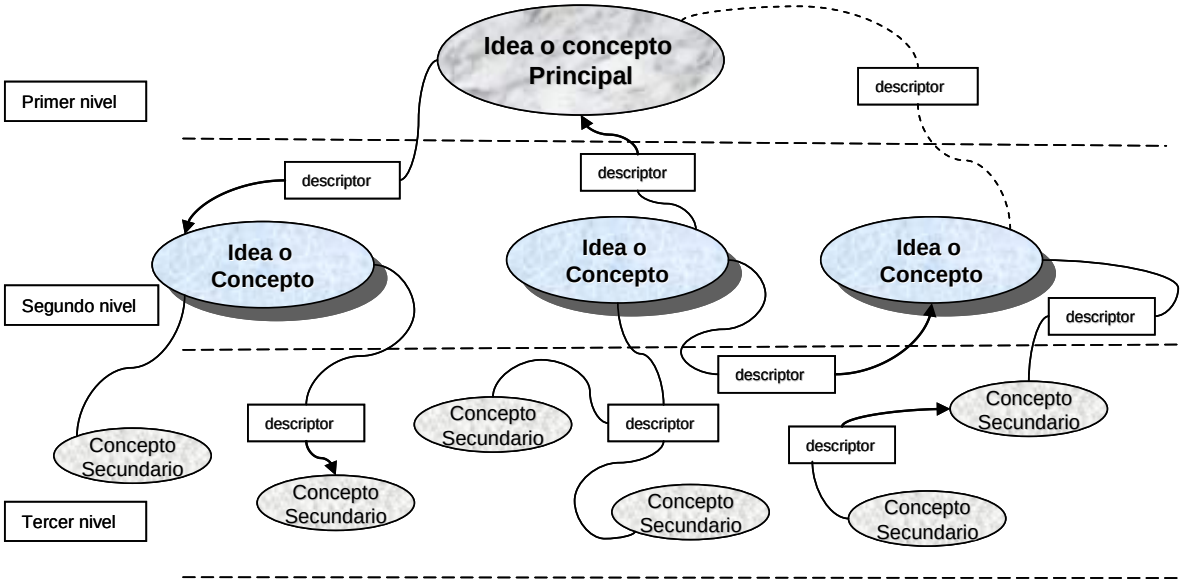


Figura 18. Mapa conceptual

2.4.5 Análisis de Stakeholders

Un stakeholder es el personal directamente involucrado en las situaciones problemáticas de la empresa, actúan como los expertos para la solución de los problemas (o su impedimento) y son la fuente de información. Es decir, son las personas que tienen algo que ganar o perder en el proceso de solución de un problema. Puede decirse que el personal de una empresa adquiere el "estatus" de stakeholder, cuando tiene interés en un problema por cualquiera de las tres formas siguientes (Banville, 1998):

- porque pueden afectar el curso de solución de un problema;
- porque están siendo afectados por su solución;
- ambas cosas, porque están siendo afectados y pueden afectar al problema.

Los stakeholders dependen de la organización para la realización de algunas de sus metas y ésta a su vez de ellos para la realización de sus metas, objetivos y, por lo tanto, de su misión. Es una mutua interacción.

El enfoque de los stakeholders afirma que las empresas mejoran su desempeño en la medida que sus actores son tomados en cuenta y se encuentran comprometidos con las operaciones de ésta (Argenti, 1997). En la práctica, la noción de stakeholder debe ser concretamente

especificada de acuerdo con la situación. De hecho, el concepto está directamente relacionado con el problema: los stakeholders cristalizan alrededor de un problema dado. Pero también un problema es construido con base y por los stakeholders identificados, produciéndose un efecto circular.

Esto significa, que no es posible considerar un problema independientemente de la identificación de los dueños del problema. En este sentido, este análisis sirve, entre otras cosas, para determinarlos con mayor precisión. Por lo tanto, el proceso de identificación de los stakeholders asiste significativamente a la formulación y solución de los problemas y es determinante para la implantación de estrategias.

Tomando en consideración la clasificación de otros autores como (Rowe, 1989), se establece que para definir a los stakeholders es conveniente enfocarse sobre una organización o departamento y listar al personal que tenga una relación importante con esta unidad de la empresa.

En este contexto, el proceso de toma de decisiones será de carácter grupal, el llamado tipo (G), las decisiones se realizarán en grupo. Es decir, la decisión es tomada por el grupo de personas que participan en el análisis de la problemática, normalmente es un subconjunto de personas relacionadas con el problema.

2.4.6 Análisis Causa- Efecto

Es una técnica sencilla y flexible para la identificación y análisis de las causas y efectos de un problema, consiste en construir e interpretar el diagrama causa-efecto (conocido también por su apariencia como esqueleto de pescado).

El diagrama de análisis causal fue inicialmente desarrollado por el profesor Kaoru Ishikawa de la Universidad de Tokyo y fue y utilizado por primera vez en 1953 en Japón por la compañía acerera Kawasaki; años después en la Universidad de Oregon, fueron generadas algunas extensiones al mismo.

Con la práctica se ha ido modificando. Actualmente esta técnica es ampliamente citada y usada durante el proceso de solución de problemas.

La técnica es esencialmente una extensión del proceso de la “caja negra”. Consiste en colocar en un rectángulo (caja) el problema por analizar. Del lado izquierdo se colocan las principales causas (entradas) y de manera similar, del lado derecho, los principales efectos (salidas) que derivan del problema, tal como se muestra en la figura 19.

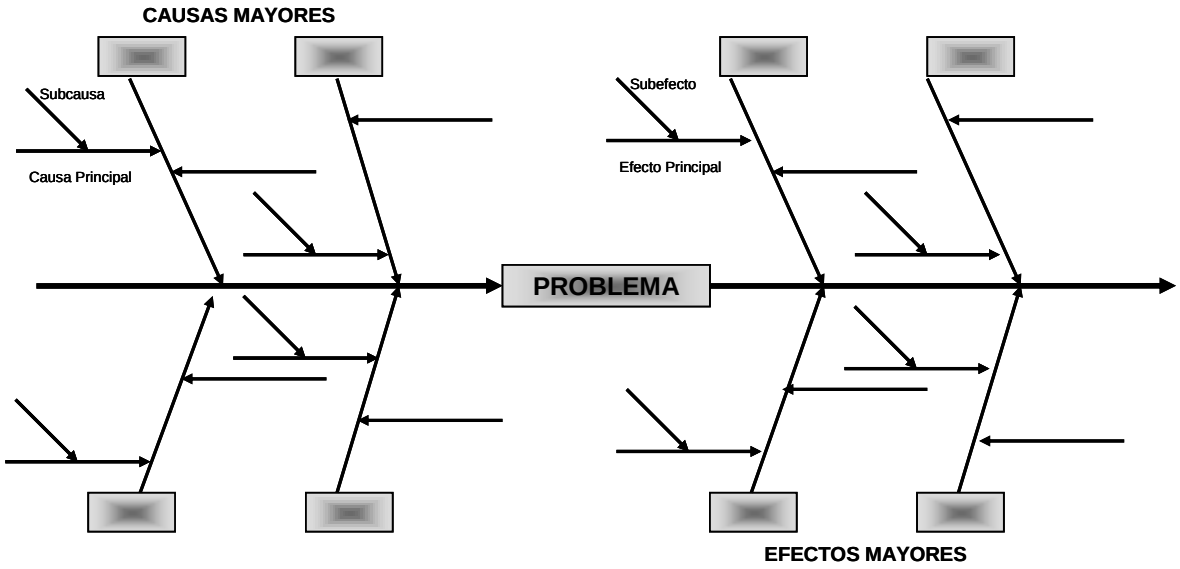


Figura 19. Diagrama causa-efecto

Es importante señalar que la técnica se puede realizar utilizando tan sólo el lado izquierdo (las causas), como inicialmente fue creada, o también, empleando el lado derecho (los efectos) o ambos lados.

Algunas de las ventajas de la técnica son: elimina el síndrome de la causa única, produce un entendimiento uniforme del problema al presentar la misma información a todos los involucrados y algo muy importante, los hace corresponsales del problema.

El diagrama tiene las limitantes de las cadenas causales: las causas son mutuamente excluyentes, no hay relación entre ellas y se mantiene un pensamiento determinista y mecánico. Sin embargo se pueden mitigar estas insuficiencias realizando relaciones entre las causas y dibujándolas en el diagrama empleando una nomenclatura consistente.

Esta técnica demanda un conocimiento más o menos profundo de la organización y de los problemas que se presentan y sólo se aplica a un problema a la vez, aunque se detecten otros vinculados con el problema analizado.

Es importante reconocer que el diagrama por sí mismo no califica el grado de influencia o peso que tienen las causas individuales sobre el efecto. Esto tiene que determinarse con la ayuda de otras técnicas asociadas como el Diagrama de Pareto.

2.5 Conclusiones

Actualmente las empresas dependen en gran medida de los sistemas de información para operar. Frente a una Interrupción de estos, la empresa ve comprometida su operación. Por tanto, debe estar preparada para enfrentar cualquier evento imprevisto que pueda causar una Interrupción de los sistemas de información, manteniendo así su compromiso de continuidad de cara al cliente.

Aunque el riesgo operacional es inherente a todas las operaciones de negocios y no puede ser eliminado totalmente, si puede ser gestionado, mitigado y, en algunos casos, asegurado.

Recuperación ante desastres es el proceso para recuperar el acceso a los datos, hardware y software necesarios para reanudar las operaciones críticas de negocio, después de un desastre natural o causado por personas. También debe incluir planes para hacer frente a la pérdida inesperada o repentina de personal clave. Un Plan de Recuperación ante Desastres es parte de un plan mayor, el Plan de Continuidad del Negocio.

Un plan adecuado garantiza que la empresa minimice el tiempo de inactividad y las pérdidas. También permite una respuesta coherente a un desastre con el personal vital en la organización que conoce efectivamente las funciones que tendrá que desempeñar. Por lo tanto, es imperativo que el plan esté actualizado y completo.

Si no se cuenta con especialistas en la empresa, existen consultorías que ofrecen servicios para desarrollar este tipo de planes. Incluso si el plan se desarrolla en casa, es conveniente que sea revisado por expertos externos para ayudar a identificar sesgos. También están disponibles software y plantillas para desarrollarlos y pueden ser una alternativa más barata y fácil.

Existen múltiples beneficios de la planeación de continuidad del negocio dentro de la organización. No sólo los datos, hardware, software, etc., estarán mejor protegidos, las personas que componen la organización serán mejor salvaguardadas en caso de que ocurra un desastre. También se obtiene un mejor conocimiento de los activos con los que cuenta la empresa; mismo que ayudará en la planeación, uso de recursos, control y mejoramiento de procesos.

En contraparte, es necesario considerar las dificultades que esperan a aquellos que desarrollan planes de continuidad del negocio. Cuando se está desarrollando un DRP se tiene que ajustar a las necesidades de la organización y en función a estas determinar la respuesta más apropiada. Así mismo, es necesario detallarlos a fin de presupuestar correctamente los costos asociados y evitar dolores de cabeza al personal de la organización en tiempos de desastre.

Más aún, si bien los conceptos de continuidad del negocio y recuperación ante desastres se originaron a partir de tecnologías de la información, la planeación conceptual sólo para infraestructura de TI deja a la organización abierta a una posible catástrofe.

El Enfoque de Sistemas permite conceptualizar un objeto de estudio como un sistema. Puede ser aplicado en el estudio de las organizaciones permitiendo identificar y comprender con mayor claridad y profundidad los problemas organizacionales, sus múltiples causas y consecuencias. Así mismo, viendo a la organización como un ente integrado, conformada por partes que se interrelacionan entre sí a través de una estructura que se desenvuelve en un entorno determinado, se estará en posibilidad de poder detectar con la amplitud requerida tanto la problemática, como los procesos de cambio que de manera integral, es decir a nivel humano, de recursos y procesos, serían necesarios implantar, para tener un crecimiento y desarrollo sostenibles y en términos viables en un tiempo determinado.

CAPÍTULO 3. ELABORACIÓN DE LA ESTRATEGIA

La Comisión Nacional de Seguros y Fianzas requiere elaborar una estrategia a través de la cual sea posible responder ante un incidente que pueda interrumpir su operación y reanudarla en un tiempo aceptable, de tal forma que pueda controlar el impacto resultante, en términos de credibilidad e imagen principalmente.

Para dar respuesta a esta necesidad se propone el uso de dos teorías validadas:

La elaboración de un Plan de Recuperación ante Desastres que permita garantizar que los servicios informáticos que provee al exterior así como que los procesos internos críticos operen a un nivel aceptable en caso de desastre, de tal forma que se logre una recuperación efectiva y se mitiguen los efectos causados.

El Enfoque de Sistemas que permita conceptualizar al objeto de estudio como un sistema.

El concepto de sistema ha llegado a desempeñar un papel fundamental en la ciencia contemporánea. Esta preocupación se refleja entre los responsables de la gestión, para los que el enfoque de sistemas a problemas es fundamental y para los cuales las organizaciones, un tipo especial de sistema, son el principal objeto de estudio.

Su carácter hace que éste sea muy efectivo en la mayoría de tipos de problemas que involucran cuestiones complejas, que dependen en gran medida del pasado o de las acciones de los demás y/o que se derivan de la coordinación ineficaz entre los implicados.

El Enfoque de Sistemas permite integrar los elementos necesarios a fin de evitar los errores comunes que se presentan en la implantación de un DRP. En adición a los expuestos anteriormente, tenemos los siguientes (Dávila, 2005):

a) No se tiene definido claramente lo qué es un análisis de impacto al negocio (BIA) y como se puede integrar con los proyectos de administración del riesgo (principalmente el operacional); qué debe de hacerse para justificar una estrategia de contingencia y cuál es la diferencia entre los distintos tipos de planes, que no es otra que el enfoque que tiene sobre determinada área o propósito.

b) No considerar a los planes como un medio para lograr la continuidad del negocio sino como el objetivo.

c) Falta de una definición de responsabilidad conjunta en el tema de continuidad del negocio; no sólo el apoyo político proporcionado por la alta Gerencia es suficiente. Todos los empleados son igualmente responsables.

d) Se considera la continuidad del negocio como un “proyecto”; se involucra personal de varias áreas y no se formaliza la función, lo cual es una de las mayores causas de su fracaso. Lo que se debe hacer es instaurar una coordinación responsable de la continuidad del negocio, la cual no debe tener más de dos o tres personas, un coordinador y asistentes, y entre ellos deberán ser capaces de articular todo lo necesario en la organización para cumplir con los objetivos de la continuidad del negocio. Obviamente, pretender implementar la continuidad con sólo dos o tres personas es prácticamente imposible; por ello, es importante distribuir la responsabilidad entre los propietarios de los procesos y/o aplicaciones críticas del negocio y que la coordinación actúe como tal: coordinando, dando guías, y estandarizando el trabajo de toda la organización. Al distribuir la responsabilidad se logran dos cosas:

- Que la continuidad de negocio sea implementada con mejor calidad, esto debido a que los mismos dueños del proceso y/o aplicación crítica son quienes definen, documentan y prueban sus procedimientos de contingencia.
- Que la coordinación no asume la responsabilidad completamente, sino también los dueños de los procesos y/o aplicaciones críticos.

e) No se logra uniformizar y estandarizar el lenguaje de continuidad del negocio que hablan todas las áreas involucradas, entonces aparecen planes, términos, conceptos, y opiniones que lo único que logran es crear una complejidad en el tema que hace imposible su integración y mantenimiento.

3.1 Diseño de la Estrategia

Basados en las mejores prácticas, la elaboración tradicional de un Plan de Recuperación ante Desastres requiere de los siguientes pasos para su elaboración:

1) Análisis de impactos al negocio, BIA.

   Este determina qué aplicaciones son las más críticas del negocio, lo cual a su vez, identifica los activos necesarios (datos, HW y SW) para su funcionamiento.

   Aplicación crítica = f (criticidad del proceso)

2) Evaluación de riesgos

   Determina los posibles riesgos que pueden presentarse en la CNSF

   Riesgo = f (Vulnerabilidad, Amenaza)

3) Establecer la estrategia, con apoyo de los datos anteriores, que se utilizará para llevar a cabo la recuperación ante un evento de desastre.

A fin de enfrentar los problemas comunes, cada vez más complejos, que presenta la elaboración de este tipo de planes, la estrategia propuesta a desarrollar integrará un paso inicial, consistente en la definición del sistema, lo cual nos permitirá identificar los elementos que lo integran, sus relaciones entre sí y con el medio ambiente.

Se elaborará un cuestionario para obtener información de procesos y aplicaciones establecidos, así como del historial de incidentes. Éste será contestado por los propietarios de procesos y aplicaciones a través de la herramienta Mitigator, de Evergreen, la cual, permite realizarlo en línea, y a su vez, almacenar las respuestas en la base de datos correspondiente.

Una vez realizadas las encuestas, las respuestas se analizarán y afinarán, en caso de presentarse duda en colaboración con los responsables, a través de entrevistas.

Para legitimizar la metodología se presentará a los stakeholders. Así mismo se darán las instrucciones necesarias para contestar las encuestas que se deben de responder para realizar el BIA.

En forma gráfica la estrategia diseñada se muestra a continuación en la figura 20:

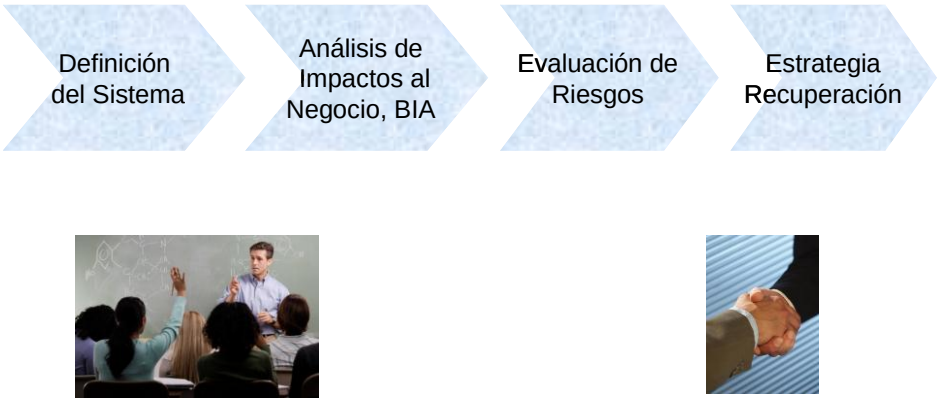


Figura 20. Estrategia propuesta para la elaboración del DRP

3.1.1 Definición del Sistema

Los pasos empleados para definir el sistema son los siguientes:

1) Ubicar el sistema dentro de su contexto.

   El contexto está definido por espacio, tiempo y causalidad. Esto permite definir las fronteras del sistema.

2) Establecer el modelo del sistema productivo.

   Este modelo nos permitirá explicar el comportamiento o propiedades del contexto o del sistema total, así como el comportamiento o propiedades del sistema en términos de su papel o función dentro del contexto o sistema total; qué es y qué hace.

   a) Identificar el tipo de sistema y de problema a resolver.

   b) Realizar un primer acercamiento a través de la técnica de la caja negra.

      Esta técnica se recomienda para los problemas de carácter táctico-operacionales.

   c) Establecer el modelo del sistema productivo, desagregando en los niveles necesarios.

Es conveniente mencionar que el análisis de stakeholders, necesario para terminar de definir un sistema, no se realiza en esta etapa porque ya está considerado dentro de las siguientes. Particularizando, en el Análisis de Impactos al Negocio se determinan los responsables de procesos y aplicaciones; incluyendo tanto personal de TI como de las áreas operativas (sustantivas y de apoyo) de la CNSF. Así mismo, en la Estrategia de Recuperación se determina el personal vital para llevar a cabo las labores de recuperación y los proveedores críticos necesarios.

3.1.2 Análisis de Impactos al Negocio

Los pasos que integran el análisis se muestran a continuación:

1) Definir las aplicaciones críticas

   Se definen las aplicaciones que soportan los procesos críticos de la CNSF. También, se determinan los tiempos objetivos de recuperación (RTO) y los puntos objetivos de recuperación (RPO) correspondientes.

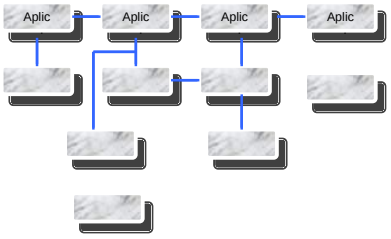
2) Definir el impacto de las interrupciones

   Se define el impacto originado por la ausencia de alguna de las aplicaciones que soportan cada proceso crítico.

   En este caso, únicamente se consideran impactos operacionales ya que la CNSF es una Entidad Reguladora del Gobierno Federal.

3) Establecer las relaciones entre aplicaciones

   Se establecen las relaciones entre las aplicaciones y se determinan los activos que las soportan y otros elementos críticos de la operación: Herramientas y Registros Vitales.



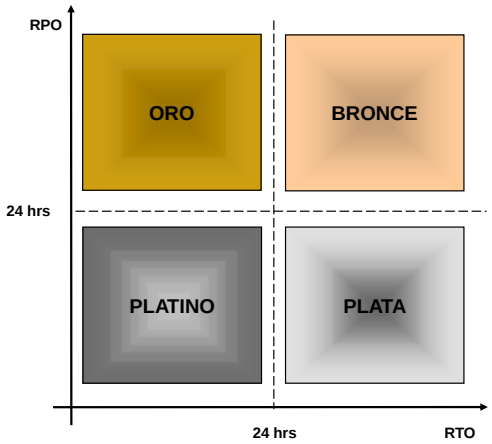
4) Determinar la criticidad de las aplicaciones

5) Establecer el orden de recuperación de las aplicaciones.

   De acuerdo a los tiers de aplicación establecidos se categorizan las aplicaciones para establecer el orden inicial de recuperación. Los tiers de aplicación se definen en base a los valores de RTO y RPO mostrados en la tabla 2:

Tier	RTO, (hrs)	RPO, (hrs)
Platino	<= 24	<= 24
Oro	<= 24	> 24
Plata	> 24	<= 24
Bronce	> 24	> 24

Tabla 2. Valores de RTO y RPO para establecer los tiers de aplicación



3.1.3 Evaluación de Riesgos

Los pasos para realizar el análisis son los siguientes:

1) Establecer las posibles amenazas

   Se establecen las amenazas cuya materialización, dadas las vulnerabilidades latentes, afectarían a la Organización. Para este efecto se recurre a la relación de amenazas establecida en las mejores prácticas de los organismos internacionales.

   A cada una de las amenazas se les debe asignar un valor, particular al caso de análisis, que se determina de acuerdo con la información que se disponga. La tabla 3 muestra los valores posibles:

Incidencias		
Nombre	**Ocurrencia promedio**	**Valor**
Inminente	Una o más por semana	5
Próxima	Una por mes	4
Potencial	Una por semestre	3
Distante	Una por año	2
Remota	Una en más de un año	1

Tabla 3. Valoración de amenazas

2) Determinar las vulnerabilidades

   Las causas mayores encontradas a través de la técnica causa-efecto, se determinan como vulnerabilidades, las cuales exponen a la organización a la materialización de posibles amenazas.

3) Determinar los posibles riesgos.

   La identificación de las amenazas materializadas a través de las vulnerabilidades establecidas representan los posibles riesgos a los que se encuentra expuesta el área de TI en la Continuidad de su operación.

   Riesgo = F (Amenaza, Vulnerabilidad)

4) Medir las vulnerabilidades.

A cada una de las vulnerabilidades encontradas es necesario asignarle un valor que permita establecer el grado de preparación de la operación para afrontar las diferentes amenazas. Para tal efecto se recurrió a los criterios de valoración de vulnerabilidades, establecidos en las mejores prácticas y que se presentan en la taba 4.

Valor	Criterio
5	La operación está expuesta a la amenaza, no habiéndose identificado con anterioridad, por lo que no existen controles, políticas, procedimientos, ni herramientas para mitigarla. Los responsables y usuarios de la operación la desconocen o ignoran. Las responsabilidades de la operación y de seguridad no están asignadas ni difundidas. Las condiciones son propicias para la ocurrencia del evento.
4	La amenaza esta identificada por los especialistas; existen procedimientos y herramientas para mitigarla, aunque se carece de políticas y controles. Las responsabilidades de la operación y de seguridad no están asignadas ni formalizadas, por tanto, existe bajo involucramiento en lo referente a la protección contra ésta.
3	Los responsables están identificados, están concientes de los riesgos y actúan sobre los mismos. Existen medidas para mitigarlos, aunque se carece de políticas y controles. Las responsabilidades de seguridad son explicitas y están formalizadas. Se cuenta con personal especializado en seguridad.
2	Las responsabilidades han sido definidas y asignadas. El riesgo es reconocido y se toman las medidas acordes al nivel que representa; existen controles, políticas, planes, procedimientos y herramientas para manejarlo. El personal de seguridad conoce y tiene experiencia en las prácticas correspondientes.
1	Las responsabilidades han sido definidas y asignadas. El riesgo es reconocido y se toman las medidas acordes al nivel que representa con una visión integral de la seguridad en la empresa; existen controles, políticas, planes, procedimientos y herramientas para manejarlo. Se realizan evaluaciones continuas y programas para mantener al personal conciente de los riesgos y para evaluar el cumplimiento de los controles.

Tabla 4. Valoración de vulnerabilidades.

5) Determinar la probabilidad de ocurrencia de un riesgo.

Para determinar la probabilidad de ocurrencia de un riesgo se recurre a la matriz de incidencias (vulnerabilidades vs. amenazas) y se determina para cada uno, la cantidad de incidencias dentro de ésta. N representa el riesgo más posible de presentarse.

Para la elaboración de la matriz de probabilidad de ocurrencia de un riesgo, se realiza una categorización de incidencias de los riesgos en la matriz de incidencias, en rangos proporcionales de acuerdo al mayor número de incidencias presentadas (N). Se establecen 5 rangos en donde se ubica el riesgo dependiendo de la cantidad de veces que se pueda materializar.

Por otra parte se tiene la categorización de la valoración de las diferentes amenazas y de las vulnerabilidades que permiten su materialización en cada uno de los riesgos identificados. Esto permite establecer en la matriz el coeficiente promedio de riesgo,

$$\text{Coeficiente Promedio de Riesgo} = \frac{\Sigma \text{ (Valor de la Amenaza) (Valor de la Vulnerabilidad)}}{\text{No de Incidencias del Riesgo}}$$

Para estos coeficientes de igual manera se establecen rangos, obtenidos a partir de la asignación proporcional de intervalos desde el mayor hasta el menor coeficiente posible.

La matriz de probabilidad se obtiene ubicando el nivel de probabilidad de cada uno de los riesgos, dependiendo del rango proporcional de incidencias y del rango en el que se encuentre el coeficiente promedio de riesgo.

En la tabla 5 se muestran los niveles de probabilidad de un riesgo:

Nivel	Descriptor	Descripción
A	Casi cierto	Se espera que ocurra en muchas circunstancias conocidas o desconocidas. Altísima probabilidad
B	Probable	Puede ocurrir en circunstancias conocidas o desconocidas. Alta probabilidad
C	Posible	Es posible que ocurra solamente en circunstancias conocidas
D	Improbable	Podría ocurrir en algún momento o circunstancia no conocida
E	Raro	Puede ocurrir solamente en circunstancias excepcionales

Tabla 5. Niveles de probabilidad de un riesgo

6) Determinar el nivel del impacto.

Para determinar el nivel de impacto asociado a la materialización de los diferentes riesgos identificados, es necesario definir para cada uno de estos los tipos de impactos posibles, determinados a través del Análisis de Impactos al Negocio BIA. Para esto debe considerarse:

a) La importancia de cada impacto para la Comisión, dado que no todos los impactos afectan de la misma manera el cumplimiento de su misión y sus objetivos estratégicos.

b) No todos los riesgos son igualmente viables en su materialización, puesto que dependen de las características propias de la Comisión y de su entorno. Por lo que es necesario revisar la matriz de incidencias para identificar el número de incidencias de cada riesgo, y a partir del número mayor, asignar valores proporcionales que permitan darle a cada tipo de impacto una ponderación.

Con los valores obtenidos, es necesario calcular en la matriz de riesgos contra tipos de impacto, el producto del valor de cada tipo de impacto a la Comisión por la viabilidad de materialización de cada riesgo. Los valores totales en la matriz representan el valor proporcional de los impactos asociados a cada riesgo de acuerdo con su viabilidad de materialización.

Una vez obtenidos los valores promedio de impacto por cada riesgo es necesario definir el valor porcentual que cada uno de estos representan, con el cual se puede determinar el nivel de impacto asociado a cada riesgo en las categorías de Insignificante, Menor, Moderado, Mayor y Catastrófico.

7) Determinar el nivel de riesgo.

Para determinar el nivel de riesgo asociado es necesario tener en cuenta los dos valores que definen un riesgo, la probabilidad de ocurrencia y el impacto. Los valores obtenidos previamente se ubican en la matriz de probabilidad de ocurrencia contra impacto del riesgo, figura 21.

Riesgo = Probabilidad x Impacto

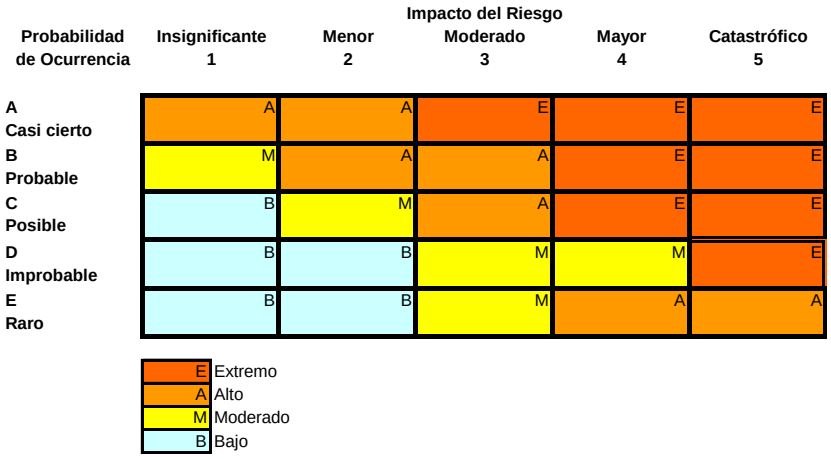


Figura 21. Nivel de riesgo

3.1.4 Estrategia de Recuperación

Los pasos para determinar la estrategia de recuperación son los siguientes:

1) Determinar la secuencia de recuperación de aplicaciones.

   Es necesario reestructurar el orden de acuerdo con las relaciones críticas establecidas en el análisis de interdependencias entre aplicaciones. Esto garantizará que al momento de recuperar una aplicación crítica, tendrá a su disposición toda la información, proveniente de otras aplicaciones, que pueden ser menos importantes, pero indispensables para ser recuperada exitosamente.

2) Definir el tipo de centro de datos (site) alterno así como el de replicación de datos

   La definición del tipo de site alterno así como del tipo de replicación de datos adecuados para la Comisión se realiza en función de los valores para los criterios de RTO y RPO.

   Los tipos de site alternos para recuperación ante desastres se muestran en la tabla 6.

Tipo	Descripción	RTO
Cold Site	Sitio con espacio físico, mobiliario para cierto número de personas y con los servicios básicos de infraestructura disponibles, por ejemplo: electricidad, agua corriente, aire acondicionado, cableado de voz y datos, terminales telefónicas, etc. Se requiere la instalación del software y los datos para poder poner el sistema productivo nuevamente.	> 1 y < 7 días
Warm Site	Similar al Cold Site, pero dispone de cierta infraestructura informática, como estaciones de trabajo con configuración básica y algunos servicios de redes tales como direccionamiento IP, servicios de nombres, autenticación, file and print, etc.	> 8 y < 24 horas
Hot Site Cold Start	Además de las características de un Warm Site, dispone de todo el hardware requerido tanto para el entorno cliente como servidor, pero el software debe ser cargado y configurado. Los datos no están disponibles.	241-480 minutos
Hot Site Standby	Además de las características de un Hot Site Cold Start, dispone de todo el hardware y software requerido configurado previamente, incluyendo una rápida disponibilidad de los datos. El hardware y el software están onfigurados para tomar la carga del servidor productivo, en caso que de que éste presente problemas.	6-240 minutos
Fault- Tolerant	Este sitio implica el mantenimiento de arquitecturas similares, sincronizadas en tiempo real, que garanticen disponibilidad de los servicios ante una interrupción.	0-5 minutos

Tabla 6. Tipos de site alterno.

Ahora bien, por lo que respecta a los tipos de replicación de datos, elementos asociados a los site alternos, tenemos los que se presentan en la tabla 7.

Tipo	Descripción
Synchronous Data Mirroring	Replicación síncrona de un conjunto de datos en una ubicación alternativa, frecuentemente utilizando tecnologías como Storage Área Network (SAN).
Asynchronous Data Mirroring	Replicación asíncrona de un conjunto de datos en un sitio alterno.
Tape Recovery (Daily Backup)	Es un proceso que replica datos almacenados en discos a un conjunto de cintas que luego son transportadas manualmente offsite.
Tape Recovery (No Daily Backup)	Es un proceso que replica datos almacenados en discos a un conjunto de cintas que luego son transportadas manualmente offsite y guardadas hasta que sean requeridas.

Tabla 7. Tipos de replicación

3) Determinar los elementos necesarios para la recuperación

Se determinan los siguientes elementos, necesarios para la recuperación:

a) Infraestructura tecnológica,

b) Personal vital y

c) Proveedores críticos

3.2 Conclusiones

Basados en las mejores prácticas, la elaboración tradicional de un Plan de Recuperación ante Desastres requiere de los siguientes pasos para su elaboración:

- Análisis de impactos al negocio, BIA.
- Evaluación de riesgos
- Establecer la estrategia, con apoyo de los datos anteriores, que se utilizará para llevar a cabo la recuperación ante un evento de desastre.

Sin embargo, la forma tradicional en la que se elabora, en ocasiones, da como resultado planes de alto nivel, sin mucho detalle, inclusive validados por los responsables de los procesos de negocio y de aplicaciones de la empresa en la que se realicen.

Además, si bien es cierto que este tipo de planes trae consigo beneficios a las organizaciones que los desarrollan, estos no se maximizan debido al enfoque parcial que se da al objeto de estudio.

Por tanto, la estrategia propuesta a desarrollar integrará un paso inicial, consistente en la definición del sistema, lo cual nos permitirá identificar los elementos que lo integran, sus relaciones entre sí y con el medio ambiente a fin de enfrentar los problemas comunes, cada vez más complejos, que presenta la elaboración de este tipo de planes y por tanto evitar los errores comunes que se tienen para su implantación.

El factor humano, aun cuando se ha considerado para la elaboración de este tipo de planes, debe reevaluarse a través de un adecuado análisis de stakeholders que permita la inclusión de todos los recursos necesarios para una adecuada definición del sistema.

Para la elaboración de un DRP se utilizará una herramienta automatizada que permita realizarla de una manera más sencilla y rápida.

CAPÍTULO 4. ESTUDIO DE CASO

4.1 Aplicación de la Estrategia

El sistema general se definió en base a las leyes y reglamento que dan fundamento legal a la Comisión Nacional de Seguros y Fianzas:

- Ley Orgánica de la Administración Pública Federal

  Artículos 17 y 19
- Ley General de Instituciones y Sociedades Mutualistas de Seguros

  Artículos 108, 108a, 108b, 108c y 109
- Ley Federal de Instituciones de Fianzas

  Artículos 68 y 69
- Reglamento Interior de la Comisión Nacional de Seguros y Fianzas

Por otro lado, para la elaboración del DRP se utilizó el software Mitigator. Se realizó la creación de cuentas de usuario para cada uno de los responsables de los procesos y aplicaciones establecidas, permitiéndoles el acceso en línea, para contestar las encuestas previamente definidas y almacenadas dentro de la base de datos con la que cuenta; lo cual, permite mantener la información completa y organizada ya que está dividida en áreas, oficinas y responsables. Esta información es la base para soportar el análisis que fue realizado y, permitirá mantenerla actualizada de una manera más ágil.

4.1.1 Definición del Sistema

En la figura 22 se presenta la Ubicación del sistema, considerando los elementos temporal, sectorial y espacial.

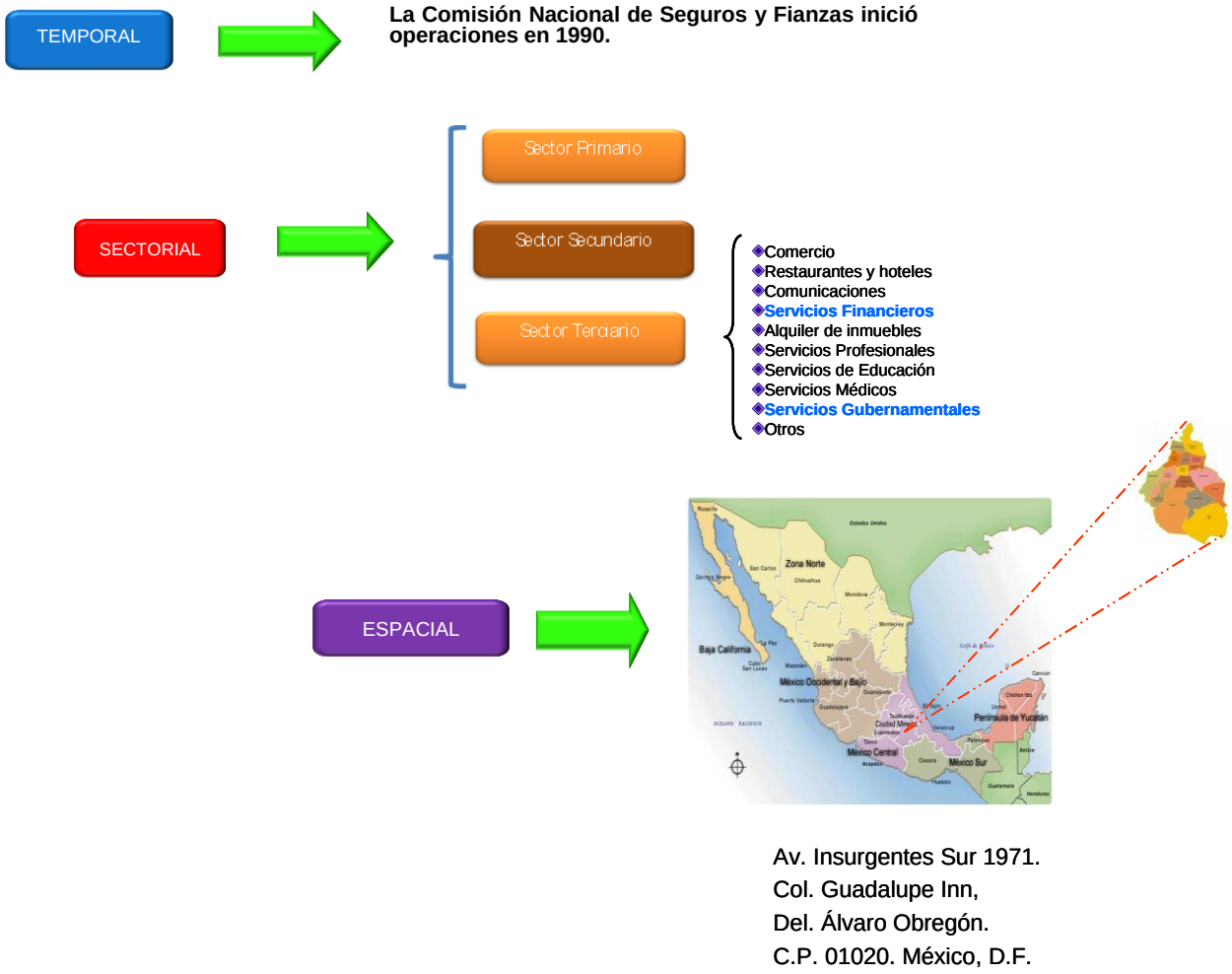


Figura 22. Ubicación del sistema CNSF

Modelo del sistema productivo en la Comisión Nacional de Seguros y Fianzas

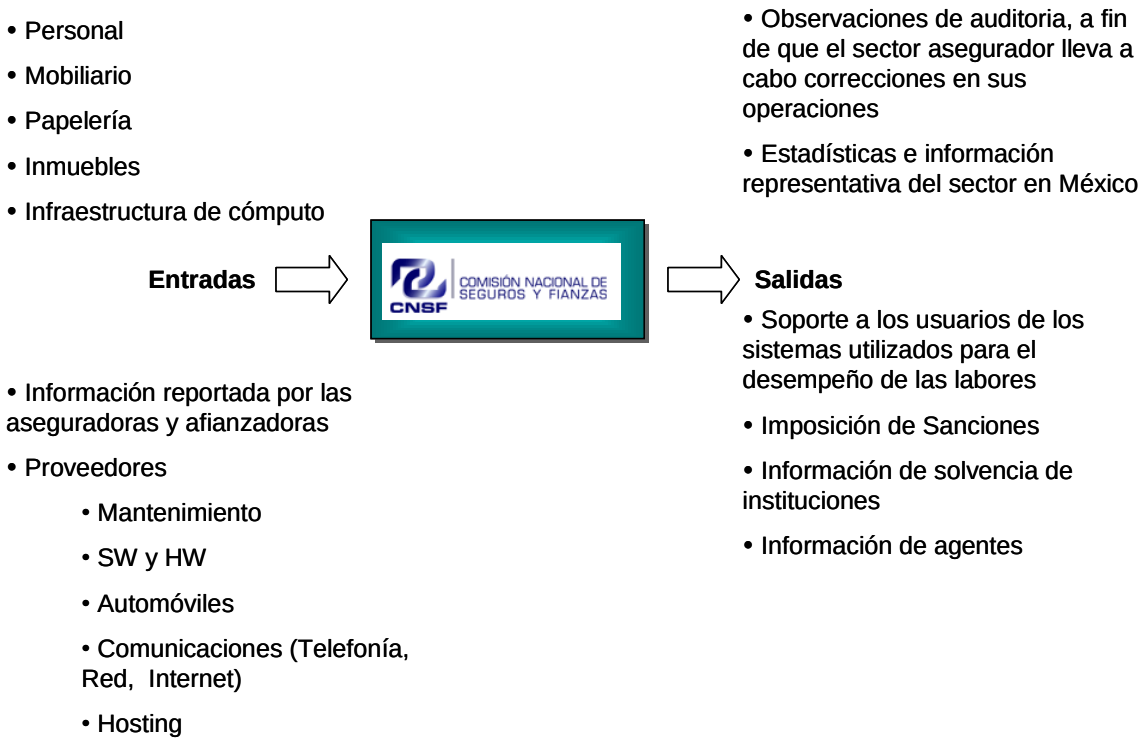
Partimos de un sistema productivo existente en operación que requiere el mejoramiento de sus procesos. Identificar el tipo de sistema con el que estamos tratando nos permite, a su vez, determinar el tipo de problema que enfrentaremos.

En la tabla 8 se enuncian la misión y visión de la Comisión Nacional de Seguros y Fianzas así como la misión de la Dirección General de Informática.

CNSF	**Misión**	Supervisar, de manera eficiente, que la operación de los sectores asegurador y afianzador se apegue al marco normativo, preservando la solvencia y estabilidad financiera de las instituciones, para garantizar los intereses del público usuario, así como promover el sano desarrollo de estos sectores con el propósito de extender la cobertura de sus servicios a la mayor parte posible de la población.
	Visión	Una CNSF cuya función supervisora opere bajo principios de eficiencia, eficacia y calidad acordes con los estándares internacionales en la materia, con el objeto de coadyuvar a la estabilidad y solvencia de las industrias aseguradora y afianzadora, como elemento para estimular la seguridad y confianza del público usuario de estos servicios financieros.
DGI	**Misión**	Crear un marco de arquitectura tecnológica, que integre, ordene, dicte y de referencia al desarrollo de la Comisión en esta materia. Aprovechar las oportunidades del uso de la tecnología para incrementar la productividad y eficiencia institucional. Disponer de la plataforma tecnológica que permita brindar servicios en cualquier lugar y en todo momento con altos niveles de seguridad. Generar una cultura de análisis y de evaluación del uso de la plataforma tecnológica

Tabla 8. Principios de la CNSF y de la DGI

El primer acercamiento al sistema productivo en la CNSF se presenta a continuación:



La Comisión Nacional de Seguros y Fianzas tiene como propósito fundamental establecer una efectiva coordinación entre sus unidades administrativas, así como su intervención en el esquema global de la supervisión de los sectores asegurador y afianzador; mismo que se

deriva de su fundamento legal y permite generar su modelo de sistema productivo correspondiente que se presenta en la figura 23.

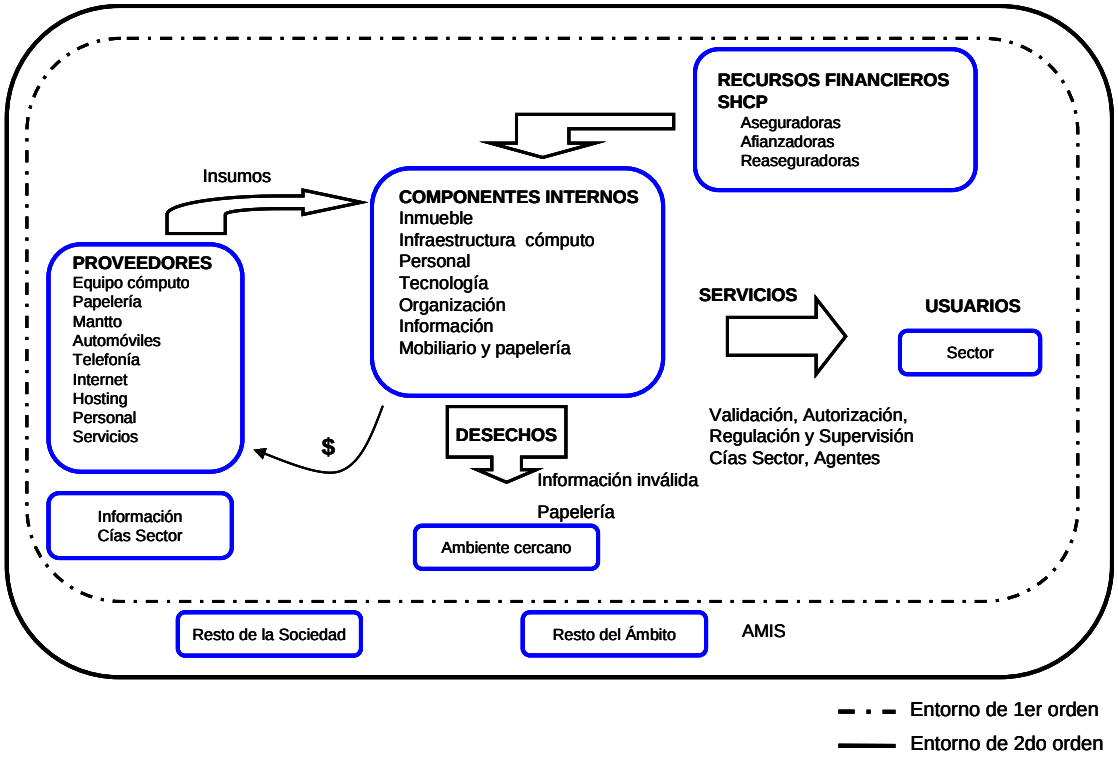


Figura 23. Modelo del sistema productivo en la Comisión Nacional de Seguros y Fianzas

A partir del sistema productivo en la CNSF, se obtiene por desagregación el correspondiente a la Dirección General de Informática, figura 24. En este caso, adicionalmente, se realizaron entrevistas a su personal, relativas a las actividades que realizan dentro de ésta.

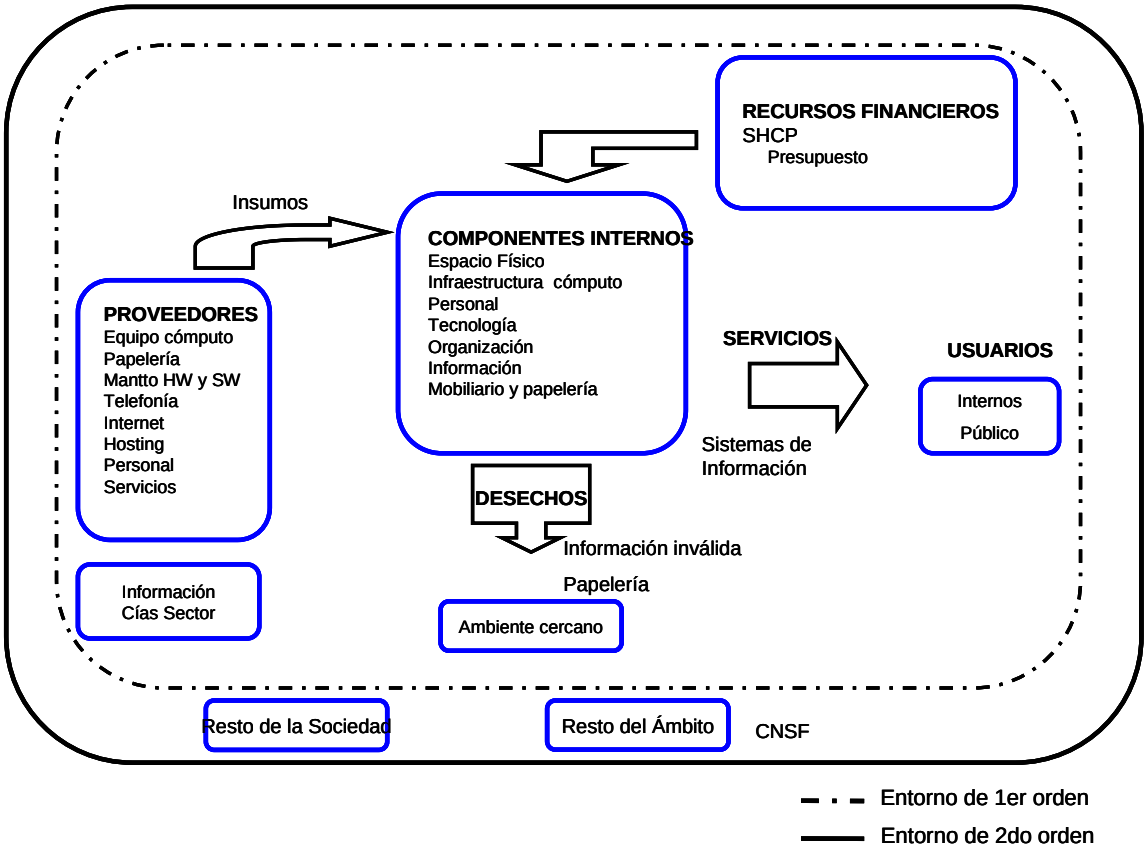


Figura 24. Modelo del sistema productivo en la Dirección General de Informática

4.1.2 Análisis de Impactos al Negocio

4.1.2.1 Definir las Aplicaciones Críticas

Como primer paso, la Dirección General de Informática determinó cuáles eran los procesos de Operación Institucional más críticos, considerando el papel que tienen en la consecución de los objetivos operativos de la Comisión, así como una primera relación de las aplicaciones que los soportaban.

En las áreas cubiertas por el análisis se llevó a cabo un estudio de las características de los procesos existentes así como de las aplicaciones, herramientas y registros vitales que soportan actualmente su realización.

Durante el desarrollo de las encuestas, se observó que no todas las aplicaciones definidas en el alcance inicial, soportaban todos los procesos y viceversa; por lo que, con el apoyo de los stakeholders se agregaron los procesos administrativos y jurídicos; así mismo, se agregaron nuevas aplicaciones.

El análisis de las encuestas realizadas permitió determinar las aplicaciones necesarias para la operación de los procesos críticos de la Comisión, así como la criticidad en tiempo (horas) de tolerancia sin la aplicación (RTO) y la cantidad máxima de transacciones (en horas) que se puede perder respectivamente.

A continuación se presentan, en las tablas 9 y 10 respectivamente, la relación de procesos y de aplicaciones correspondientes incluidas en el análisis:

Proceso	Responsable
Recursos Financieros	Jefe depto contabilidad
Recursos Humanos	Jefe depto nómina
Servicio Medico	Médico institucional
Desarrollo Sistemas	Subdirector
Control Calidad	Líder de proyecto
Atención Usuarios (MA)	Líder de proyecto
Soporte y Mantenimiento Sistemas Notes	Líder de proyecto
Base Datos	Jefe depto
Operación	Jefe depto
Atención Usuarios (SAI)	Líder de proyecto
Atención Redes	Jefe depto
Soporte Técnico	Líder de proyecto
Acreditación Actuarios	Subdirector
Operaciones Ilícitas	Subdirector
Inspección Actuarial	Director
Vigilancia Actuarial	Director
Inspección Financiera	Director
Vigilancia Financiera	Director
Inspección Reaseguro	Subdirector
Vigilancia Reaseguro	Director
Inspección Seguro Pensiones	Director
Vigilancia Seguro Pensiones	Director

Tabla 9. Procesos críticos CNSF.

Aplicación	
Cve	Nombre
IPR	Informe Periódico Reaseguro
IPRF	Informe Periódico Reafianzamiento
	Lavado Dinero
	Límites Retención
SAAC	Sistema Acreditación Actuarios
SAMA	Sistema Administración Mesa Ayuda
SIE	Sistema Información Ejecutiva
SIIF	Sistema Integral Información Financiera
SIMEPREV	Sistema Médico Prevención
SIRF	Sistema Integral Recursos Financieros
SIRH	Sistema Integral Recursos Humanos
	Sistema Agentes
	Sistema Control Gestión
	Sistema Despacho Documentos
SONR	Siniestros Ocurridos No Reportados
SUI	Sistema Único Inspección
SVC	Sistema Vigilancia Corporativa R2
UNICCO	Sistema Unificado Catálogo Compañías
VAR	Sistema Integral Información Financiera (VAR)
SEIVE	Sistema Entrega Información Vía Electrónica
	Módulos Explotación
SUC	Sistema Único Cotización
SAEA	Sistema Auditores Externos Actuariales
SAEF	Sistema Auditores Externos Financieros

Tabla 10. Aplicaciones críticas CNSF

Para determinar los criterios de recuperación (RTO y RPO) de las aplicaciones de la CNSF se emplearon los correspondientes a los de sus procesos soportados; los cuales, se obtuvieron a través de las encuestas realizadas al personal responsable. Estos datos se muestran en la tabla 11.

Aplicación		RTO, (hrs)	RPO, (hrs)
Cve	Nombre		
IPR	Informe Periódico Reaseguro	168	72
IPRF	Informe Periódico Reafianzamiento	168	72
	Lavado Dinero	48	72
	Límites Retención	720	200
SAAC	Sistema Acreditación Actuarios	168	168
SAMA	Sistema Administración Mesa Ayuda	24	48
SIE	Sistema Información Ejecutiva	24	24
SIIF	Sistema Integral Información Financiera	24	12
SIMEPREV	Sistema Médico Prevención	168	72
SIRF	Sistema Integral Recursos Financieros	24	48
SIRH	Sistema Integral Recursos Humanos	24	72
	Sistema Agentes	24	24
	Sistema Control Gestión	24	12
	Sistema Despacho Documentos	24	8
SONR	Siniestros Ocurridos No Reportados	720	200
SUI	Sistema Único Inspección	24	8
SVC	Sistema Vigilancia Corporativa R2	168	120
UNICCO	Sistema Unificado Catálogo Compañías	72	48
VAR	Sistema Integral Información Financiera (VAR)	168	120
SEIVE	Sistema Entrega Información Vía Electrónica	24	24
	Módulos Explotación	24	24
SUC	Sistema Único Cotización	24	24
SAEA	Sistema Auditores Externos Actuariales	24	24
SAEF	Sistema Auditores Externos Financieros	24	24

Tabla 11. Valores de RTO y RPO de las aplicaciones críticas de la CNSF

4.1.2.2 Definir el Impacto de las Interrupciones

Los tipos de impacto evaluados que pueden afectar a los procesos y por consecuencia a las aplicaciones se muestran en la tabla 12.

Impacto	
Tipo	Descripción
Seguridad de Información	Posibilidad de fuga de información, por divulgación inadecuada de información confidencial o por divulgación de información equivocada.
Procesos Internos	Impacto a otros procesos, en caso de que no reciban los insumos generados por el proceso evaluado.
Entidades Externas	Impacto a Entidades Externas (aseguradoras, afianzadores, etc.) por no recibir los insumos generados por el proceso evaluado.
Imagen	El impacto que la indisponibilidad del proceso puede generar en la imagen de la CNSF.
Moral de los Empleados	Puede generar necesidad de trabajo extra, indisposición con el liderazgo y con la empresa.
Eficiencia Operacional	Afectar cumplmiento de fechas, calidad del trabajo y del servicio.

Tabla 12. Tipos de impactos evaluados

El establecimiento de los impactos al negocio causado por la indisponibilidad del proceso, producto de la ausencia del soporte tecnológico, se realizó en categorías definidas de variables discretas (severidad), entre valores de 1 a 5, tabla 13.

Así mismo se definieron ventanas de tiempo para la CNSF buscando reflejar las posibles situaciones de impacto presentadas dentro de la organización, tabla 14.

Severidad	
1	No severo
2	Poco severo
3	Severo
4	Muy servero
5	Extremadamente severo

Tabla 12. Valores de severidad

Ventana de Tiempo	
Ventana	**Descripción**
< 1 hora	Los procesos más críticos son los que presentan impactos de manera casi inmediata;esta criticidad se presenta casi en el momento mismo de la interrupción.
> 1 hora, < 12 horas	Representa la interrupción de un proceso a lo largo de todo un día laboral y su respectivo impacto para la organización.
> 12 horas, < 24 horas	Busca identificar la criticidad de los procesos que deben operar las 24 horas del día y cuya interrupción no debe superar un día calendario.
> 24 horas, < 72 horas	Procesos cuya criticidad es estacionaria en los ciclos semanales de operación.
> 72 horas	Busca identificar los impactos frente a interrupciones de alta magnitud.

Tabla 14. Valores de ventanas de tiempo

Posteriormente, se definió para cada proceso cuál sería la severidad de su ausencia dentro de las ventanas de tiempo establecidas para cada tipo de impacto.

Para determinar los valores de los tipos de impacto para las aplicaciones es necesario relacionar los impactos de los procesos que son soportados por éstas. También debe considerarse en qué porcentaje depende el proceso de la aplicación y finalmente seleccionar los valores más altos de cada tipo de impacto, por cada ventana de tiempo.

4.1.2.3 Establecer las Relaciones entre Aplicaciones

Derivado de las respuestas de los responsables, tanto de los procesos como de las aplicaciones, relativas a la información que envían o reciben, fue posible generar un mapa de relaciones entre aplicaciones. Se presentan en color azul aquellas que se consideraron inicialmente y en color gris las que se incorporaron posteriormente, como resultado de la inclusión de personal externo a la DGI, figura 25.

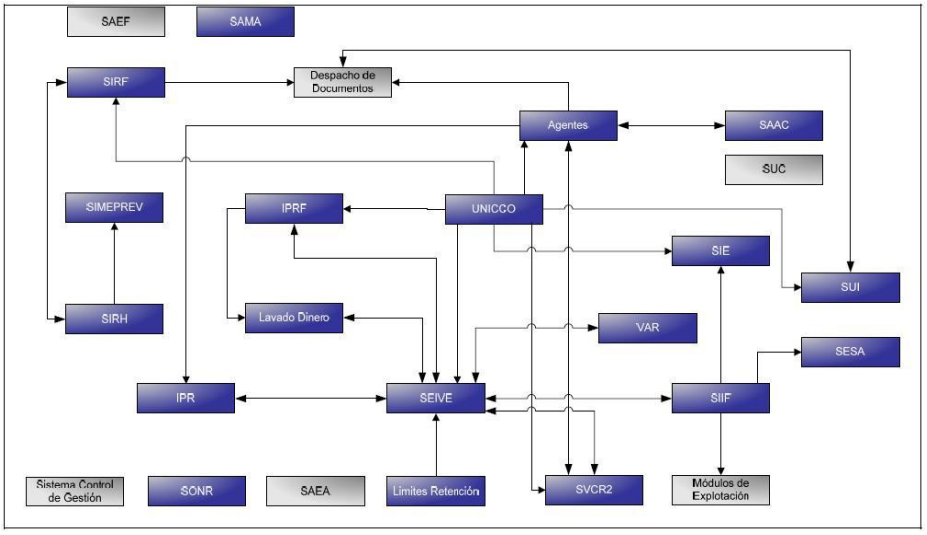


Figura 25. Relación entre las aplicaciones

También fue posible relacionar a las aplicaciones dentro de la infraestructura actual de producción de la Comisión. Por ejemplo, el Sistema de Control de Gestión se encuentra instalado en el servidor DSA, el cual a su vez tiene provisionado disco del servidor de almacenamiento. Esto se muestra en la figura 26.

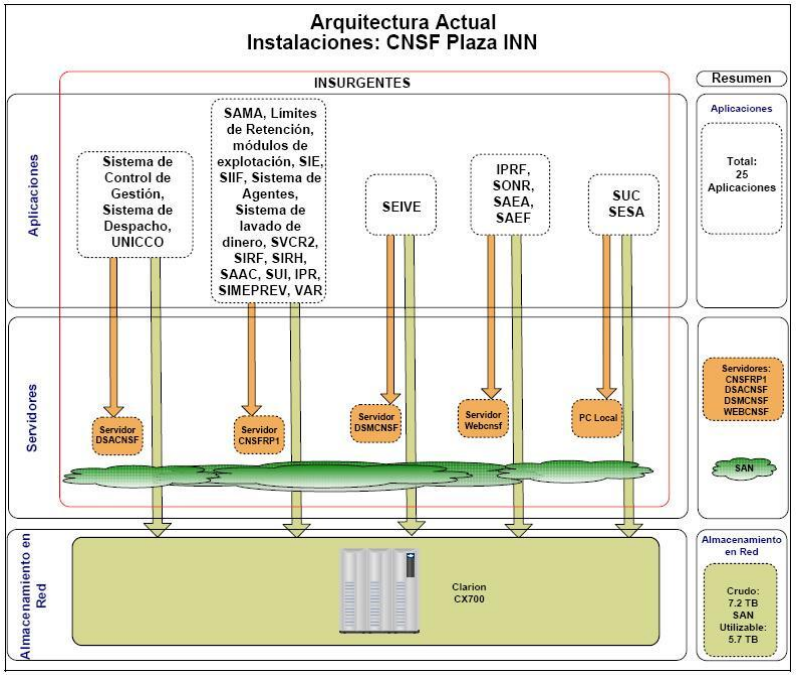


Figura 26. Arquitectura actual CNSF

Adicionalmente se determinaron otros elementos críticos de la operación, como lo son las Herramientas y los Registros Vitales. Como ejemplo respectivo, se determinó que las bases de datos Oracle son necesarias para el desarrollo de sistemas y que para la administración de éstas son necesarios los manuales correspondientes.

4.1.2.4 Determinar la Criticidad de las Aplicaciones

Para la determinación de la criticidad de las diferentes aplicaciones de la Comisión, deben ser considerados todos los criterios evaluados, a través de una asignación proporcional ponderada por el grado de importancia de cada uno de estos, de acuerdo a la estrategia funcional y operativa de la Comisión. Esta asignación se presenta en la tabla 15.

Concepto	Criterio	Ponderación, %
Recuperación	RTO	12
	RPO	10
Impacto	Seguridad de información	8
	Procesos internos	10
	Entidades externas	15
	Imagen	20
	Moral de empleados	3
	Eficiencia operacional	9
Interrelación	Aplicaciones afectadas	5
	Procesos afectados	8

Tabla 15. Criterios evaluados

Una vez que se calculan todos los porcentajes de cada aplicación, por cada criterio, se obtiene el total correspondiente a todos los criterios por aplicación. Como resultado se obtienen las aplicaciones más críticas definidas para la Comisión, mismas que se presentan en la tabla 16.

No	Aplicación	Total Puntaje Aplicación
1	Sistema Integral Información Financiera	88
2	Sistema Despacho Documentos	81
3	Sistema Información Ejecutiva	77
4	Sistema Único Inspección	67
5	Sistema Agentes	65
6	Sistema Auditores Externos Financieros	61
7	Sistema Entrega Información Vía Electrónica	56
8	Sistema Control Gestión	56
9	Sistema Administración Mesa Ayuda	52
10	Sistema Integral Recursos Humanos	51

Tabla 16. Aplicaciones críticas CNSF

Las aplicaciones de mayor puntaje representan las aplicaciones más críticas para la Comisión. No sólo requieren una recuperación rápida, lo que infiere soportar procesos críticos; sino que son poco tolerables a la pérdida de datos, lo que infiere que los procesos soportados son altamente sensibles a los cambios de información.

También impactan de manera significativa a un número importante de usuarios; este impacto es extensivo a varios procesos y aplicaciones interrelacionadas y soportadas por esas aplicaciones.

4.1.2.5 Establecer el Orden de Recuperación de las Aplicaciones

De acuerdo con los criterios establecidos para la definición de los tiers de aplicación, se presenta en la tabla 17 la relación de las aplicaciones establecidas y sus valores de RTO y RPO asociados.

Tier	Aplicación	RTO, (hrs)	RPO, (hrs)
Platinum	Sistema Despacho Documentos	24	8
	Sistema Único Inspección	24	8
	Sistema Integral Información Financiera	24	12
	Sistema Control Gestión	24	12
	Sistema Información Ejecutiva	24	24
	Sistema Agentes	24	24
	Sistema Entrega Información Vía Electrónic	24	24
	Módulos Explotación	24	24
	Sistema Único Cotización	24	24
	Sistema Auditores Externos Actuariales	24	24
	Sistema Auditores Externos Financieros	24	24
Gold	Sistema Administración Mesa Ayuda	24	48
	Sistema Integral Recursos Financieros	24	48
	Sistema Integral Recursos Humanos	24	72
Bronze	Lavado Dinero	48	72
	Sistema Unificado Catálogo Compañías	72	48
	Informe Periódico Reaseguro	168	72
	Informe Periódico Reafianzamiento	168	72
	Sistema Médico Prevención	168	72
	Sistema Vigilancia Corporativa R2	168	120
	Sistema Integral Información Financiera (VA	168	120
	Sistema Acreditación Actuarios	168	168
	Límites Retención	720	200
	Siniestros Ocurridos No Reportados	720	200

Tabla 17. Aplicaciones críticas CNSF con orden de recuperación.

4.1.3 Evaluación de Riesgos

4.1.3.1 Establecer las Posibles Amenazas

El equipo de TI estableció las posibles amenazas que pudieran afectar a la CNSF, así como su posibilidad de ocurrencia, asociándolas a una de las 5 categorías previamente establecidas. Así mismo, se les asignó un valor para su incidencia. La relación de amenazas consideradas se presenta en la tabla 18.

Amenazas					
Categoría	**No**	**Nombre**	**Ocurrencias**		**Valor**
Ambientales	1	Falla de electricidad	1	5 semanas	3
Hechas por personas	2	Corte de cables	2	1 década	1
	3	Incendio provocado	1	1 década	1
	4	Falla aire acondicionado	1	1 década	1
	5	Falla electricidad	1	2 años	1
	6	Inestabilidad de voltaje	1	4 años	1
Naturales	7	Terremotos	3.4	10 años	1
	8	Rayos	1.4	1 década	1
	9	Precipitaciones	5	10 décadas	1
Sociales	10	Explosión	1	2 décadas	1
	11	Disturbios	1	1 año	2
	12	Sabotaje	1	20 décadas	1
	13	Amenaza de bomba/Terrorismo	6	1 década	1
	14	Paros laborales	1	1 década	1
Falla de sistemas	15	Falla proveedores telefonía	1	5 años	1
	16	Falla de cableado comunicaciones	1	6 meses	3
	17	Falla equipos	2	6 meses	3
	18	Falla BD	1	1 día	5
	19	Robo por parte empleados	2	1 década	1
	20	Errores humanos	2	3 meses	3
	21	Falla PBX	1	1 año	2
	22	Fallas de SW	1	1 día	5
	23	Virus	1.5	1 semana	5

Tabla 18. Amenazas posibles para la CNSF

4.1.3.2 Determinar las Vulnerabilidades

Para determinar las vulnerabilidades se realizaron encuestas relativas a las Instalaciones y Centro de Datos de la CNSF. El objetivo de la primera era obtener toda la información posible acerca del edificio en el que se labora y de la infraestructura con la que se cuenta como fuentes de poder, cableado eléctrico, métodos de detección y combate de incendios, etc.

Por su parte la encuesta del Centro de datos se enfocó en todas las actividades que se llevan a cabo dentro de éste, como la administración del almacenamiento y la seguridad de TI.

Las respuestas se analizaron y agruparon en un diagrama causa-efecto, determinando una alta exposición al riesgo operacional. Se detectaron 5 vulnerabilidades principales:

- Continuidad

  Inexistencia de niveles de servicio y criterios adecuados para tolerancia de pérdida de información. Las políticas de administración de datos no son divulgadas, y el personal no tiene capacitación para entender sus funciones y responsabilidades.

- Administración de respaldos

  Los respaldos son realizados diariamente, pero pocas o nulas son las necesidades de recuperación, no indicando la real necesidad de pruebas. No hay monitoreo y tampoco un programa de mejora continua.

- Administración de almacenamiento

  No existe infraestructura de alta disponibilidad. La dependencia de los procesos sobre tecnología es grande y pocos son los procedimientos alternos para actuar en caso de indisponibilidad de sistemas.

- Control de acceso

  No existe un esquema de seguridad distinto para las áreas de la empresa (existe a los pisos, y a sala de producción, pero no evita la entrada con otra persona). La entrada a la empresa es controlada por la seguridad del edificio, que tiene una política general para todas las organizaciones que pertenecen al edificio.

- Seguridad informática

  Hay posibilidades de fuga de información, ya que no existe una política clara de confidencialidad de información, no se utiliza criptografía y se cuenta con pocos procedimientos de protección a la información.

A continuación, en la figura 27, se presenta el diagrama causa-efecto realizado:

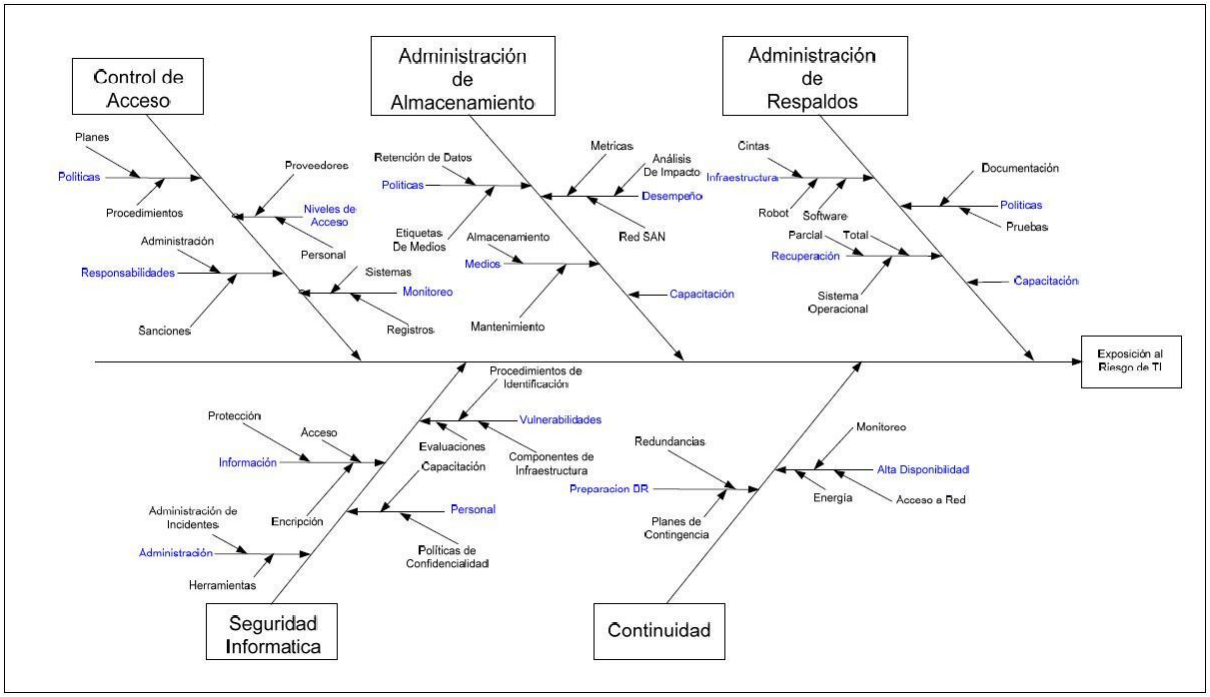


Figura 27. Diagrama causa-efecto

4.1.3.3 Determinar los Posibles Riesgos

Una vez determinadas las vulnerabilidades de la operación y teniendo en cuenta las diferentes amenazas del entorno que podrían materializar un riesgo, es necesario establecer los posibles riesgos asociados, tabla 19:

Vulnerabilidad	Riesgo Asociado
Administración de Almacenamiento	Niveles de servicio comprometidos, con aplicaciones afectadas y posible pérdida de información.
Administración de Respaldos	Pérdida de información crítica para el negocio, que puede no recuperarse.
Continuidad	Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.
Control de Acceso	Exposición de la información confidencial manejada por la Comisión, ya sea por error o como consecuencia de un acto malintencionado.
Seguridad Informática	Pérdida o alteración de información por no contar con un esquema adecuado de protección de los sistemas de información y de la custodia interna y externa de los respaldos.

Tabla 19. Riesgos asociados a vulnerabilidades

4.1.3.4 Medir las Vulnerabilidades

En la matriz de incidencias, tabla 20, se determina como las vulnerabilidades son impactadas por cada amenaza existente; por ejemplo, una falla de electricidad puede impactar al almacenamiento, al respaldo, la continuidad y el control de acceso.

Vulnerabilidad / Amenaza	Administración de Almacenamiento	Administración de Respaldos	Continuidad	Control de Acceso	Seguridad Informática	Total Amenazas
Falla de electricidad (amb)	X	X	X	X		**4**
Corte de cables	X	X	X	X		**4**
Incendio provocado	X	X	X	X		**4**
Falla aire acondicionado	X		X			**2**
Inestabilidad de voltaje	X					**1**
Terremotos	X	X	X	X		**4**
Rayos	X	x	X	X		**4**
Precipitaciones			X	X		**2**
Explosión			X	X		**2**
Disturbios			X	X		**2**
Sabotaje	X	X		X	X	**4**
Amenaza de bomba/Terrorismo			X	X		**2**
Paros laborales			X		X	**2**
Falla proveedores telefonía			X			**1**
Falla de cableado comunicaciones	X	X	X			**3**
Falla equipos	X	X	X	X		**4**
Falla BD	X	X	X	X		**4**
Robo por parte empleados				X	X	**2**
Errores humanos	X	X		X	X	**4**
Falla PBX			X			**1**
Fallas de SW	X	X			X	**3**
Virus	X				X	**2**
Total Vulnerabilidades	**14**	**11**	**16**	**14**	**6**	

Tabla 20. Matriz de incidencias

4.1.3.5 Determinar la Probabilidad de Ocurrencia de un Riesgo

A partir de la matriz de incidencias, se determinan los valores de los coeficientes promedio de riesgo así como el de la mayor cantidad de veces que se repite un riesgo, N, de 16; lo cual permite establecer, en la matriz de probabilidad de ocurrencia de un riesgo, figura 28, los rangos de incidencias de riesgo.

		No. Incidencias de Riesgo en la Matriz de Vulnerabilidades vs Amenazas				
		[1-3]	[4-6]	[7-10]	[11-13]	[14-16]
Coeficiente Promedio de Riesgo	[21-15]	B	B	A	A	A
	[16 -20]	C	B	B	A	A
	[11-15]	C	C	B	B	A
	[6-10]	D	**5** **D**	C	**2** **C**	**1** **C**
	[1-5]	E	E	D	D	**3, 4** **C**

Figura 28. Matriz de probabilidad de ocurrencia de un riesgo.

Como puede observarse, la mayor parte de los riesgos tiene una probabilidad de tipo C, lo que significa que es posible su manifestación de acuerdo a las características actuales de operación. En la tabla 21 se presentan estos resultados.

	Riesgo	Coeficiente Prom de Riesgo	Incidencias	Probabilidad
1	Niveles de servicio comprometidos, con aplicaciones afectadas y posible pérdida de información.	7	14	C
2	Pérdida de información crítica para el negocio, que puede no recuperarse.	7	11	C
3	Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.	4	14	C
4	Exposición de la información confidencial manejada por la Comisión, ya sea por error o como consecuenca de un acto malintencionado.	3	14	C
5	Pérdida o alteración de información por no contar con un esquema adecuado de protección de los sistemas de información y de la custodia interna y externa de los respaldos.	9	6	D

Tabla 21. Probabilidad de ocurrencia de un riesgo.

4.1.3.6 Determinar el Nivel de Impacto

La relación existente entre los riesgos identificados y los tipos de impactos definidos, de acuerdo con la posibilidad de materialización del riesgo para la Comisión, se presentan en la matriz de riesgos contra tipos de impactos, tabla 22.

Riesgo	Impacto					
	Seguridad	Procesos Internos	Entidades Externas	Imagen	Moral	Eficiencia Operacional
Niveles de servicio comprometidos, con aplicaciones afectadas y posible pérdida de información.				x	x	x
Pérdida de información crítica para el negocio, que puede no recuperarse.		x	x	x		x
Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.	x	x	x	x	x	x
Exposición de la información confidencial manejada por la Comisión, ya sea por error o como consecuencia de un acto malintencionado.	x	x		x	x	
Pérdida o alteración de información por no contar con un esquema adecuado de protección de los sistemas de información y de la custodia interna y externa de los respaldos.	x	x	x	x		

Tabla 22. Matriz de riesgos contra tipos de impactos.

Por ejemplo, la pérdida de información crítica afecta a la Comisión tanto internamente, a nivel de la realización de sus procesos y su eficiencia operacional, como a las entidades externas que dependen de dicha información, afectando por tanto su imagen.

Para determinar el nivel de impacto del riesgo es necesario considerar:

a) El valor ponderado asignado a cada impacto, tabla 23

Impacto	Ponderación
Seguridad Información	8%
Procesos Internos	10%
Entidades Externas	15%
Imagen	20%
Moral Empleados	3%
Eficiencia Operacional	9%
Total	65%

Tabla 23. Valores ponderados de impactos

b) El número total de incidencias de cada riesgo con el fin de asignar valores proporcionales, tabla 24.

Riesgo	%	Total Incidencias
Niveles de servicio comprometidos, con aplicaciones afectadas y posible pérdida de información.	88	14
Pérdida de información crítica para el negocio, que puede no recuperarse.	69	11
Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.	100	16
Exposición de la información confidencial manejada por la Comisión, ya sea por error o como consecuencia de un acto malintencionado.	88	14
Pérdida o alteración de información por no contar con un esquema adecuado de protección de los sistemas de información y de la custodia interna y externa de los respaldos.	38	6

Tabla 24. Total de incidencias por riesgo

Los valores obtenidos se presentan en la tabla 25, mismos que permiten determinar el nivel de impacto asociado a cada riesgo:

Riesgo	Ponderación %	Promedio	Valor %	Nivel Impacto
Niveles de servicio comprometidos, con aplicaciones afectadas y posible pérdida de información	43	0.9	**18**	**Menor**
Pérdida de información crítica para el negocio, que puede no recuperarse.	57	1.4	**29**	**Moderado**
Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.	100	2.1	**41**	**Moderado**
Exposición de la información confidencial manejada por la Comisión, ya sea por error o como consecuencia de un acto malintencionado.	55	0.7	**15**	**Menor**
Pérdida o alteración de Información por no contar con un esquema adecuado de protección de los sistemas de información y de la custodia interna y externa de los respaldos.	31	0.6	**12**	**Menor**

Tabla 25. Nivel de impacto asociado a cada riesgo.

4.1.3.7 Determinar el Nivel de Riesgo

De acuerdo con los niveles de impacto y probabilidad de ocurrencia obtenidos previamente, se determina utilizando la matriz de probabilidad de ocurrencia contra el impacto del riesgo, el nivel de riesgo para cada posible riesgo como se presenta a continuación en la tabla 26:

Riesgo	Probabilidad de Ocurrencia	Nivel Impacto	Nivel Riesgo
Niveles de servicio comprometidos, con aplicaciones afectadas y posible pérdida de información.	Posible	Menor	**Moderado**
Pérdida de información crítica para el negocio, que puede no recuperarse.	Posible	Moderado	**Alto**
Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.	Posible	Moderado	**Alto**
Exposición de la información confidencial manejada por la Comisión, ya sea por error o como consecuencia de un acto malintencionado.	Posible	Menor	**Moderado**
Pérdida o alteración de información por no contar con un esquema adecuado de protección de los sistemas de información y de la custodia interna y externa de los respaldos.	Improbable	Menor	**Bajo**

Tabla 26. Nivel de riesgo.

4.1.4 Estrategia de Recuperación

Cómo se mencionó en la sección de Análisis de Impactos al Negocio, los tiers de aplicación establecidos definen la prioridad de la recuperación, más no directamente la secuencia de la misma.

4.1.4.1 Determinar la Secuencia de Recuperación de Aplicaciones

El nuevo orden de recuperación tomando en cuenta las relaciones críticas establecidas en el análisis de interdependencias entre aplicaciones se presenta en la tabla 27:

Posición	Aplicación		RTO (hrs)	RPO (hrs)
	Clave	Nombre		
1		Sistema Despacho Documentos	24	8
2		Sistema Control Gestión	24	12
3		Módulos Explotación	24	24
4	UNICCO	Catálogo Unificado Compañías	72	48
5	SUI	Sistema Único Inspección	24	8
6	SIIF	Sistema Integral Información Financiera	24	12
7		Sistema Agentes	24	24
8	SIE	Sistema Información Ejecutiva	24	24
9	SAEF	Sistema Auditores Externos Financieros	24	24
10		Limites Retención	720	200
11	SEIVE	Sistema Entrega Información Vía Electrónica	24	24
12	SUC	Sistema Único Cotización	24	24
13	SAEA	Sistema de Auditores Externos Actuariales	24	24
14	SAMA	Sistema Administrativo Mesa Ayuda	24	48
15	SIRF	Sistema Integral Recursos Financieros	24	48
16	SIRH	Sistema Integral Recursos Humanos	24	72
17	IPRF	Informe Periódico Reafianzamiento	168	72
18		Lavado Dinero	48	72
19	IPR	Informe Periódico Reaseguro	168	72
20	SIMEPREV	Sistema Médico Prevención	168	72
21	SVC	Sistema Vigilancia Corporativa R2	168	120
22	VAR	Sistema Integral Información Financiera (VAR)	168	120
23	SAAC	Sistema Acreditación Actuarios	168	168
24	SONR	Siniestros Ocurridos y No Reportados	720	200

Tabla 27. Secuencia de recuperación de aplicaciones.

4.1.4.2 Definir el Tipo de Site Alterno así como el de Replicación de Datos

De acuerdo con los criterios de recuperación de las aplicaciones más críticas, el site alterno y el tipo de replicación de datos más adecuados para la Comisión, se presentan en la figura 29, siendo estos warm standby y asynchronous respectivamente.

RPO / RTO	Synchronous Data Mirroring	Asynchronous Data Mirroring	Tape Recovery (Daily Backup)	Tape Recovery (No Daily Backup)
	0 < 3 horas	1 < 24 horas	12 > 36 horas	>36 horas
Fault Tolerant — 1 – 5 minutos				
Hot Site Standby — 5 – 240 minutos				
Hot Site Cold Start — 240 - 480 minutos				
Warm Standby — 1 – 24 horas		X		
Cold Standby — 1 – 7 días				
No DR Standby — 1 – 2 semanas				

Figura 29. Tipo de site alterno y de replicación de datos propuesto

La forma en que la CNSF debe evolucionar a un Warm Site, se muestra gráficamente en la figura 30:

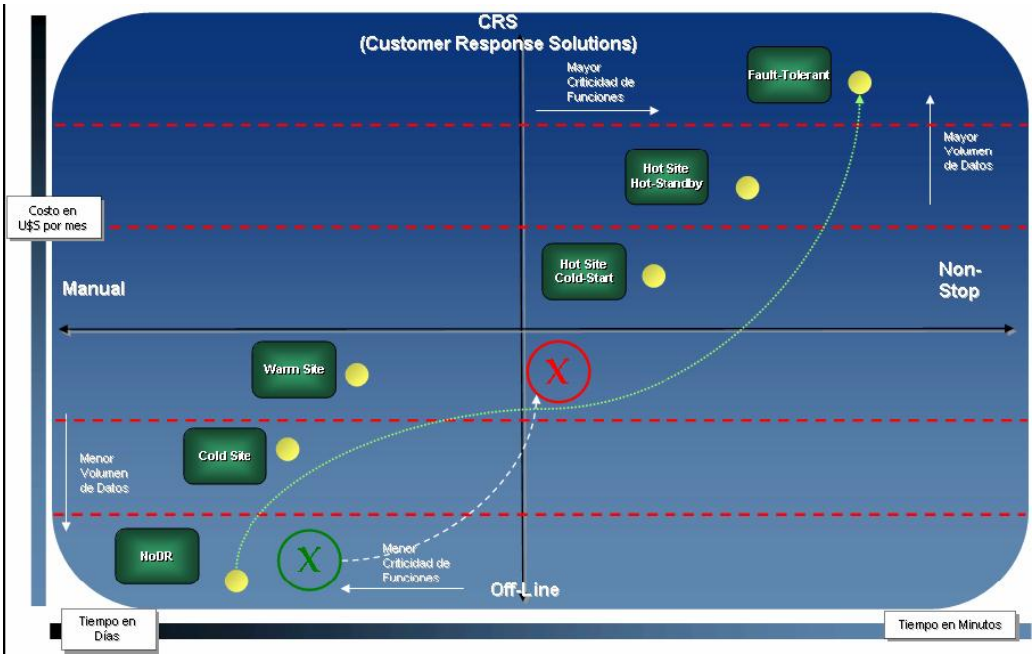


Figura 30. Evolución de tipo de site alterno

4.1.4.3 Determinar los Elementos Necesarios para la Recuperación

Con la información obtenida previamente, se determinó que las aplicaciones a ser recuperadas en el sitio alterno corresponden a los tiers Platino y Oro, así como los elementos que integran la plataforma Lotus Domino (aplicaciones y correo).

Adicionalmente, se debe incluir las herramientas y registros vitales identificados como críticos por los usuarios de negocios, la herramienta DRP de Evergreen (Mitigator Administrador), servicios de nombres DNS, firewall, balanceadores, etc, así como el servicio de administración de respaldos.

a) Infraestructura Tecnológica

A continuación, en la figura 31, se presenta la infraestructura tecnológica necesaria para la recuperación de los servicios críticos que provee el área de TI, a ser implementada en un sitio alterno

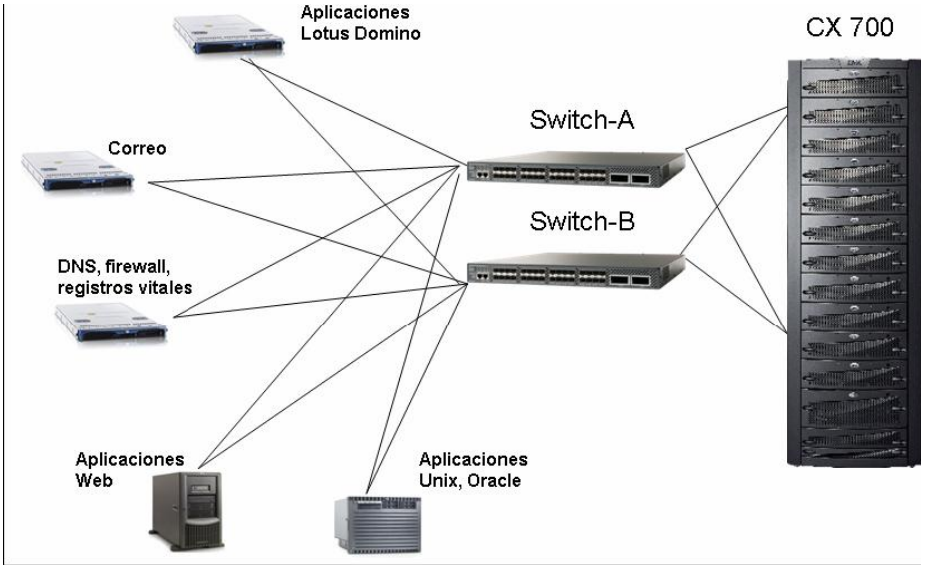


Figura 31. Infraestructura tecnológica propuesta.

b) Personal Vital

El personal vital para la recuperación inicial de los procesos críticos proporcionados por la DGI se presenta en la tabla 28.

Personal Vital para Recuperación
Jefe Depto Base Datos
Jefe Depto Operación
Jefe Depto Redes
Líder Proyecto Soporte Técnico
Líder Proyecto Control Calidad
Subdirector Desarrollo Sistemas
Líder Proyecto Soporte Mantenimiento Sistemas Notes

Tabla 28. Personal vital.

c) Proveedores Críticos

Para el caso de apoyo a recuperación en sitio alterno, hay que considerar los distintos proveedores críticos que proporcionan soporte a la infraestructura tecnológica de la CNSF, siendo estos los que se muestran en la tabla 29:

Proveedores	
Hardware	HP
	Dell
	EMC
Software	IBM
	Oracle
Servicios	Infotec

Tabla 29. Proveedores críticos.

4.2 Conclusiones

En términos generales, el Estudio de Caso permitió obtener los resultados esperados en cada una de las etapas de la elaboración tradicional de un DRP. Así mismo, servir para retroalimentar el trabajo de investigación y mejorar la estrategia propuesta. A continuación se presentan los logros obtenidos, destacando aquellos que se derivan de conceptualizar al objeto de estudio (CNSF) como un sistema.

Análisis de Impactos al Negocio

El mapa de relaciones entre aplicaciones se enriqueció, ya que el alcance inicial, planteado por la DGI, no tenía considerados procesos y aplicaciones que se derivaron de las respuestas de responsables externos al área de TI.

Evaluación de Riesgos

El un diagrama causa-efecto, las causas principales determinaron las vulnerabilidades a las que se encuentra expuesta la CNSF. En la estrategia el grado de influencia o peso que tienen las causas individuales sobre el efecto se determina a través del nivel de impacto de cada riesgo asociado.

De acuerdo con esta evaluación los principales riesgos (nivel alto) en la Comisión son:

- Pérdida de información crítica para el negocio, que puede no recuperarse.
- Indisponibilidad de tecnología y falta de procedimientos alternos adecuados para manejar tal situación en momento crítico.

En este caso, las acciones tendientes hacia la mitigación del riesgo deben enfocarse a la disminución de la probabilidad de su ocurrencia, disminuyendo las vulnerabilidades detectadas en la operación sobre estos aspectos.

Para los riesgos de nivel moderado es importante establecer una estrategia de mediano plazo que permita llevar a cabo una mitigación de las consecuencias de la materialización del riesgo.

Estrategia de Recuperación

El site alterno y el tipo de recuperación de datos más adecuados para la CNSF son el warm standby y el asynchronous data mirroring respectivamente. Este alternativa no es muy costosa, porque no requiere arquitectura compleja de replicación ni tampoco la construcción de un site alterno.

Es posible utilizar una oficina ya existente, o arrendar un espacio con empresas que ofrecen este tipo de servicio. Se propone la oficina de archivo ubicada en Av. Universidad, para facilitar el traslado de personas y cintas, rapidez de pruebas y recuperación.

Se estableció que los servicios tecnológicos más importantes que deben realizarse en el site alterno son la recuperación de las aplicaciones correspondientes a los tiers de aplicación Platino y Oro, así como la plataforma Lotus Domino. En esta última se consideran servicios de correo y aplicaciones integrados, por lo que no se pueden considerar de forma individual.

Posteriormente otros servicios deben ser recuperados, una vez que los procesos más críticos de la CNSF estén operando e inicie el regreso a la normalidad. Para esto, es necesario involucrar al personal de producción y los responsables de las aplicaciones, porque conocen su funcionamiento y pueden realizar pruebas.

CAPÍTULO 5. CONCLUSIONES GENERALES

El Plan de Recuperación ante Desastres desarrollado en la Comisión Nacional de Seguros y Fianzas permite tener un elemento vital para su estabilidad, no sólo a largo plazo, al estar preparada para la mayoría de los desastres potenciales; hoy en día le representa la posibilidad de brindar a las entidades reguladas y a sus usuarios los compromisos contraídos de una manera satisfactoria, al poder mantener la continuidad de sus prácticas de negocios. Redundándole en una mayor credibilidad e imagen.

El proceso de creación requirió de un gran esfuerzo para su realización; sin embargo, el resultado obtenido lo justificó plenamente. Con la elaboración del DRP se da el primer paso para el establecimiento de un Plan de Continuidad del Negocio, en el cual los sistemas informáticos son considerados de apoyo a los procesos de negocio.

La responsabilidad de su elaboración se compartió, desde su justificación hasta su elaboración. Los directivos respondieron ante la necesidad del mismo, aprobándolo, estableciendo su alcance y asignando los recursos financieros necesarios, mientras que, una parte del personal participó no sólo en su creación, sino también en su preparación para saber qué papel deben desempeñar en el proceso de recuperación ante desastres en caso de que se requiera llevar a cabo.

El empleo del software de continuidad del negocio Mitigator, de Evergreen, permitió a los responsables de procesos y aplicaciones responder en línea, de una manera ágil, los cuestionarios elaborados y almacenar en su base de datos las respuestas generadas. Con esto se tuvo un mayor control sobre esta información, empezando en el momento de afinar las respuestas sobre las que existían dudas, a través de entrevistas directas con el personal, y continuará en el momento en que se le realice mantenimiento en el futuro.

La elaboración del DRP, a través de la estrategia elaborada, nos ha permitido reafirmar las siguientes consideraciones:

- Se tiene un contexto global cada vez más complejo y competido.
- Las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos.
- Existe una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas de clientes (en el caso de la CNSF, de sus entidades reguladas) y usuarios.
- Los procesos eficaces y eficientes de la Gestión de Servicios de Tecnología de la Información se convierten en esenciales para el éxito de los departamentos de Tecnología de la Información.
- Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada.
- El servicio debe ser fiable, consistente, de alta calidad, y de costo aceptable.

Ahora bien, por lo que refiere a Enfoque de Sistemas, efectivamente desempeñó un papel fundamental en la estrategia, al permitir conceptualizar al objeto de estudio, la CNSF, como un sistema; lo cual, ayudó a evitar los errores comunes que se presentan en la implantación de un DRP y, sobretodo, a ampliar los beneficios y ventajas que se obtienen con este tipo de

planes. Por ejemplo, obtener una mejor comprensión de la organización como un todo, de su infraestructura, procesos, interrelaciones e inclusive de las personas; lo cual, indudablemente ayudarán a mejorarla en el corto plazo.

Por lo tanto se puede afirmar que el Enfoque de Sistemas es indispensable para los responsables de la gestión de servicios de TI, ya que les permite abordar de una mejor manera la problemática de las organizaciones y obtener mejores soluciones acordes al contexto.

También, es conveniente mencionar que el proceso para legitimar el desarrollo del DRP permitió crear conciencia y compromiso por parte de todos los responsables de procesos y aplicaciones involucrados.

La mejor forma de evaluar la efectividad del Plan de Recuperación ante Desastres desarrollado ha sido la realización de pruebas de funcionalidad de sus elementos en el Site Alterno establecido; éstas nos han permitido, inicialmente, validar que se ha contratado toda la infraestructura de hardware y software necesaria, así como comprobar que se cuenta con los recursos humanos necesarios, tanto internos como externos (incluidos los proveedores) para realizar las actividades relacionadas que nos permitan alcanzar los objetivos planteados en el Plan citado.

Al considerar a la Comisión como un sistema, se han establecido las relaciones entre sus componentes y por tanto entre sus procesos y aplicaciones, lo cual se ha validado al momento de poner en funcionamiento los componentes de una plataforma específica, como por ejemplo Lotus, sin requerir ningún elemento adicional a los considerados en los estudios realizados.

Las formas de respaldar y de replicar seleccionadas nos han permitido alcanzar los RPO y RTO definidos; sin embargo, se han identificado posibles alternativas para la realización de este tipo de actividades que nos permitan mejorar los tiempos de recuperación y disminuyan los datos perdidos.

Las pruebas realizadas han permitido que el personal conozca mejor el papel que juega dentro del proceso de recuperación, consiga una mayor especialización en éste e inclusive aporte opciones para afinar las actividades específicas que realiza, permitiendo disminuir los tiempos empleados en éstas y la posibilidad de error.

5.1 Estrategia Propuesta

La Teoría General de Sistemas fue un elemento importante en la síntesis interdisciplinaria, ya que satisface las exigencias actuales de los responsables de la gestión de servicios de TI, relativas al generalismo y a la exposición de “principios básicos” interdisciplinarios.

Adicionalmente, el Enfoque de Sistema desempeñó un papel fundamental en la elaboración de la Estrategia para Implantar un Plan de Recuperación ante Desastres en la Comisión nacional de Seguros y Fianzas. No sólo al problema, por sí mismo, se le dio solución, sino también a aquellos que históricamente han impedido resolverlo plenamente y, permitió ampliar los beneficios y ventajas que este tipo de planes traen consigo. Así mismo, se ratificó su utilidad ante un problema complejo, dependiente en gran medida de acciones pasadas y en donde se requería una coordinación eficaz entre los implicados.

El uso de la herramienta Mitigator, de Evergreen, facilitó el proceso de conducción del BIA, de la Evaluación de Riesgos y de la Estrategia de Recuperación en un tiempo menor a la elaboración cuando no se usan herramientas automatizadas. Se empleó para la elaboración de los cuestionarios e incluso para la logística de las entrevistas y el análisis de los datos. Los modelos de cuestionarios que la herramienta ofrece se adaptaron a la realidad de la CNSF.

Cada una de las etapas de la elaboración de un DRP tradicional se realizaron satisfactoriamente, por lo tanto se cumplieron los objetivos particulares planteados inicialmente. En adición, al conceptualizar al objeto de estudio (CNSF) como un sistema se obtuvieron beneficios en cada una de las etapas de la elaboración de un DRP tradicional. Como ejemplo puede citarse la inclusión de un mayor número de procesos y aplicaciones al definido inicialmente. Aunque, cabe citar que esta reconsideración también fue consecuencia de un análisis de stakeholders, que resultó en la inclusión de personal externo al del área de Tecnología de Información. Otras ventajas ya fueron mencionadas en el capítulo previo.

El Análisis de Impacto al Negocio y la Evaluación de Riesgos realizadas constituyen los principales cimientos para crear la base fundamental en que se apoyan los planes de continuidad de Tecnología de Información y del Negocio que toda empresa debe lograr. Estos cimientos que DRII (Disaster Recovery Intitute International) los denomina Requerimientos Funcionales, constituyen las primeras fases en la metodología a utilizar en la elaboración de los planes de Recuperación ante Desastres y de Continuidad del Negocio.

5.2 Estudio de Caso

Como se planteó en la Introducción, uno de los objetivos particulares de este trabajo fue la realización de un Estudio de Caso que permitiera retroalimentar el trabajo de investigación y mejorar la estrategia propuesta.

Durante la realización del Estudio de Caso, como se esperaba, se determinó la necesidad de mayor información relativa tanto al desarrollo de un DRP como a los conceptos de sistemas, lo cual, obligó a la búsqueda de información adicional para validar y en algún caso ajustar la estrategia; por lo que, el proceso de retroalimentación cumplió su función primordial: estabilizar las acciones necesarias para alcanzar una meta, redundando a su vez en la mejora de la estrategia.

5.3 Líneas de Acción a Desarrollar

Convertir al DRP en una Política

Los planes de recuperación ante desastres son útiles sólo cuando se encuentran dentro de las políticas de la compañía. Por lo tanto, el personal directivo necesita emitir declaraciones claras que hagan conciencia de estos. Con el fin de que sean más eficaces se necesita pasar del papel a la realidad práctica. Deben ser probados y actualizados de forma regular por todo el personal en la organización que participa en la planeación o que tiene alguna responsabilidad en la ejecución de lo que se ha planeado. Así mismo, todos los empleados deben conocer los procedimientos del plan y cuál es su papel en el proceso de recuperación en caso de una emergencia.

Probar el plan en un entorno simulado puede ser muy útil. Esto mostrará si el plan se puede aplicar en la vida real si un caso de desastre se produce. Esta práctica también sacará a la luz algunos elementos no considerados en el plan. Además esto ayudará a los empleados a permanecer en calma y confiados acerca de las acciones que tendrán que tomar si hay crisis, que por extensión, ayudará a la empresa a regresar a un estado normal de operación con gran rapidez.

Dar Mantenimiento al DRP

La implementación de un plan de recuperación ante desastres que funcione sin problemas y tenga éxito depende en gran medida del desempeño de las personas a las que se les asigne la responsabilidad de esta actividad. Con el fin de tener mayor éxito, las personas involucradas deben comprender a fondo cada una de sus funciones en el proceso y cómo su rendimiento afectará en el resto del proceso.

Es importante capacitar a todo el personal que interviene en el proceso de recuperación ante desastres. Ellos deben revisar periódicamente sus responsabilidades y participar en prácticas al menos dos veces al año, de preferencia trimestralmente. También es importante para la organización mantener una lista actualizada del personal necesario para su actual proceso de recuperación. Cambios como los ascensos, despidos y renuncias deberán tenerse en cuenta en el plan de recuperación ante desastres realizando los cambios pertinentes.

Por otra parte, cada vez que la empresa se somete a cambios en la infraestructura, por ejemplo actualizaciones de la red, deben incorporarse en el plan de recuperación ante de desastres. Un plan desactualizado sólo es un poco mejor que no tener alguno. Esto es el DRP necesita estar actualizado, lo que implica tener un inventario al día de todos los recursos de TI.

Establecer controles para mitigar los riesgos

Se deben establecer controles que mitiguen los riesgos y vulnerabilidades identificadas. Por ejemplo, para mitigar las fallas frecuentes de energía eléctrica se recomendaría la instalación de un UPS y/ o de generadores de potencia eléctrica.

Glosario de Conceptos

Administración de riesgo

Es el proceso mediante el cual se identifica, se mide y se controla la exposición al riesgo. Es un elemento esencial para la solvencia de cualquier negocio. Refuerza la capacidad de análisis, define metodología de valoración, mide los riesgos y, establece procedimientos y controles homogéneos.

Amenaza

Peligro latente asociado a una vulnerabilidad del ambiente tecnológico que puede causar efectos adversos a la operación regular de una compañía.

Aplicación crítica

Aplicación que soporta un Proceso de Negocios vital o crítico.

Captura de datos huérfanos (Catch-Up)

Proceso de recolección de datos huérfanos mediante procedimientos alternativos o manuales, reingresándolos a los sistemas correspondientes para igualar la información al día de negocio respectivo.

Continuidad operacional

Procesos de Negocio que permanecen operando durante una interrupción generalizada. Pueden incluir procedimientos manuales, mientras se transfiere la operación o durante un evento catastrófico, hasta que se activan los procedimientos de recuperación.

Costo de tiempo de inactividad

Los costos por pérdidas potenciales como consecuencia del desastre y recuperación.

Datos huérfanos

Información registrada en el sistema, desde el resguardo almacenado off-site y el momento del desastre, y que no han sido salvados por los últimos resguardos de información (back up).

Declaración de desastre

Acto formal de aceptación de una situación de desastre, emitido por un funcionario responsable, que implique la activación del Plan de Recuperación de Desastres.

Desastre

Cualquier evento accidental, inesperado, natural o malicioso que amenace o interrumpa las operaciones de la Organización, durante un período de tiempo significativo para el negocio.

Estrategia

Principios y rutas fundamentales que orientarán el proceso administrativo para alcanzar los objetivos a los que se desea llegar.

Evaluación de riesgos

La evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

Evento

Hecho, o secuencia de sucesos anormales, que pueden conducir a la indisponibilidad de la operación del negocio por un tiempo significativamente prolongado.

Función de negocio

Estructura operativa que ejecuta un conjunto lógico e interrelacionado de operaciones de Negocio.

Función de negocio vital

Función de Negocio que debe continuar o ser restaurada bajo cualquier circunstancia para la supervivencia de la organización.

Implantar

Establecer y poner en ejecución nuevas doctrinas, instituciones, prácticas o costumbres

Implementar

Poner en funcionamiento, aplicar los métodos y medidas necesarios para llevar a cabo algo.

Manejo de crisis

Coordinación de las respuestas de una Organización a una crisis, en forma efectiva y en los tiempos requeridos, con el objeto de evitar o minimizar daños a la Organización y a su entorno.

Mantenimiento del plan

Acción continua de actualización de la información contenida en los Planes, para asegurar su vigencia permanente.

Personal vital

Cantidad mínima de personal requerido para llevar a cabo un Proceso de Negocio crítico.

Plan de Recuperación de Desastres

Conjunto de procedimientos e información, desarrollado, coordinado, conocido, ejercitado, emitido y actualizado, para ser utilizado en caso de emergencia o desastre. Diseñado para la recuperación de una parte esencial del negocio.

Plan de Continuidad del Negocio

Conjunto de procedimientos e información, desarrollado, coordinado, conocido, ejercitado, emitido y actualizado, que asegure la preparación necesaria para que la Organización pueda continuar operando su negocio. Incluye el Plan de Recuperación de Desastres, más las estrategias, los procedimientos y los recursos para recuperar el conjunto de actividades propias del negocio.

Procedimiento

Sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación. Todo procedimiento involucra actividades y tareas del personal, determinación de tiempos de métodos de trabajo y de control para lograr el cabal, oportuno y eficiente desarrollo de las operaciones.

Procedimientos manuales

Procedimientos de captura, procesamiento y/o emisión de información necesaria frente a una falla en el servicio de sistemas.

Proceso de Negocios

Grupo de actividades y/o procedimientos que se inicia con una entrada determinada y genera un producto de valor especifico necesario y útil para el negocio.

Punto crítico

Es un punto en el tiempo a partir del cual un Proceso de Negocio, fuera de operación, comienza a generar impactos severos a los Procesos interrelacionados y a la Organización en su conjunto.

Punto Objetivo de Recuperación (RPO)

Punto en el tiempo en el cual los sistemas y los datos deben ser recuperados después de un desastre. Es un factor de restauración de datos utilizado para reflejar la antigüedad de la información.

El punto en el tiempo al que los datos deben ser recuperados: inicio de la jornada, la última copia de seguridad o la última transacción.

Recuperación de un Desastre

Proceso para normalizar la operación de un Proceso de Negocios, luego de un desastre

Registro vital

Información esencial para el soporte y restablecimiento de un Proceso de Negocio crítico, cuya ausencia total o parcial impide su operación.

Seguridad de la información

La preservación de la confidencialidad, integridad y disponibilidad de la información.

- Confidencialidad: garantía de que acceden a la información, sólo aquellas personas autorizadas a hacerlo.
- Integridad: mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Tiempo Objetivo de Recuperación (RTO)

Período máximo de tiempo para disponer de los Procesos de Negocios operando en forma normal.

Vulnerabilidad

La vulnerabilidad es cualquier debilidad en el ambiente tecnológico y esta dada por el grado en que un sistema es susceptible o incapaz de enfrentarse a efectos adversos del ambiente tecnológico.

Bibliografía

- Ackoff R.L., (1973). "Science in the Systems Age: Beyond IE, OR, and MS,". Operations Research. Vol. 21, No. 3, mayo-junio 1973.
- Argenti, John (1997). "Stakeholders: the Case Against". Long Range Planning. Vol. 30, Junio 1997.
- Banville, Claude y otros, (1998). "A Stakeholder Approach to MCDA". System Research. Vol. 15, 1998.
- Bartalanffy, Ludwig Von, (1968). "Teoría General de los Sistemas. Fundamentos, desarrollo, aplicaciones". FCE, México. Cuarta reimpresión, 1984. Traducción Juan Almena.
- BIS, (2006). "International Convergence of Capital Measurement and Capital Standards". Bank for International Settlements, Press & Communications. Junio, 2006. Basel, Switzerland.
- Dávila, Yves (2005). "Un Enfoque Integral sobre BCM".
- EMC^2, (2008). "Estrategia para Elaborar un DRP". México.
- Gelman, O., (1978). "Metodología de la Ciencia e Ingeniería de Sistemas: Algunos Problemas, Resultados y Perspectivas". Memorias del IV Congreso de la Academia Nacional de Ingeniería. Mérida, Yucatán. Octubre, 1978
- Gelman, O. y J. L: García, (1989). "Formación y Axiomatización del Concepto de Sistema General". Boletín Instituto Mexicano de Planeación y Operación de Sistemas. Año XIX, No. 92. México, D. F.
- Gelman, O y Negroe, G., (1982). La Planeación como un Proceso Básico en la Conducción. Revista de la Academia Nacional de Ingeniería, México. Vol. 1, No. 4, Junio 1982.
- Hartwig, Robert P., (2005). "Financial and Market Impacts of Hurricanes on Property/Casualty Insurers Past, Present & Future". Presentado en "2007 National Hurricane Conference". New Orleans. 5 de abril de 2007.
- HP & Score, (2007). "Impact on U.S. Small Business of Natural & Man-Made Disasters".
- III, (2007). "Hot Topics" Insurance Information Institute. Agosto 2007. Ver: http://www.iii.org/media/hottopics/insurance/catastrophes/
- III, (2007). "Stats by Issues – Earthquakes" Insurance Information Institute. Agosto, 2007. Ver http://www.iii.org/media/facts/statsbyissue/earthquakes/
- Nieto Giménez-Montesinos, Ma. Ángeles. "El Tratamiento del Riesgo Operacional en Basilea II" Banco de España, España.
- Ochoa, Felipe (1997). "Cuadernos de Planeación y Sistemas No 10: Método de los Sistemas". DEPFI, UNAM. México.
- ODI, (2000). "Safeware Loss Study: Understanding Data Loss". Ontrack Data International, Inc.

- Rowe, (1989). “Strategic Management a Methodological Aproach”. 3a Ed, Addison Wesley.

Mesografía

- www.cnsf.gob.mx
- www.emc.com
- www.drii.org
- www.deloitte.com
- www.bcm-institute.org
- www.evergreen-data.com
- www.strohlsystems.com
- www.en.wikipedia.org
- www.bis.org
- www.disasterrecovery.org
- www.comunidadbcm.com
- www.continuitycentral.com
- www.drj.com
- www.thebci.org