UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE ESTUDIOS DE POSGRADO

T E S I S

LINEAMIENTOS PARA PLANES DE CONTINGENCIAS DE LOS SISTEMAS DE CÓMPUTO DEL CPG. CACTUS DE PEMEX GAS Y PETROQUÍMICA BÁSICA

QUE PARA OBTENER EL GRADO DE

MAESTRO EN INGENIERÍA
(PLANEACIÓN)

P R E S E N T A:

ALEJANDRO MENDOZA AGUILAR

DIRECTOR DE TESIS:

DR. RICARDO ACEVES GARCÍA

MÉXICO, D.F. DICIEMBRE DEL 2000

AGRADECIMIENTOS

A mis padres Alfonso y Petra.
Por el amor que me han dado y enseñarme
el camino de la vida.

A mi esposa Teresita y mis hijos Annel, Alejandro.
Con todo mi amor, gracias por su apoyo para continuar superándome.

A mis hermanos Juan, Claudio, Hortencia,
Taide, Noé, Willybaldo y Wuesley.
Por su gran cariño y apoyo en todos los aspectos de mi vida.

A toda mi familia.
Por todo el apoyo que me han dado.

INDICE

RESUMEN

Un plan de contingencias es un documento que sistemáticamente trata de responder a la pregunta ¿qué se debe hacer cuando los sistemas basados en tecnología fallan?, que facilita tanto la continuidad del negocio, así como el restablecimiento de las operaciones después de una interrupción causada por un problema en los sistemas de cómputo, de forma tal que la empresa pueda seguir operando.

Con el advenimiento de la tecnología es innegable la conexión que existe entre el funcionamiento eficaz de los recursos de cómputo de los sistemas de automatización de las plantas industriales y la competitividad de la empresa; es por ello que la tecnología de automatización se ha convertido en un factor clave dentro de la planeación estratégica de toda industria por lo que se considera que los sistemas de cómputo son elementos críticos de producción y deben de protegerse a toda costa.

La forma de controlar los daños que puede causar una falla en un sistema de cómputo, es realizar una planeación detallada de las contingencia, considerando los componentes críticos que los soportan, bien sean programas y aplicaciones, equipos de cómputo o sistemas incorporados.

En este trabajo se aborda el tema del establecimiento de los lineamientos necesarios para elaborar planes de contingencias para cuando fallan los sistemas de cómputo del CPG. Cactus de Pemex Gas y Petroquímica Básica, el plan de contingencia establece las condiciones estratégicas que den continuidad operativa a los sistemas de cómputo, con el fin de anticiparse a las posibles fallas de los mismos en el presente.

La aplicación de la técnica de causa – efecto como herramienta de análisis permite identificar las causa y los efectos que generan las contingencias, asignar prioridades a las aplicaciones de los sistemas de cómputo existentes, así como detectar cuales son estratégicas para la operatividad de la empresa.

Dentro de la planeación de las contingencias del sistema de cómputo del CPG. Cactus se establece el alineamiento al plan estratégico de Pemex Gasa, con la finalidad de que ayude a alcanzar los objetivos de las empresas y apoyar las estrategias operativas de la misma.

INTRODUCCIÓN

En la actualidad los sistemas de cómputo son elementos vitales dentro de la operación de cualquier proceso de la industria del petróleo y a una falla no controlada de algún elemento del sistema de automatización podría desencadenar un paro de la planta de procesamiento de hidrocarburos, para resaltar la importancia que ello involucra, imaginemos los problemas que se generarían si se reduce la producción o distribución de algún derivado del petróleo y, más aún si esta se detuviese por completo.

Las medidas de seguridad, determinadas bajo el plan de contingencia, son empleadas para prevenir o detectar daños sean intencionales o accidentales de los sistemas de cómputo, bien sea la modificación, destrucción de datos o la pérdida de la capacidad de comunicación y procesamiento.

Estadísticamente el 90% de las empresas que han sufrido un fallo en sus sistemas basados en tecnología, han dejado de operar hasta 18 horas. Se sabe que las causas de las fallas son:

- **40%** Causados por gente - cables cortados, errores por falta de capacitación, omisiones y vandalismo.
- **45%** Debido a fallas de equipo - programas, pérdida de energía, falla de circuitos, pérdida de redes de comunicación.
- **10%** Por problemas de instalaciones - aire acondicionado, humedad excesiva.
- **5%** Por causas naturales - terremotos, huracanes, inundaciones, tormentas, incendios.

El impacto de la no operación de los sistemas de cómputo generalmente se traduce en:

- Pérdida de producción.
- Pérdida de ventas.
- Pérdida de la ventaja competitiva .
- Deterioro de la imagen.
- Reducción de participación en el mercado.
- Demandas legales.

La creciente dependencia de las empresas en los sistemas basados en tecnología y en la información que éstos generan, ha incrementado la importancia de los planes de contingencia para prevenir la falta de disponibilidad de dichos sistemas

La planeación para la continuidad de la operación del negocio, en caso de contingencia, es un elemento estratégico para toda empresa. El plan de contingencias constituye un elemento crítico de éxito, que permite minimizar el impacto de algún siniestro y recuperarse de la manera más eficiente, garantizando la continuidad del negocio.

Es por ello que en la planeación de las contingencias es fundamental que el plan de contingencias este alineado al plan estratégico, a la visión y misión de la empresa, ya que se busca que los planes de contingencia coadyuven a alcanzar los objetivos de la empresa y apoyen a las estrategias operativas de la misma.

Debido al carácter impredecible de la ocurrencia de una contingencia, se hace necesaria su planeación haciendo uso de herramientas creativas y visionarias que nos permitan enfrentar con éxito el impacto de las fallas en sus respectivos ámbitos, reduciendo a un nivel aceptable las consecuencias de una disminución en el nivel de seguridad, o en la capacidad de operación de la empresa.

El producto de la planeación de contingencias es un plan que debe facilitar la continuidad del negocio, para lo cual es indispensable que su planeación este alineada al plan estratégico de la empresa, y enmarcado dentro de la misión y visión de la organización.

Dentro del negocio de procesamiento del petróleo, en Pemex, se están actualizado los sistemas para control, seguridad y administración, todos ellos basados en tecnología de microprocesadores integrada en todos los sistemas de control distribuido, control avanzado, sistemas instrumentados de seguridad, sistemas de circuito cerrado de TV y sistemas de gestión financiera y administrativa, de los diferentes centros de procesamiento y almacenamiento de hidrocarburos que integran la industria del petróleo.

En el Centro Procesador de Gas (CPG) Cactus perteneciente a Pemex Gas y Petroquímica Básica (PGPB), se cuenta con un plan integral de contingencias para el caso de que se presente un accidente industrial, sin embargo no se tiene un plan especifico alternativo para la continuidad de las operaciones críticas para cuando los sistemas de cómputo presenten una falla.

Tomando en cuenta lo anterior, surgió el presente trabajo, que tiene como objetivo proporcionar los lineamientos necesarios para realizar un plan de contingencias que permita, de forma efectiva, asegurar la continuidad de las funciones críticas de los sistemas de cómputo de la empresa, así como restablecer las condiciones operativas normales en el mínimo de tiempo posible.

La aplicación de técnica grupales dentro de la planeación de las contingencias, permitirá que el grupo responsable de las contingencias cuenten con herramientas novedosas y creativas para realizar un adecuado análisis de riesgos y enfrentar el impacto de las contingencias en sus respectivos ámbitos.

La técnica de causa/efecto aplicada en la planeación de contingencias, es una poderosa herramienta para que los grupos responsables de las contingencias de empresas y organizaciones entiendan la naturaleza dinámica y compleja de las fallas de los sistemas de cómputo e identifiquen las estrategias operativas a largo plazo, buscando el máximo de flexibilidad frente a la incertidumbre y dando claridad a una situación o acontecimientos del problema planteado.

Se debe tener presente que la atención a la contingencia es un trabajo en equipo bajo una situación de emergencia, por lo que la planeación de las contingencias es una tarea en la que deben participar las diferentes áreas técnica especializadas de la empresa, y su éxito depende del conocimiento que ellas tengan sobre las operaciones de sus procesos, y de sus dependencias tecnológicas.

En el capítulo I Marco de Referencia, se presentan los aspectos generales de un Plan de Contingencia, su estructura, utilidad y beneficios, así como el ciclo de vida del mismo..

En el capítulo II Ärea de Aplicación, se describe la Organización General de Pemex Gas Petroquímica Básica, haciendo referencia a los objetivos estratégicos de la empresa, así como la descripción de la infraestructura operativa del CPG. Cactus y como esta constituido su sistema de cómputo.

En el capítulo III Lineamientos del Plan de Contingencia, se describen de forma detallada los lineamientos que permitirán desarrollar los Plan de Contingencia de los sistemas de cómputo.

Por último, en el capítulo IV se presenta el Plan de Contingencia del Sistema de Cómputo del CPG Cactus, el cual se desarrolló aplicando los lineamientos establecidos en el capítulo anterior.

Capítulo I

MARCO DE REFERENCIA.

I.1 Definición de plan de contingencia.

Un plan de contingencias es un conjunto de procedimientos alternativos a la operación normal, que facilitan tanto la continuidad del negocio por posibles fallas en los sistemas y procesos automatizados sobre los cuales descansan las operaciones vitales (de misión crítica) de la empresa, así como el restablecimiento de las operaciones después de una interrupción causada por un problema en los equipos, de forma tal que la empresa pueda seguir operando.

Planear para las contingencias ocurridas en los sistemas de cómputo no es lo mismo que planear para un desastre medioambiental o industriales. Los dos planes están relacionados pero son distintos.

Los planes de contingencia para los sistemas automatizados deben de desarrollarse teniendo en cuenta la presentación de las fallas siguientes:

- Fallas en las aplicaciones y equipos electrónicos propios como de los socios de negocios (proveedores de productos, proveedores de servicios de información, clientes).

- Fallas simultáneas en varios lugares, sistemas, procesos, terminales, etc.

- Fallas en las infraestructuras de soporte técnico tanto interno como externo (redes LAN/WAN).

Como se puede apreciar, ninguna institución o industria esta a salvo de los efectos de las interrupciones o fallas que se pueden presentar en sus sistemas de cómputo. Las fuentes de tales interrupciones pueden estar relacionadas a problemas a nivel de hardware y/o software o a las fallas de las infraestructuras de los servicios públicos y de telecomunicaciones.

I.2 Utilidad del plan de contingencia.

Los planes de contingencia deben servir para antes, durante y después de que ocurra una falla en los sistemas basados en tecnología de la empresa para:

- Garantizar la continuidad del negocio ante fallas de sistemas críticos que son vitales para la operación de los procesos técnicos, administrativos y financieros de la empresa.
- Reducir las interrupciones de servicios técnico - administrativos ante fallas de los sistemas de cómputo.
- Asegurar el restablecimiento oportuno de las operaciones.
- Limitar las pérdidas a las utilidades y al capital.

I.3 Ventajas del plan de contingencias.

La aplicación del plan de contingencia para la continuidad del negocio nos proporciona las siguientes ventaja:

- Determinar los procesos y relaciones críticas de la empresa.
- Evaluar los riesgos a los que están expuestos estos procesos y relaciones.
- Determinar las medidas preventivas a ser utilizadas para eliminar o mitigar riesgos.
- Determinar y evaluar los casos de riesgo con el fin de identificar los riesgos que deben ser encarados ya sea debido a la probabilidad que estos ocurran o su impacto potencial.

Los planes de contingencia identifican los procesos y relaciones críticas que guardan entre si los sistemas basados en tecnología. Adicionalmente identifican los factores de riesgo para cada proceso crítico de la empresa y sus relaciones.

Estos factores identifican:

- Puntos de fallas potenciales a nivel interno o externo .
- Probabilidad de falla en cada uno de los puntos.

- Riesgos potenciales en las relaciones críticas:

  - Demanda continua de productos o servicios a nivel de los clientes.
  - Capacidad de los proveedores para suministrar bienes/servicios con sujeción a las restricciones de tiempo y calidad.

I.4 Estructura del plan de contingencias.

Antes de desarrollar un plan de contingencias se deben cumplir los siguientes requisitos:

- **Apoyo de la dirección y de los usuarios.**

No se podré conseguir un mínimo de éxito si la dirección y los usuarios no conocen la necesidad de los planes de contingencias ni apoyan su desarrollo.

- **Revisión de los objetivos de la empresa, plan estratégico y gestión de riesgos.**

A la hora de preparar un plan de contingencias, debe recopilarse y hacer el análisis de los objetivos de la empresa, del plan estratégico y de la gestión de riesgos, así como aquellos otros documentos que determinen el nivel de servicio y tiempo de respuesta, qué condicionarán el desarrollo del plan de contingencias.

- **Identificación de los recursos que requieren planes de contingencias.**

Un punto fundamental en la preparación de los planes de contingencias, es que estos se apliquen a la totalidad de recursos que de alguna forma se consideran críticos par cumplir los objetivos de la empresa.

- **Priorización.**

Es muy importante establecer las prioridades de los planes según el impacto que pueden causa y la decisión de la dirección.

De acuerdo con la literatura de planes de contingencias, su estructura generalmente está basada en las siguientes fases:

- **Preparación e inicio.**

Los objetivos de está fase están centrados en la creación del grupo de trabajo, el desarrollo de un estrategia de planeación de continuidad de los servicios, desarrollo de las planificaciones e hitos principales, y por encima de todos ellos conseguir el apoyo de la alta dirección.

- **Análisis y gestión de riesgos.**

Esta fase tiene como objetivo principal la determinación del efecto que los fallos de cualquier sistema basado en tecnología considerado como crítico, produce en la empresa.

- **Planificación de contingenias.**

La fase de planificación de contingencias asimila y actúa sobre los resultados del análisis y gestión de riesgos. El producto de esta fase consiste en un plan de contingencias. El plan describirá los recursos, papeles del personal, procedimientos y fecha de cara a su implantación.

- **Pruebas.**

El objetivo de las pruebas es evaluar si los planes de contingencias son capaces de suministrar el nivel de garantía exigido por los sistemas críticos.

El plan de contingencias requiere de una definición perfecta de las acciones que se deben realizar en caso de una contingencia. Esta definición deberá estar reflejada en un documento que deberá constar de las siguientes secciones:

- **Objetivos o alcances que debe cumplir el plan de contingencia.**

  Los objetivos o alcances siempre estarán marcados por las propias prioridades de la empresa además de por sus costos económicos.

- **Criterios par invocar el plan de contingencia.**

  Siempre se debe tener muy claro y de forma explícita, los criterios para invocar un plan de contingencia, intentando eliminar cualquier decisión de tipo subjetivo que pueda crear acciones ante determinados fallos.

- **Vida del plan de contingencia.**

  Cualquier plan de contingencia debe definir el máximo tiempo que estará activo cada uno de sus niveles.

- **Responsabilidades de los distintos responsables del plan.**

  Es fundamental identificar los papeles y responsabilidades que asumirán los diferentes profesionales y usuarios de un plan de contingencia.

- **Procedimientos para invocarla situación de contingencia.**

  Los pasos a seguir a la hora de operar un plan de contingencia deben estar muy claros en lo que afecta a la forma de operarlo, por parte de los responsables.

- **Procedimientos para operar la situación de contingencia.**

  Los pasos a seguir a la hora de operar un plan de contingencia deben estar muy claros en lo que afecta a la forma de operarlo, por parte de los responsables y los usuarios.

- **Planificación de recursos cuando se opera un plan de contingencia.**

  Los recursos necesarios a la hora de actuar en la eventualidad de una contingencia pueden ser muy diferentes a los necesarios en funcionamiento normal.

- **Procedimientos para el retorno a operaciones normales.**

  Debe existir un criterio muy claro, automático y determinante que defina cuando se abandona la modalidad de contingencia y se retorna a funcionamiento normal.

  Es fundamental eliminar cualquier decisión de tipo subjetivo para que la transición sea lo organizada posible.

Capítulo II

ÁREA DE APLICACIÓN.

Los lineamientos del plan de contingencia se aplicarán en los sistemas basados en tecnología del Centro Procesador de Gas (CPG) Cactus, que es uno de los ocho centros procesadores de gas que integran al corporativo Pemex Gas y Petroquímica Básica.

Es el mayor centro procesador de gas, purificándose 37 % del gas natural que se consume en el país, por lo que guarda una posición estratégica a nivel nacional en la producción de hidrocarburos, se localiza en la parte sureste de México, a 45 Km de la ciudad de Villahermosa, Tabasco.

II.1. Organización general de PGPB.

II.1. 1 Antecedentes.

El Centro Procesador de Gas Cactus forma parte del organismo Pemex Gas y Petroquímica Básica que fue constituida el 16 de julio de 1992, a través del decreto emitido por el Congreso de los Estados Unidos Mexicanos en el que se dispuso que la paraestatal PEMEX estaría constituida por cuatro organismos descentralizados de carácter técnico, industrial y comercial con personal jurídica y patrimonios propios:

- Pemex Exploración y Producción.
- Pemex Refinación.
- Pemex Gas y Petroquímica Básica.
- Pemex Petroquímica.

Dentro de la cadena del petróleo Pemex Gas y Petroquímica Básica ocupa una posición estratégica, al tener la responsabilidad del procesamiento del

gas natural, líquidos del gas natural y el gas artificial; almacenamiento, transporte, distribución y comercialización de estos hidrocarburos, así como de derivados que sean susceptibles de servir como materias industriales básicas.

En el ámbito internacional Pemex Gas y Petroquímica Básica es una de las principales empresas procesadoras de gas natural, con un volumen procesado de 3,527 millones de pies cúbicos diarios y la segunda empresa productora de líquidos con una producción de 446 millones de barriles diarios. Cuenta con una extensa red de gasoductos a través de la cual se transportan cerca de 4,000 millones de pies cúbicos diarios de gas natural, así como Terminales de Almacenamiento y Distribución, lo que la ubica en décimo lugar entre las principales empresas transportistas de este energético en Norteamérica.

En México Pemex Gas y Petroquímica Básica se encuentra entre las 10 más grandes por su nivel de ingresos, superiores a $52,500 millones de pesos anuales, con activos del orden de $41,000 millones de pesos.

Dentro de Pemex Gas y Petroquímica Básica, el CPG. Cactus es el centro de procesamiento que tiene el mayor número de plantas de tratamiento de gas, teniendo una facturación diaria de $27,450,000.00.

II.1.2 Visión, Misión y Objetivos Estratégicos.

Debido a su carácter paraestatal el organismo Pemex Gas y Petroquímica Básica y el Cetro Procesador de Gas Cactus orientan su misión a la atención de la seguridad, el cliente, el estado y el corporativo PEMEX, definiendo esta en los siguientes términos:

Seguridad industrial, operaciones y protección ambiental:

- **Operar toda la base de activos en forma eficiente, segura y confiable.**

Cliente y mercado:

- **Proporcionar productos y servicios de valor agregado.**
- **Fomentar la elección de combustibles con base a criterios económicos.**

Estado:

- **Obtener un rendimiento adecuado que preserve los activos.**

PEMEX:

- **Crear una cultura de colaboración y transparencia económica con otras entidades de PEMEX.**

- **Atraer, desarrollar y retener personal de calidad.**

La visión de PGPB - CPG. Cactus describe la imagen objetivo de la empresa estableciendo a lo que aspira alcanzar, siendo responsabilidad de todos los que integran la empresa hacer posible la visión a largo plazo:

- **Ser una empresa reconocida por su compromiso con la seguridad de sus trabajadores y de sus operaciones, y con la preservación del medio ambiente.**

- **Ser una empresa que contribuya a la creación de riqueza para el Estado.**

- **Responder a las necesidades del mercado mediante la oferta de servicios y productos de valor agregado.**

- **Proporcionar un ambiente laboral que promueva y recompense la iniciativa propia y el trabajo en equipo.**

La misión y visión establecidos en el plan estratégico de PGPB determinan la dirección de los objetivos estratégicos que deben alcanzarse en un futuro próximo, y que son la base para ponderar los contextos internos y externos de la empresa:

- ***Seguridad, Salud y Protección Ambiental.***

  Distinguirse por el compromiso de la empresa y sus trabajadores con la seguridad, salud y protección ambiental.

Flexibilidad operativa.

Asegurar la flexibilidad operativa y comercial que responda oportuna y eficientemente a las necesidades del mercado.

- ***Participación en el proceso regulatorio.***

  Contribuir al estricto cumplimiento de los requisitos regulatorios y a la evolución eficiente de la industria, mediante el trabajo conjunto con las autoridades regulatorias.

- ***Competitividad y servicio al cliente.***

  Desarrollar prácticas comerciales y de servicios a clientes que aseguren una posición de mercado preferencial y que contribuyan al creación de valores para Pemex y sus clientes en condiciones de mercado a través del uso de gas y líquidos de gas.

- ***Eficiencia operativa y administrativa.***

  Asegurar la competitividad de PGPB consolidando las prácticas operativas y administrativas en los mejores niveles de eficiencia.

- ***Recursos Humanos.***

  Garantizar el desarrollo y retención del capital humano que permita cumplir con los objetivos de negocios de la empresa.

II.2 INFRAESTRUCTURA OPERATIVA DEL CPG. CACTUS.

El CPG. Cactus es la unidad de negocios de Pemex Gas y Petroquímica Básica que cuenta con el mayor número de plantas industriales para el procesamiento de gas natural, almacenamiento y venta.

El CPG. Cactus tiene capacidad para procesar 1275 miles de millones de pies cúbicos de gas, a través de las siguientes instalaciones:

- 12 Plantas endulzadoras de gas
- 12 Plantas de azufre.
- 2 Plantas estabilizadoras de hidrocarburos.
- 6 Plantas criogénicas recuperadoras de etano.
- 1 Planta fraccionadora de hidrocarburos.
- 4 Turbogeneradores de energía eléctrica.
- 1 Planta de generación de vapor.
- 1 Terminal de Almacenamiento y Distribución.

Uno de los objetivos del Plan Estratégico de Pemex Gas y Petroquímica Básica, es el lograr la actualización tecnológica, por lo que se ha puesto en marcha un programa de inversión que tiene como objetivo lograr una mayor seguridad, un sensible mejoramiento en el control de emisiones contaminantes de sus instalaciones industriales, un mayor control en los procesos de distribución y venta de productos, este programa de modernización tecnológica esta aplicándose en cada uno de los Centros Procesadores de Gas, estando a la cabeza de la modernización el CPG. Cactus que ha logrado instalar el mayor número de sistemas de automatización basados en computadoras.

II.3 SISTEMA DE CÓMPUTO DEL CPG. CACTUS.

Los sistemas de cómputo se están instalando en las diferentes plantas de procesamiento de gas debido a que producen los siguientes beneficio:

- Evita la paralización de la planta cuando las variables críticas del proceso pasa de sus límites permisibles.
- Mejora la eficiencia del funcionamiento de las plantas y la recuperación de productos secundarios.
- Mantiene la especificación deseada del producto.
- Mejora el control de distribución y venta de los productos.

Actualmente el sistema de cómputo del CPG. Cactus, está integrado por los sistemas de automatización de las siguientes plantas de procesamiento:

- 2 Plantas criogénicas
- 4 Plantas de azufre.
- 12 Plantas de endulzamiento de gas.
- 4 Turbogeneradores de energía eléctrica.
- 2 Plantas generadoras de vapor.
- 1 Planta fraccionadoras de hidrocarburos.
- 1 Terminal de almacenamiento y distribución.

Debido a que estos sistemas de automatización son los responsables del control y la correcta operación de las plantas de procesamiento, y de la terminal de almacenamiento, es de vital importancia la intercomunicación que debe existir entre ellos, para lo cual se ha creado una red de comunicaciones (red LAN), que tiene como objetivo el establecer una ruta de intercambio de información que permita el monitoreo, registro, balance de producción de cada planta.

En el sistema de cómputo del CPG. Cactus no únicamente se procesa la información de los diferentes sistemas de automatización de cada una de las plantas procesadoras (Área Operativa), también confluyen las siguientes Áreas:

- Nomina.
- Facturación.
- Despachos de distribución.
- Control de almacenamiento.
- Sistema de control avanzado.
- Sistema SAP.
- Control de personal.
- Microcomputadoras y Redes LAN/WAN.
- Sistema de información de Plantas.
- Red WAN.
- Correo Electrónico.

Entre las diferentes Áreas de operación de los sistemas cómputo que conforman la red se procesan alrededor de 20,000 variables de control y de historia de los procesos, toda esta información es tratada en tiempo real debido a que es utilizada tanto para hacer el ajuste de los parámetros de producción, así como para la toma de decisiones de negocio a nivel ejecutivo.

La importancia del buen funcionamiento del sistema de cómputo, es vital para la buena operación (y competitividad) del CPG. Cactus, debido a que los productos básicos que se generan en este centro son la base o materia prima para otras industrias que generan productos terminados y que son consumidos en el mercado nacional y exportados a otros países; un ejemplo claro de esto es el procesamiento del gas natural a través del proceso conocido como endulzamiento (eliminación del azufre del gas), este gas es usado en grandes volúmenes en los procesos industriales de las industrias: metalúrgica, cemento, hulera y química. Por lo que una falla del sistema de cómputo afecta directamente a las áreas de operación, almacenamiento y distribución que maneja la información de la planta o del la terminal de almacenamiento y distribución, y no solamente traería grandes pérdidas financieras al CPG. Cactus, si no que también ocasionaría graves daños en la economía nacional.

Lo anterior da idea de lo fundamental que resulta la buena operación del sistema de cómputo del CPG. Cactus, y es por ello que para cada Área del sistema de cómputo deberá desarrollarse un plan de contingencias que no únicamente tome en cuenta los aspectos técnicos de los sistemas basados en tecnología, si no que se tomen den cuenta los entornos financieros, legal, administrativo, comercial y las relaciones que guarda con los clientes internos y externos.

Capítulo III

LINEAMIENTOS DEL PLAN DE CONTINGENCIAS.

La implementación exitosa de un plan de contingencias en los negocios requiere de un enfoque exhaustivo que involucre a cada una de las áreas de una organización y cada producto, servicio y función aún cuando no posean un vínculo conocido con la tecnología computarizada.

Los lineamientos para los planes de contingencias tienen como finalidad que las diferentes áreas que usan sistemas basados en tecnología, de los CPG´s de PGPB, apliquen un método de planeación general para elaborar su correspondiente planes de contingencias.

En los lineamientos que se describen en este capítulo, se tienen como aspecto central, para la elaboración del plan de contingencias, la planeación para definir las estrategias que nos permitan atender las posibles fallas de los sistemas de cómputo; la evaluación de los riesgos del negocio, así como el manejo de los mismos; la asociación de soluciones con cada escenario de riesgo identificado; las estrategias que permitan identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia; la capacitación y documentación del plan de contingencias que permita tener preparado al personal que ayudará en la recuperación del negocio.

LINEAMIENTOS PARA EL PLAN DE CONTINGENCIAS.

Cualquier plan de contingencias requiere de una definición correcta de las acciones que debe realizar cada uno de los participantes en caso de una contingencia, para lograr esta definición se deben considerar los

siguientes lineamientos o actividades al desarrollar el plan de contingencia.

III.1 Planificación.

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia. Las actividades durante esta fase incluyen:

- Definición explícita del alcance — indicando que es lo que se queda y lo que se elimina, y efectuando un seguimiento de las ambigüedades. Una declaración típica podría ser, "La continuidad de los negocios no cubre los planes de recuperación de desastres que ya fueron emitidos."

- Definición de una estrategia de planificación de la continuidad del negocio de alto nivel.

- Identificación y asignación de los grupos de trabajo iniciales; definición de los roles y responsabilidades.

- Identificación de las fuentes de financiamiento y beneficios del negocio; revisión del impacto sobre los negocios.

- Duración del enfoque y comunicación de las metas y objetivos, incluyendo los objetivos de la empresa.

- Definición de estrategias para la integración, consolidación, rendición de informes y arranque.

- Definición de los términos clave (contingencia, continuidad de los negocios, etc.).

- Obtención de la aprobación y respaldo de la empresa y del personal gerencial de mayor jerarquía.

RECOMENDACIONES.

- Las suposiciones iniciales deberían ser hechas por escrito y revisadas tan pronto como sea posible en el proceso, incluyendo:

- Las áreas de negocios cubiertas en el plan.
- El calendario de eventos para el plan (por ejemplo, las fechas de inicio y conclusión, los hitos durante la vigencia del mismo).
- Áreas de vulnerabilidad conocidas, incluyendo la infraestructura, los procesos críticos, etc.

- El plan debe ser ejecutado independientemente de las operaciones y procedimientos operativos normales.
- Las pruebas para el plan serán parte de (o mantenidas en conjunción con) los ejercicios normalmente programados para la recuperación de desastres y la realización de pruebas a nivel de todos los escenarios.
- Si ocurre un desastre, una interrupción, o un desfase de gran magnitud en los negocios de la empresa, se pondrán en práctica los planes de continuidad de los negocios o de contingencia.

III.2 Inventario.

La mayor parte de las organizaciones ya han desarrollado un inventario de los proyectos de remediación de fallas. Este inventario puede ser usado como base para el inventario de planificación de contingencias.

Las tareas clave durante esta fase incluyen:

- Conclusión, revisión y validación del inventario de funciones de la empresa o las descripciones de los flujos del proceso de alto nivel. Esta puede ser simplemente la representación de una función del negocio (por ejemplo, la entrega de un producto a un cliente) empleando las casillas y flechas básicas.

- El Roll out de los flujos del proceso de alto nivel en una función principal del negocio o área clave para asegurarse que todos los procesos elementales sean identificados, prestando atención específica a los procesos ejecutados al azar o en forma esporádica.

- Identificación de las funciones esenciales del negocio y definición de una lista inicial de riesgos, agrupados por áreas funcionales y que estén basados en la tecnología, la realización de esta actividad se llevará a cabo, haciendo uso del Formato 1- Proceso Integral de Riesgos.

- Depuración del calendario de eventos con el fin de reflejar la primacía de las funciones esenciales de la empresa.

- Se recomienda realizar una evaluación global del impacto o impactos que pueden tener en su área, cualquier interrupción producida por una falla en los sistemas de automatización. Para el logro de esta actividad se debe de efectuar la:

  - Identificación de los procesos de negocios del área, y que están basados en tecnología.

  - Identificación de los clientes internos y externos a los cuales les presta servicios para poder medir el impacto en las relaciones con los mismos.

  - Identificación de los proveedores de servicios (públicos, financieros, transaccionales), internos y externos, y que son críticos para el cumplimiento de los objetivos del área.

- Descripción del impacto que puede tener en el área la falta de prestación de servicios a los clientes tanto operacionales, financieros y administrativos.

Para facilitar la realización de esta actividad, se hará uso del Formato 2- Análisis del Impacto Global del Área.

Formato 1 — Gestión Integral de Riesgos: Lista

Area:	
Función:	

Categoría de Riesgo	**Definición**
Operacional	
Servicio	
Planeación de Contingencias Internas	
Seguridad	
Otros	

Firma

Nombre:
Gerente División/Director Departamento

Firma

Nombre:
Líder Usuario Grupo Interdisciplinario

Definiciones:

Area es la unidad organizacional a cargo del usuario, y cuyos procesos de negocio están basados en tecnología.
Función es el conjunto de actividades relacionadas que soportan los servicios críticos que el Area presta a sus clientes.
Categoría de Riesgo en este contexto se refiere a un grupo de eventos que pueden ocurrir dadas ciertas condiciones y que pueden afectar adversamente uno o más procesos de negocio..
Definición es una breve descripción del riesgo relacionado.

Formato 2 ---- Análisis de Impacto Global del Área

Usuario Líder que elabora el Formulario :
Área o Coordinación a su cargo: :
Sistema :
Fecha: :

1. **UBICACIÓN DEL AREA EN LA ORGANIZACION**

Sección	: de la cual depende el Área o Coordinación.
Departamento	: del cual depende la Sección.
Gerencia	: de la cual depende el Departamento.
Vicepresidencia (	: a la cual reporta la Gerencia.

2. **SERVICIOS DEL AREA**
   - **Objetivos del Area:**
   - **Procesos de negocio basados en tecnología** (servicios claves que el Area presta y que se soportan en tecnología) :
   - **Aplicaciones críticas** (aplicaciones de misión crítica sobre las cuales descansa el Area para cumplir los objetivos)
   - **Otros procesos de negocio** (servicios claves no soportados por la tecnología).

3. **CLIENTES** (internos y externos, a los cuales el Area presta los servicios)

4. **PROVEEDORES** (Areas o Aplicaciones y/o Entidades Externas de los cuales depende su Area o Aplicaciones críticas para la prestación de los servicios críticos)

5. **IMPACTOS**
   - **Impactos** (Breve descripción de los efectos que produciría el Area en caso de que no pueda prestar sus servicios por interrupciones prologandas de las aplicaciones criticas internas o externas), analizando impactos en la atención a los clientes, ingresos que se dejan de percibir, pérdida de mercado, imagen de la empresa y sanciones o multas a que se hace acreedor la compañía.
   - **Períodos críticos en caso de que se presente una interrupción prolongada en los servicios del Área** (fines de mes, días festivos, día de la madre, mes de diciembre, puentes, el primer día de cada semana):
   - **Tiempo que el Area podría operar sin el apoyo de la tecnología:**
   - **Impacto en las operaciones de otras Areas o Aplicaciones críticas:**

6. **PROCEDIMIENTOS ALTERNOS** (procedimientos manuales u otros de que dispone el Area en caso de una interrupción prologada de los servicios de información internos o externos)

7. **COMENTARIOS ADICIONALES**

III.3 Evaluación.

Así como la fase de inventario se concentra en el impacto potencial de las fallas, la fase de evaluación también toma como punto central el impacto directo o indirecto sobre las funciones y procesos clave que son de "importancia crítica para la empresa,". Si los efectos relacionados con las fallas deben ser considerados en primer término, cualquier clase de impacto debe ser evaluado, especialmente a la luz de los efectos indirectos.

Los impacto indirectos ocurren cuando algo falla o no produce resultados aceptables, y esa falla a su vez afecta una función clave o proceso de importancia crítica para la misión. Por ejemplo, una computadora que sufre un colapso, constituye un efecto directo. Si la computadora genera posteriormente un resultado que es ingresado a un sistema y utilizado posteriormente en un proceso clave de la empresa, este constituye un efecto indirecto sobre un proceso específico de la empresa. Si dicho proceso genera resultados incorrectos, este constituye otro efecto indirecto.

De modo que la fase de evaluación debería evaluar los siguientes aspectos:

- La importancia crítica del elemento inventariado sobre el caudal de ingresos, los procesos de la empresa, o las funciones de la misma, incluyendo la infraestructura.

- Los planes existentes de continuidad de los negocios/contingencia o de recuperación de desastres, proporcionan los requisitos mínimos para mantener las operaciones de la empresa.

- La importancia crítica de las funciones o procesos de la empresa que han sido inventariados, prestando una atención especial a las funciones/procesos en los que una falla podría ocasionar un impacto sobre los procesos o el caudal de ingresos que es de importancia crítica para la misión, o producir una exposición crítica de su organización.

- Las amenazas e impactos clave sobre los elementos inventariados (por ejemplo, fallas directas, fallas indirectas, deficiencias en la información ingresada/resultante) y la reanudación del análisis del impacto sobre la empresa.

- Riesgos de tipo regulador, legal, financiero y comercial de las fallas de los equipos.

- Riesgos de tipo regulador, legal, financiero y comercial si falla cualquier proceso de la empresa, el caudal de ingresos, o una función de la misma.

- Preparación de eventos, con fechas "proyectadas," "potenciales," y "que probablemente fallen".

- Riesgos e impactos de los golpes directos (es decir, la falla de un componente o ítem utilizado en un proceso).

- Riesgos e impactos de golpes indirectos (es decir, debido a información faltante o errónea o a la falta de disponibilidad de datos o infraestructura).

- Casos "catastróficos" u otros casos de fallas, siendo uno de los casos la ocurrencia de un evento analizado a tiempo, en contraposición con todo el proceso o función en su integridad — por ejemplo, el colapso de una aplicación a cargo de administrar fondos no tiene el mismo impacto cuando ocurre antes de que comience el día, y no se ha procesado nada, que cuando ocurre a medio día, cuando hay montos considerables que ya han sido procesados.

- Verificación cruzada de los riesgos y procesos/caudales/funciones inventariados.

RECOMENDACIONES

- El desarrollo de escenarios catastróficos debería ser un área de importancia significativa. Recomendamos dividir esta fase por lo menos en cuatro subsecciones:

    1. Evaluación de la importancia crítica de los procesos.
    2. Evaluación del riesgo (componentes individuales)
    3. Escenarios de riesgo.
    4. Matriz causa – efecto para análisis de riesgos (componentes individuales..

- Un equipo de ejecutivos, gerentes, administradores y coordinadores debería realizar un análisis rápido del impacto sobre los negocios de

acuerdo al tipo de negocio/producto basándose en los siguientes pasos:

1. Identificación de los grupos de trabajo críticos que implementan procesos esenciales del negocio.

2. Definición/documentación de los casos de falla y de aquellos que no están relacionados con los sistemas de cómputo.

3. Evaluación del impacto de los efectos de las fallas sobre la habilidad de los grupos de trabajo críticos para proveer servicios a sus clientes, generar ingresos, cumplir con ciertas funciones y adecuarse a los requisitos de tipo regulador o legal.

4. Determinación del nivel mínimo aceptable de los productos y servicios de los grupos de trabajo críticos en caso de ocurrir alguna falla.

Este proceso supone que los planificadores de contingencia ya han elaborado y analizado una lista de procesos esenciales del grupo de trabajo durante sesiones de trabajo previas. A través de las cuales se reconocen o generan los escenarios posibles (que puedan ocurrir y tener efecto adverso en la empresa) que tengan suficiente impacto en los procesos de negocio de la empresa, y que justifiquen el desarrollo, las pruebas y la implantación de planes de contingencia.

Los escenarios de contingencia deben describir los eventos que podrían suceder y tener efecto adverso en la empresa, bajo que condiciones pudieran ocurrir, donde y como.

En términos generales es imposible identificar todos los problemas potenciales, y tampoco es eficiente hacerlo. Sin embargo, es importante identificar los efectos de los riesgos que potencialmente tendrán un fuerte impacto en el área.

Una vez identificados los escenarios del área, se calcula la probabilidad de ocurrencia de cada escenario, la cual se determinará en forma cualitativa y la calificaremos como Alta (A), Media (M) o Baja (B), basándonos exclusivamente en el conocimiento operacional, financiero y de competitividad que tenga el grupo de contingencias del área funcional dueña del producto o servicio en los procesos de negocios críticos que maneja.

Por último, se procede a determinar el impacto de cada riesgo en la prestación de servicios del área. El impacto en el negocio o área, que pueden tener los riesgos, lo hemos clasificado en: operacionales, financieros y competitivos. El impacto de cada uno de estos riesgos, al igual que la estimación de la probabilidad, se puede calificar de acuerdo a la experiencia en Alta (A), Media (M) o Baja (B).

El impacto en el área (impacto global), se determina haciendo una evaluación cuidadosa sobre cual de los tres impactos en cada escenario es el que más pesa. Si es necesario llegar a la cuantificación correspondiente, entonces habría que hacerla para tomar la decisión correcta. El impacto global se determina de acuerdo a la siguiente tabla:

Si la categoría de riesgo que considera más importante en el escenario tiene un impacto:	Entonces el impacto global será:
Alto (A)	Alto (A)
Medio (M)	Medio (M)
Bajo (B)	Bajo (B)

La identificación de los problemas potenciales y su impacto en los procesos de negocio se llevará a cabo a través del Formato 3 --- Planeación de escenarios, teniendo en cuenta las siguientes premisas:

1. Los tipos de riesgos que vamos a manejar en el área pueden ser:

    - Internos. En este nivel se contemplan todos los equipos, software, redes de comunicaciones, aplicaciones, procedimientos y manuales de la empresa que forman parte del área.

    - Externos. En este nivel se contemplan los servicios y las infraestructuras de los proveedores de productos y/o servicios que se interrelacionan con el área, y que necesita para intercambiar información o para sus procesos transaccionales (sistema en línea) o para poder operar sus equipos y/o aplicaciones.

2. Un escenario es una combinación de eventos probables que pueden ocurrir simultáneamente o en forma muy cercana.

3. La probabilidad de ocurrencia de un escenario, es decir, la posibilidad de que se materialice el escenario en el futuro, puede ser Alta (A), Media (M) o Baja (B).

4. El riesgo describe el problema que podría presentarse en área, en caso de que el escenario fuera una realidad.

5. El impacto en el negocio se puede medir a través de las siguientes categorías de riesgos:

   - Operacionales. Riesgos que afecten las operaciones normales del área por fallas tecnológicas, internas o externas, y que le causen pérdidas. El impacto puede ser Alto (A), Medio (M) o Bajo (B).

   - Financieros. Riesgos legales por culpa de la empresa y que la exponen a pérdidas por demandas o sanciones por incumplimiento en las obligaciones que tiene. El impacto puede ser Alto (A), Medio (M) o Bajo (B).

   - Competitividad. Riesgos que reduzcan la base de clientes de los portafolios de productos de la empresa o que reduzcan sus utilidades o que le originen litigios costosos, etc, por publicidad negativa u otros eventos. El impacto puede ser Alto (A), Medio (M) o Bajo (B).

Formato 3 — Planeación de escenarios.

Area:
Proceso:
Responsable del proceso:
Elaborado por:
Fecha:

Tipo de riesgo	Escenario (problemas potenciales en el Area)	Riesgo (amenaza a la que se vería expuesta la empresa)	Probabilidad de ocurrencia del escenario	Impacto en el área (A,M,B)			
				Operacionales	Financieros	Competitividad	Global
Interno							
Interno							
Externo							
Externo							

Una vez identificados los escenarios posibles, se clasificarán en base a las prioridades indicadas en la tabla 1, donde la probabilidad de ocurrencia y el impacto global en el negocio se deben haber determinado previamente.

A continuación se realizar el análisis e identificación de causas y efectos de los riesgos para lo cual se recomienda usar la técnica de causa – efecto y el Formato 4 – Matriz Causa – Efecto.

Posteriormente se llena el Formato 5 – Clasificación y Priorización de Riesgos.

Tabla 1.

Probabilidad de Ocurrencia	Impacto Global en el Negocio	Prioridad
A	A	A
A	M	A
A	B	M
B	A	M
B	M	M
B	B	B
M	A	A
M	M	M
M	B	B

* Alto – A; Medio – M; Bajo – B.

Formato 4 – Matriz Causa – Efecto.

			EFECTOS
CAUSAS	Escenario	Riesgo	
		Riesgo	
	Escenario	Riesgo	
		Riesgo	

Formato 5 —Clasificación, Priorización y Efecto de los riesgos.

Area:
Proceso:
Responsable del proceso:
Elaborado por:
Fecha:

Rango	Prioridad	Escenario (problemas potenciales propiciados por la falla en el Área)	Riesgo (amenaza a la que se vería expuesta la empresa)	Efecto probable de la falla (descripción o cuantificación del efecto que se tendría)
1				
2				
3				

III.4 Identificación de Soluciones.

En esta fase, las soluciones que se han identificado de los riesgos específicos están documentadas. La meta es reducir el costo de encontrar una solución en la medida posible, a tiempo de documentar todos los riesgos identificados.

Las actividades más importantes deberían incluir:

- La asignación de equipos de solución para cada función, área funcional, o área de riesgo de la empresa.

- En la asociación de soluciones con cada escenario de riesgo identificado es aconsejable contar con más de una solución, porque las soluciones se calificarán y compararán posteriormente, algunas de las posibles soluciones que se pueden contemplar son:

- El diseño de procedimientos manuales.
- El diseño de procedimientos técnicos alternos.
- Realización de contratos con proveedores de servicios alternos.
- Reposición de componentes (hardware, software, aplicaciones).
- Recursos humanos adicionales.
- Nuevos programas y pruebas completas.

Todos ellos tratando de obtener uno de los siguientes niveles de servicios:

- Normal: proporcionar el mismo de servicio que se presta en operación normal (por ejemplo: diseñar un plan de acción que especifique actualizar o reponer un componente de un sistema de información).

- Degradado: proporcionar un nivel de servicio menor al que se presta en operación normal.

- Ninguno: no se presta el servicio.

Todas esas soluciones tienen como objetivo la reducción del efecto de los riesgos que se identificaron en el punto IV.2.3 Evaluación (última columna Forma 4--Priorización y clasificación de los riesgos).

- Sopesar los riesgos y su importancia crítica en términos del impacto de los mismos.

- Sopesar las soluciones y los riesgos y su importancia crítica en lo que respecta a su eficacia y su costo, siendo la meta la determinación posterior del mejor balance o de la solución más inteligente — es posible que no se escoja la solución que arregle todo pero a un costo inaceptable, cuando se compara con una solución menos "pura" que podría reducir los costos o ser más apta para volver a ser utilizada.

- La definición e identificación de equipos de acción rápida o equipos de intensificación por área funcional o de negocios de mayor importancia.

- La clasificación de los riesgos y escenarios utilizando una clasificación cualitativa de "probabilidad", para determinar si se acepta el riesgo o no.

Para realizar la toma de la decisión de si aceptamos o no el riego, al evaluar los impactos en el área, se empleará el Formato 4 – Clasificación, Priorización y Efecto de los Riesgos.

Recuerde que el resultado final de la evaluación del impacto en el área es tomar la decisión de si acepta el nivel de riesgo o no. Si el riesgo se acepta, entonces no hay necesidad de ninguna acción.

Entre los niveles de riesgos que se pueden aceptar incluimos:

- Nivel degradado de servicio: proporcionar un nivel de servicio menor al que se presta en operación normal.

- Nivel de no servicio: no se presta el servicio.

Si el riesgo no se acepta, entonces se requieren acciones adicionales que trataremos en el punto IV.3.5. Estrategias.

RECOMENDACIONES

- El inventario, evaluación y otras fases descritas en el presente ciertamente podrían aplicarse al centro de datos; sin embargo, el nivel de complejidad, la diversidad del inventario incluyendo la infraestructura, y el impacto potencialmente desastroso de que una computadora vital no se encuentre disponible ya sea en su totalidad o parcialmente requiere de un enfoque más específico.

- Este enfoque incluye (por lo menos) una etapa física, una etapa lógica, una etapa de aplicación y una etapa de operación del negocio, y enfatiza los aspectos de recuperación, que se pueden complicar rápidamente. La idea no es replicar un plan de recuperación de desastres de un centro de datos existente, sino hacer frente a situaciones menos complejas.

- Los esfuerzos para encontrar soluciones a situaciones complejas no deben descartarse simplemente porque estos no fueron tomados en cuenta durante esta fase.

- Las medidas de contingencia de los sistema de cómputo deberían proporcionar un plan amplio para encarar las situaciones de emergencia, aún los desastres, con las herramientas apropiadas para declarar una emergencia, adoptar las acciones necesarias para mitigar impactos significativos, reanudar las operaciones y posteriormente volver a las condiciones normales.

III.5 Estrategias.

Las estrategias de contingencia de los negocios están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. En esta fase también se decide si se adoptarán las soluciones de gran escala como las opciones de recuperación para un centro de datos.

Las actividades más importantes deberían incluir:

- La definición de los criterios más importantes de riesgos aceptables por área o función clave de la empresa.

- La revisión de los procesos, flujos, funciones y opciones de importancia crítica.

- La definición de las opciones de contingencia seleccionadas para cada riesgo identificado (nivel del componente, nivel del proceso de la empresa).

- La consolidación de soluciones de acuerdo a las funciones o áreas de negocios más importantes, con el fin de resaltar los elementos comparables e identificar las estrategias "globales".

- La identificación de los impactos de las soluciones y estrategias para ahorrar costos sobre los costos, como ser la selección de una solución para cubrir varios riesgos. Se deberían considerar varios elementos de costo: el costo de crear la solución, el costo de implementar la solución y el costo de mantener vigente dicha solución. Debido a que la continuidad de los negocios constituye el enfoque primordial, la estrategia de la empresa rige el análisis de costos.

- La identificación/depuración de los beneficios de al empresa. A medida que se revisan los procesos de la empresa, la relación costo-beneficio y "la astucia" de ciertas soluciones en particular serán analizadas y comparadas con el impacto sobre la continuidad de los negocios. Algunas veces, las soluciones podrían producir beneficios inesperados, o podrían ser ampliadas para producir algunos retornos adicionales. Por ejemplo, una organización podría adquirir una capacidad de almacenamiento adicional como una solución para cubrir las fallas relacionadas con la capacidad. Una solución inteligente en

este caso consistiría en encontrar la forma de utilizar esta capacidad adicional.

- La obtención de aprobaciones finales para el financiamiento. Antes de que se coloque el sello de aprobación a una solución — especialmente porque las empresas se encargarán primordialmente de las soluciones — el financiamiento debe ser verificado. En algunos casos, las soluciones podrían costar más que los problemas, y es posible que el gasto sea inaceptable para la empresa. En tales casos, una solución podría consistir en adoptar acciones especiales, como la contratación de pólizas de seguro o previsiones presupuestarias, para compensar las pérdidas potenciales.

Las estrategias que se definan y los objetivos correspondientes deberán registrarse en el Formato 5 -- Acciones de Prevención y Mitigación.

RECOMENDACIONES

La fase de la estrategia es cuando el plan de acción realmente se inicia con el financiamiento, el personal y la atención requeridos. La identificación de los beneficios es un elemento clave para asegurar que el costo del proyecto esté equilibrado con los retornos reales de la empresa. También pone a los proyectos en la perspectiva apropiada, aclarando cuáles son los costos así como quién los cubrirá.

En muchos casos, a pesar de que el programa para la contingencia se financia utilizando una disposición contable especial, la planificación de contingencia de los negocios está financiada directamente por los departamentos o áreas de la empresa afectadas. La razón más importantes para este tipo de contabilidad directa es que si los costos de las fallas se vuelven a cargar empleando reglas específicas, la planificación de la continuidad de los negocios tendrá entonces una relación simple con las funciones de la empresa. La continuidad de los negocios constituye un golpe directo, y el costo de proteger la empresa y el caudal de ingresos debe ser evaluado y sopesado en contraposición con estos ingresos.

No hay motivo para mantener una función en épocas difíciles si el costo de hacerlo es mayor al beneficio o retorno ya sea directo o indirecto. Solamente los administradores de la empresa pueden tomar esta determinación, que es la razón por la que tienen que acelerar y asumir las

soluciones de continuidad de los negocios, incluyendo el financiamiento de las mismas.

Formato 6 — Acciones de Prevención y Mitigación

Area:
Proceso:
Responsable del proceso:
Elaborado por:
Fecha:

Escenario		
Riesgos	**Efectos probables**	**Acciones de Prevención / Mitigación**

IV.6 Desarrollo y documentación.

La frase "desarrollar una solución" puede implicar una diversidad de actividades, desde reemplazar equipos a trasladarse a otro edificio o crear un manual de procesos. Cualquiera que sea la actividad, la documentación apropiada ahorrará mucho tiempo y energía. También proporciona al personal involucrado en situaciones caóticas o poco usuales algunas pautas que le podrían ayudar a encontrar o inspirarle una solución.

Las actividades más importantes deberían incluir:

- La asignación de equipos y tareas para encontrar soluciones de contingencia y garantizar la continuidad de los negocios.

- La creación e implementación de un plan para cada solución a ser desarrollada/ implementada, en esta fase se desarrollan las estrategias que reduzcan los efectos de las posibles fallas en los sistemas automatizados. En el anexo I se incluye el formato 6— Estrategias de Acción, en el que se deberán señalar las estrategias a seguir para la reducción de los efectos.

- El desarrollo de un central de acopio de riesgos, opciones y soluciones, utilizando palabras clave en la medida posible.

- La documentación de los riesgos, opciones y soluciones por escrito y en detalle.

- El desarrollo e implementación de planes de prueba cuando sea relevante.

- La definición de procedimientos de mantenimiento para los documentos de referencia.

- La definición de un plan de capacitación cuando sea relevante; definiendo la estrategia y los materiales de comunicación; la creación de materiales de comunicación (principalmente de comunicación interna).

- La identificación y documentación de listas de contacto de emergencia; la identificación de responsables de las funciones con el fin de garantizar que siempre haya alguien a cargo que dicha persona pueda ser contactada si falla un proceso de importancia crítica para la misión.

- La actualización de los planes de recuperación de desastres, procedimientos y documentación existentes.

RECOMENDACIONES

Uno de los factores de éxito más importantes en una situación de emergencia es el nivel de preparación del personal encargado de hacerle frente. Esto se puede obtener solamente a través de una capacitación específica, simulacros o ensayos, distribución del material apropiado y una comprensión amplia de los comportamientos requeridos.

La diferencia entre una situación de emergencia y una situación normal es primordialmente el hecho de tener que hacer frente a lo desconocido. Bajo presión, en una situación de caos, y sin la guía adecuada, a menudo la gente no escoge la mejor opción o no efectúa un análisis correcto. Las decisiones tomadas bajo una situación de estrés podrían en realidad empeorar las cosas y convertir una mala situación en un verdadero desastre.

La mayor parte de las acciones que pueden reducir el impacto de un evento negativo a menudo ocurren en los primeros minutos con posterioridad a la ocurrencia.

El calendario de eventos resalta el momento cuando es posible que las cosas no funcionen como se espera que deberían funcionar, ya que la incertidumbre potencialmente romperá las rutinas en todas las áreas de la vida: personal, profesional y social. Aún cuando los centros rectores de información y el personal de apoyo ayuden a mantener algún grado de organización para el manejo de los problemas, lo mejor es contar con un equipo entrenado, que posea amplios conocimientos y esté mentalmente preparado para hacerse cargo de la situación y que esté equipado con los materiales adicionales necesarios (por ejemplo, tablas de decisiones, listas de contacto, procedimientos de intensificación).

La implantación o desarrollo de las actividades propias o acordadas no tendrian ningún sentido si no son documentadas, esta documentación nos servirá de guía para hacer frente a los diversos escenarios de falla, en una forma ágil, oportuna y organizada, esta actividad se realizará a través del Formato 7 - Plan de Contingencias.

Formato 7 —Plan de Contingencias.

Area:
Proceso:.
Responsable del proceso:
Elaborado por:
Fecha:

- **Descripción y alcance** (resumen del contenido y alcance del plan):
- **Objetivo** (propósito del plan):
- **Areas afectadas** (Grupos, Areas, Agencias, Departamentos que son afectadas por la contingencia):
- **Responsabilidad** (especifique los Grupos que tienen la responsabilidad de las actividades del plan, antes, durante y después; descripción de esa responsabilidad; directorio de contactos incluyendo los proveedores de productos, insumos y servicios):
- **Criterios para invocar el plan** (una falla de la aplicación que soporta el proceso; una caída de más de 15 minutos del sistema en línea; un mantenimiento crítico que hay que poner en producción; el retiro de personal clave):
- **Procedimiento para invocar el modo de contingencia** (pasos a realizar para poder implementar el modo de contingencia):
- **Procedimiento para operar en modo de contingencia** (que tienen que hacer las Areas o personas que normalmente están cargo del proceso para trabajar en el modo de contingencia, así como los requerimiento que sean del caso):
- **Recursos para operar el modo de contingencia** (personal, hardware, seguridad, suministros, equipos de comunicaciones, listados, etc que requieran adicionalmente las Areas afectadas para que puedan operar en modo de contingencia):
- **Criterios para retornar al modo normal de operación** (acciones del responsable del proceso para poder poner en producción la aplicación crítica que falló por un problema, previa autorización de la autoridad establecida para esto):
- **Procedimiento para retornar al modo de operación normal** (que tienen que hacer las Areas o personas que normalmente están cargo del proceso, o fueron afectadas, para salir del modo de contingencia):

Los planes de contingencia deben ser funcionales y deben trabajar en forma adecuada, lo que requiere una documentación formal y clara, que debería contener como mínimo los siguientes elementos de información:

1.- Descripción y alcance: descripción breve del contenido del plan así como de su alcance.

2.- Objetivo: resultado que espera obtener con la implementación del plan.

3.- Area afectadas: relación de las Areas o clientes afectados por una falla probable, así como el impacto a que se verían sometidas.

4.- Responsabilidad: definición clara de las tareas, responsabilidades y autoridad del a) usuario dueño o Area Funcional responsable del producto o servicio, b) proveedores de servicios, c) los miembros del grupo operativo de contingencias para 1) decidir - en caso de la ocurrencia de una falla o escenario específico de falla - si se debe entrar o no en el modo de contingencia, 2) coordinar y proveer los recursos para entrar y trabajar en el modo de contingencias o mitigación, 3) determinar en que momento y bajo que circunstancias se volverá al modo de operación normal. Adicionalmente, se debe contar con una lista de todas las personas que participan en el plan, incluido los contactos con los proveedores: el nombre, el cargo, los teléfonos, la dirección.

5.- Criterios para invocar el plan: descripción clara y específica de los criterios para invocar el modo de contingencias. Por lo general, deben obedecer a un mal funcionamiento antes, durante o después de una falla. Algunos criterios podrían ser: a) una caída de la aplicación por más de 15 minutos, b) reclamos de clientes por fallas en sus procesos, c) varias fallas de la aplicación el mismo día, d) bloqueo de los computadores o de todas las terminales administrativas o financieras de la red, e) daños en la línea de un proceso de producción o del canal de comunicaciones .

6.- El proceso, por lo general, se inicia cuando el responsable del producto o servicio (líder usuario, Área Funcional que sufre el impacto) empieza a notar irregularidades en el modo de operación habitual, o a recibir reclamos o reportes de falla por parte de los clientes, o ve que se podrían presentar dificultades en las unidades de negocios después de una evaluación, o ve que se podrían presentar demandas excesivas en el tráfico de información, etc.

7.- Como segundo paso, el responsable del producto se pone en contacto con los proveedores de servicios (internos o externos) - donde posiblemente pueda haber o encontrarse el origen del problema - o con las Área internas (unidades de negocios) que por lo general les atiende los problemas para tener información sobre el grado de severidad de la falla, si es transitoria o si esta información la eleva a la Dirección del comité de contingencias, para que allí se tome finalmente la decisión de si se invoca o no el plan de contingencias.

8.- Procedimiento para invocar el plan: 1) Lista de actividades que deben realizar los proveeedores de servicios sobre los cuales descansa la operación (ejemplo: Producción: baja la aplicación y hace backups, Soporte: baja la red, Servicios administrativos: poner en marcha procesos manuales, Desarrollo Humano: contrata personal temporal, Comunicaciones: Informa a los clientes sobre la situación, Desarrollo: 1)obtiene los listados de la aplicación, 2) Lista de actividades que deben llevar a cabo los clientes para entrar a trabajar en modo de contingencia.

9.- Procedimiento para operar en modo de contingencia: 1) Lista de actividades que deben llevar a cabo los clientes afectados mientras dure el modo de contingencia, 2) Los responsables de los procesos productivos estará pendiente de que el proveedores o proveedores arreglen el problema lo más pronto posible y así mismo coordinar las actividades a que haya lugar para el logro de ese objetivo.

10.- Recursos para operar en el modo de contingencia: 1) Lista de recursos adicionales que puedan necesitar los clientes para poder prestar el servicio en el modo de contingencia.

11.- Criterios para retornar al modo normal: descripción clara y concisa de las criterios para retornar al modo de operación normal. Por lo general, esos criterios son las pruebas técnicas, las pruebas de usuario y las pruebas de integración junto con la actualización de la documentación. Una vez que el responsable queda convencido de que el sistema está listo para entrar nuevamente en operación, lleva sus conclusiones y soportes a la Dirección del Comité de Contingencias, para que allí se tome la decisión de retornar al modo normal de operación.

12.- Procedimiento para retornar al modo de operación normal: 1) Lista de actividades que deben llevar a cabo los clientes para retornar al modo normal, 2) Lista de actividades que deben realizar los proveedores de servicios sobre los cuales descansa la operación de la aplicación (Producción: cataloga la aplicación y hace los respaldos de los archivos, Producción: actualiza los archivos cuyo movimiento no pudo llegar en forma automática, Soporte: sube la red, Comunicaciones: Informa a los clientes sobre la fecha y hora en que se entrará trabajar en operación normal).

13.- Descripción detallada del plan de acción adoptado para la mitigación de los riesgos: Para los planes de mitigación de riesgos,

se debe describir detalladamente las actividades que se realizaran para reducir el impacto de las fallas.

Obsérvese en este momento que, si los planes de contingencia de los diferentes procesos críticos se han realizado cuidadosa y concienzudamente, entonces deberíamos tener al final un análisis del negocio y un plan de continuidad, es decir, un conjunto de procedimientos y de instrucciones precisas sobre las acciones a tomar en caso de falla.

Finalmente, la documentación de los planes de contingencia necesita actualizarse periódicamente. Además, deben guardarse en un sitio seguro, y por último, como recomendación, debería tenerse un respaldo o copia de esa documentación al menos en otro lugar aparte y también seguro.

IV.7 Realización de Pruebas y Validación.

Por supuesto que no podrá probar la ocurrencia de todos los riesgos. Sin embargo, una prueba que simule las condiciones de la vida real es la mejor manera de refrendar si una solución es realmente eficaz, o identificar problemas secundarios inesperados. Antes de realizar las pruebas, los planes deberían ser revisados y juzgados independientemente en lo que respecta a su eficacia y razonabilidad.

Las pruebas recomendadas para los planes de recuperación de contingencias incluyen una prueba anual preliminar y un ensayo general, en el que se crea un simulacro de un escenario con el fin de observar la eficacia del plan. Estas pruebas son esenciales para el éxito en una situación real de desastre, y generalmente constituyen una obligación contractual de cualquier proveedor de servicios para la recuperación de contingencias.

Las actividades más importantes deberían incluir:

- La validación de las estrategias de continuidad de los negocios de una unidad de negocios.
- La validación e implementación de un plan (con las operaciones de la empresa y los representantes de dichas operaciones).
- El desarrollo y documentación de planes de contingencia de prueba, a través de la realización de pruebas con sujeción a un calendario de eventos específico.
- Realización de pruebas en cada unidad para ver la eficacia de la solución (la solución en sí, por sí sola).
- La preparación y ejecución de pruebas integradas para verificar la eficacia de la solución (la solución funcionando en un medio normal).
- La preparación y ejecución de "pruebas de eficacia" (realización de pruebas que realmente resuelven el problema — por ejemplo, probar el voltaje real de salida de una unidad generadora de repuesto, inspeccionar el producto de un proceso manual que se espera que reemplace a un proceso automatizado).

- La preparación y ejecución de "pruebas de casos/eventos" — la realización de pruebas en respuesta a situaciones de crisis y casos predefinidos; probar la respuesta en situaciones de crisis, en base a un caso en el que los eventos ocurren al azar y se intensifican en forma gradual. El enfoque en este caso consiste en ensayar/analizar las acciones a ser adoptadas para evitar que la situación empeore, así como verificar que se realice el análisis correcto de los eventos.

- La conducción de un ensayo general.

- La consideración de múltiples casos de diversa gravedad.

- La actualización de cualquier plan de contingencia/continuidad de los negocios o de recuperación de desastres según fuese apropiado, utilizando los resultados o la retroalimentación de las pruebas y ensayos realizados.

IV.8 Implementación.

La implementación implica una de dos situaciones: 1) el evento ha ocurrido o se está realizando una prueba controlada; o 2) la implementación de una solución en particular se puede llevar a cabo justo antes del evento, para reducir o eliminar el riesgo, o mejorar el estado de preparación en general. Cualquiera que fuese el caso, una implementación debería difundir la documentación y proceder a la capacitación del personal requerido.

Las actividades más importantes deberían incluir:

- La difusión de documentación referente a las soluciones; y la creación de procedimientos y documentación adicionales.
- La revisión de los procedimientos operativos para incluir material nuevo — advertencia: no se debe actualizar la documentación formal referente a la recuperación de desastres y otros procedimientos, porque el calendario de eventos representa una situación temporal de corto plazo).
- La difusión de documentación referente al manejo de riesgos.
- La entrega programada de equipo, infraestructura, aplicaciones y otros artículos planificados.
- La discontinuación de los ítems y documentación implementada.
- El acopio de suministros críticos en cada lugar requerido.
- Guardar copias de respaldo (backup) de documentos y listas de contacto en lugares externos como las casas de algunos miembros del personal.
- La ejecución de la etapa final del plan de comunicación subrayando específicamente que no se debe entrar en pánico e impartir indicaciones claras y fuertes de que las cosas están bajo control.
- La definición de los procedimientos de mantenimiento y realización de pruebas según fuere apropiado/relevante.

IV.9 Mantenimiento.

Cada vez que se da un cambio en el medio, la infraestructura o la configuración, se debe realizar un mantenimiento correctivo o de adaptación.

Un ejemplo de una instancia en la que se necesita mantenimiento es cuando se ha identificado un nuevo riesgo o una nueva solución. En este caso, toda la evaluación del riesgo cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero (el primer pase).

Esta reiteración es en realidad un tipo de mantenimiento, porque los riesgos evolucionan constantemente y cada reiteración (pase) reducirá el riesgo y mejorará las soluciones.

Dentro del contexto específico de un programa para contingencias, todo el programa podría ser considerado como una primer fase para cubrir los riesgos relacionados estrictamente con las fallas. Las fases adicionales deberían encarar tanto los riesgos restantes como los riesgos incurridos en aquellos casos en los que la solución propuesta no funcionaría. El enfoque más simple para cubrir dichos riesgos, y para poder hacerles frente en forma efectiva, consiste en considerar cada ciclo como una repetición, con las funciones, sistemas y procesos de importancia críticos para la misión como el primer ciclo.

Las actividades más importantes deberían incluir:

- Verificación cruzada del avance del programa en contraposición con los riesgos identificado, y re-evaluación de la exposición específica de los riesgos.

- Monitoreo del avance del proyecto en contraposición con los riesgos y metas; reportando al personal administrativo el avance y la situación.

- Revisión de la evaluación de riesgos y puntos de importancia crítica, incluyendo la exposición indirecta y la exposición a los riesgos que no están vinculados directamente con la falla.

- Desarrollo de un "mapa" de funciones y factores de riesgo.

- Conducción de revisiones regulares de los análisis del impacto sobre la empresa para actualizar este mapa.

- Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.

- Revisión de la situación de riesgo en conjunción con el departamento legal y de finanzas.

- Revisión de la capacitación y los planes así como el nivel de preparación de los equipos y el personal.

- Revisión continua de las aplicaciones y funciones críticas para asegurar la vigencia de la evaluación; cuando ocurren cambios, implementar nuevas soluciones y actualizar la documentación y los procedimientos (reiteración rápida).

- Monitoreo del avance del programa e implementación de soluciones con sujeción al mapa de riesgos.

Capítulo IV

Plan de Contingencias para el Sistemas de Cómputo del CPG. Cactus de PGPB.

Justificación.

El procesamiento del petróleo representa uno de los pilares más importantes de la economía mexicana, para captar divisas y generar empleos. Por lo anterior, mantener un flujo ininterrumpido de esta actividad es de vital importancia para el país.

La empresa petrolera ha alcanzado un avanzado nivel de desarrollo tecnológico en la automatización de sus plantas de extracción, procesamiento, almacenamiento y distribución de productos en todo el territorio nacional. Este mismo nivel de desarrollo tecnológico, vuelve imperante el hecho de crear planes de contingencias que garanticen la continuidad de los procesos operativos y administrativos ante la ausencia de los basados en tecnología.

El problema que se visualizó que podría causar la transición al nuevo milenio, contribuyó a tomar conciencia de lo urgente y necesario que es contar con planes de contingencias en los que, pasando por diferentes fases críticas, se logre amortiguar la dependencia de los sistemas de cómputo para su reemplazo temporal por procesos o procedimientos alternos que permitan mantener la continuidad de la operación de la empresa.

Se determinó aplicar ,como primera etapa, los lineamientos desarrollados en el capítulo III, para la elaboración del plan de contingencias del Ärea de Microcomputadoras y Red LAN/WAN del sistema de cómputo del CPG. Cactus, debido a que las funciones desarrollas en esta Área son esenciales para el monitoreo e intercambio de flujos de información entre las diferentes plantas de procesamiento.

Plan de Contingencias para el Sistemas de Cómputo.

Servidores y Redes LAN/WAN

Centro Procesador de Gas Cactus

CONTENIDO

1.- Gestión Integral de Riesgos : Lista.

Area:	**SERVIDORES Y REDES LAN/WAN.**
Función:	Dar servicio continuo de interconexión de enlaces entre estaciones de trabajo y terminales de los diferentes clientes que tienen una aplicaciones en el servidor de la red.

Categoría de Riesgo	Definición
Entidades externas.	En esta área de riesgo se considera el mal funcionamiento de los servicios que prestan otra entidades.
Falla en aplicaciones.	En esta área de riesgo se consideran las fallas en las aplicaciones sobre las que se basan los procesos críticos de negocios.
Fallas en los equipos, redes y software.	En esta área de riesgo se consideran las fallas en los equipos de computación, fallas en las comunicaciones y/o equipos de red.
Seguridad física.	En esta área de riesgo se consideran los daños en las instalaciones físicas del edificio o del centro de cómputo..
Seguridad lógica.	En esta área se consideran los problemas relacionados al acceso a los sistemas de información que dañen los datos o el mal funcionamiento del sistema de cómputo por errores.
Sistemas de respaldo.	Esta área de riesgo tiene que ver con la falta de procedimientos de respaldo de equipos, programas, manuales y base de datos para recuperarlos en caso de daño y destrucción y así garantizar la continuidad del servicio.

Firma
Nombre:
Gerente División/Director Departamento

Firma
Nombre:
Líder Usuario Grupo Contingencias

2.- Análisis de Impacto Global del Area.

Usuario Líder que elabora el Formulario	Juan Miguel de la Garza
Área	Servidores y Redes LAN/WAN.
Fecha:	Junio 22 de 2000.

UBICACIÓN DEL AREA EN LA ORGANIZACION

Sección	Soporte Técnico
Departamento	Departamento de Sistemas
Gerencia	Gerencia de Tecnología

SERVICIOS DEL AREA.

Objetivos del Area.

Mantener servicios confiables y disponibles de interconexión y comunicación entre las estaciones de trabajo, sistema en línea, servidores Novell y Windows NT, sistema de comunicación, impresoras, software genérico y demás actividades relacionadas con el área.

Procesos de negocio basados en tecnología.

1. Plantas automatizadas de procesamiento de gas del CPG. Cactus.
2. Terminales de almacenamiento de productos procesados.
3. Terminales de distribución de productos procesados.

Aplicaciones críticas.

1. Sistema de Control Avanzado de Plantas Procesadores de Gas..
2. Sistema de Administración SAP.
1. Sistema de Información de Plantas 'PI'.

Correo electrónico.

Otros procesos.

1. Sistema de Nómina.
2 Sistema de Facturación.
3. Sistema de Control de Inventarios.
4. Sistema de Adquisiciones.

CLIENTES:

1. Plantas de Endulzamiento de Gas.
2. Plantas Criogenicas.
3. Plantas Fraccionadoras.
4. Servicios Auxiliares.
5. Recursos Materiales y Administración.

PROVEEDORES:

1. Proveedores de Sistemas Operativos de Administración de redes.
2. Proveedores de equipos electrónicos para redes.
3. Proveedores de materiales empleados en los procesos productivos.

IMPACTOS

Impactos:

1. En la atención de sus clientes (internos/externos):

   Atraso en transferencias de información solicitadas por los clientes.

2. En ingresos que deja de percibir:

   En caso de que el sistema de cómputo deje de operar por 12 horas se dejará de percibir un ingreso por ventas de derivados del gas de $18,000,000.00 de peso.

3. En pérdida de mercado:

   Debido a que Pemex Gas y Petroquímica Básica es una empresa paraestatal con concesión de mercado único, este impacto no tiene repercusión.

4. En la imagen de la empresa:

   Se daña la imagen de la empresa debido a la inseguridad que representan las fallas en las plantas de procesamiento de gas que están automatizadas.

5. En sanciones del órgano rector:

   Pemex Gas y Petroquímica Básica como empresa paraestatal debe cubrir cuotas de producción y en caso de incumplimiento esta sujeta a sanciones administrativas.

Períodos críticos en caso de que se presente una interrupción prolongada en los servicios del Area:

Durante todo el año.

Tiempo que el área podría operar sin el apoyo de la tecnología:

El máximo tiempo permitido es de 6 horas.

Impacto en las operaciones de otras áreas o aplicaciones críticas:

1. Errores en el sistema de administración SAP.
2. Error en la optimización de los procesos productivos de las plantas procesadoras de gas.
3. Error en almacenamiento y distribución de productos procesados.

PROCEDIMIENTOS ALTERNOS:

1. Procedimiento de carga programas de aplicación y sistemas operativos en servidores y estaciones de trabajo de la red.
2. Procedimiento para realizar respaldos de información.
3. Procedimientos para remplazar equipos electrónicos en servidores, estaciones de trabajo, de comunicación e interconexión de redes LAN o WAN.
4. Procedimiento para realizar pruebas de funcionamiento en sistemas ininterrumpibles de energía.
5. Procedimiento para realizar pruebas de bancos de baterías.

3.- Matriz Causa – Efecto.

			E F E C T O S
C A U S A S	A P L I C A C I O N E S	Fallas en el sistema de administración SAP.	• Daño parcial o total en los procesos administrativos (control de personal, compras, programación de presupuestos, control de inventarios). • Daño parcial o total en los procesos operativos (ordenes de trabajo, programación de mantenimientos preventivos y correctivos).
		Falla en el sistema de información de plantas PI.	• Funcionamiento incorrecto en los procesos productivos por transferencias erróneas entre plantas. • Suministro incorrecto de información de producción para la toma de decisiones en tiempo real.
		Falla en el sistema de control avanzado.	• Programación incorrecta de los procesos de optimización de los procesos productivos por transferencias incorrectas de información. • Tomas de decisiones equivocadas debido a información errónea.
	E X T E R N A S	Falla en el suministro de energía eléctrica.	• Daño al hardware del sistema por variaciones eléctricas. • Interrupción de los servicios de interconexión por falta de energía eléctrica. • Interrupción del procesamiento de información por pérdida de equipos claves. • Interrupción del servicio de aire acondicionado para los equipos electrónicos.
		Contaminación Ambiental	• Daño en los equipos electrónicos por elementos corrosivos derivados del procesamiento del gas.

Matriz Causa – Efecto.

			EFECTOS
CAUSAS	HARDWARE	Falla en los servidores de redes.	• Interrupción parcial o total de los servicios de transferencia de información entre plantas de producción. • Pérdida de la intercomunicación entre equipos de comunicación de plantas. • Interrupción de los servicios administrativos del centro Cactus.
		Fallas en las estaciones de trabajo.	• Interrupción de los procesos de reconfiguración y monitoreo de las plantas de producción. • Daño parcial o total de los procesadores de las estaciones de trabajo.
		Falla en los medios de enlace de red (cables).	• Pérdida de información de los procesos operacionales y administrativos. • Plantas de producción o área administrativas sin comunicación.
		Fallas en los equipos de comunicación de la red.	• Pérdida de información de los procesos operacionales y administrativos. • Pérdida de enlaces de comunicación entre plantas y áreas administrativas.
	SOFTWARE	Fallas en el sistema operativo.	• Daño en aplicaciones críticas. • Daño o interrupción en el procesamiento de información, sin que se llegue a presentar daño en el hardware y software.
		Fallas en los sistemas de administración de red.	• Mal funcionamiento de los recursos de la red (impresoras, modems, etc). • Interrupción de transferencia de información. • Respaldos erróneos de información crítica del sistema.

Matriz Causa – Efecto.

			E F E C T O S
C A U S A S	SOFT-WARE	Daño en las bases de datos.	• Procesamiento erróneo del sistema de administración. • Procesamiento erróneo del sistema de información de plantas. • Pérdida de información de las aplicaciones del sistema.
	SEGURIDAD FÍSICA	Robo de equipo electrónico.	• Desconexión y pérdida de equipo electrónico. • Pérdida de interconexiones entre servidores.
		Robo de información.	• Pérdida de software de desarrollo y aplicaciones del sistema. • Pérdida de documentación del sistema. • Pérdida de respaldos de información. • Procesamiento de datos erróneos por falta de información y documentación.
	SEGURIDAD LÓGICA	Acceso no autorizado a la red.	• Robo de información confidencial del sistema. • Alteraciones de los programas de aplicaciones críticas.
		Errores de operadores.	• Programación errónea de instrucciones de programación de la operación de las plantas de procesamiento. • Destrucción de información por operación errónea del sistema.
		Virus en la red.	• Operación inestable y errónea de los sistemas críticos. • Alteración en el funcionamiento de las estaciones de trabajo y servidores de la red. • Daño parcial o total de los sistemas de almacenamiento de información (Discos duros, discos flexibles).

4.- Planeación de escenarios.

Área: Servidor yRedes LAN/WAN.
Proceso: Sistemas de interconexión.
Responsable del proceso: Antonio Ruíz Contreras.
Fecha: Abril: Junio 2000.

Tipo de riesgo	Escenario (problemas potenciales de fallas en el área)	Riesgo (amenaza a la que se vería expuesta la empresa)	Probabilidad De Ocurrencia del escenario	Impacto en el área (A,M,B)			
				Operacionales	Financieros	Competitividad	Global
Interno	APLICACIONES	Fallas en las aplicaciones de los procesos críticos del CPG. Cactus.	A	A	B	A	A
Interno	HARDWARE	Fallas en los equipos de computación, comunicaciones y interfaces de red.	A	A	M	A	A
Interno	SOFTWARE	Fallas en los equipos de computación, comunicaciones y interfaces de red.	A	A	M	A	A
Interno	SEGURIDAD FÍSICA	Daños en la instalaciones físicas del edificio, de las instalaciones de la red y del centro de cómputo.	M	M	M	A	M
Interno	SEGURIDAD LÓGICA	Accesos no autorizados a los sistemas de información que provocan daños en los datos o en el funcionamiento de un sistema.	M	A	B	A	A
Externo	SERVICIOS EXTERNOS (ENERGÍA ELÉCTRICA)	Mal funcionamiento de los equipos de comunicación e interconexión por falta de energía eléctrica.	M	A	A	A	A

5.- Clasificación, priorización y efecto de los riesgos.

Area: Servidores y Redes LAN/WAN.
Proceso: Sistemas de interconexión.
Responsable del proceso: Antonio Ruiz Contreras.
Fecha: Junio 2000.

Rango	Prioridad	Escenario (problemas potenciales por fallas en el área)	Riesgo (amenaza a la que se vería expuesta la empresa)	Efecto probable (descripción o cuantificación del efecto que se tendría). **
1	A	HARDWARE.	Fallas en los equipos de computación, comunicaciones y interfaces de red.	Interrupción de transferencias de información de procesos operativos, producción y administrativos. **
2	A	SOFTWARE.	Fallas en los equipos de computación, comunicaciones y interfaces de red.	Daño o mal procesamiento de información de los procesos críticos. **
3	A	SERVICIOS EXTERNOS.	Mal funcionamiento de los equipos de comunicación e interconexión por falta de energía eléctrica.	Interrupción del funcionamiento del equipo de cómputo, comunicaciones y de interconexión. **
4	A	APLICACIONES.	Fallas en las aplicaciones de los procesos críticos del CPG. Cactus.	Mal funcionamiento de los procesos de óptmización de la producción, así como inoperabilidad de las aplicaciones críticas. **
5	M	SEGURIDAD LÓGICA.	Accesos no autorizados a los sistemas de información que provocan daños en los datos o en el funcionamiento de un sistema.	Destrucción de información por virus o errores cometidos por los operadores del equipo de cómputo. **
6	M	SEGURIDAD FÍSICA.	Daños en la instalaciones físicas del edificio, de las instalaciones de la red y del centro de cómputo.	Pérdida de información y documentación vital del sistema de cómputo. **

** VER MATRIZ CAUSA – EFECTO.

6.- Acciones de Prevención y Mitigación.

H A R D W A R E		
RIESGOS	**EFECTOS PROBABLES**	**ACCIONES DE PREVENCIÓN/MITIGACIÓN**
Falla en los servidores de redes.	• Interrupción parcial o total de los servicios de transferencia de información entre plantas de producción. • Pérdida de la intercomunicación entre equipos de comunicación de plantas. • Interrupción de los servicios administrativos del centro Cactus.	• Suministro y mantenimiento en stock de un servidor para contingencias. • Revisión y actualización de los procedimientos manuales aplicables a las áreas administrativas. • Instalación y puesta en operación del servidor para contingencias.
Fallas en las estaciones de trabajo.	• Interrupción de los procesos de reconfiguración y monitoreo de las plantas de producción. • Daño parcial o total de los procesa-dores de las estaciones de trabajo.	• Suministro y mantenimiento en stock de un procesador para contingencias. • Instalación y puesta en operación del procesador.
Falla en los medios de enlace de red (cables).	• Pérdida de información de los procesos operacionales y administrativos. • Plantas de producción o área administrativas sin comunicación.	• Habilitamiento de los enlaces físicos redundantes de la red. • Realizar respaldos de información locales con mayor frecuencia en las plantas o los procesos administrativos que están aislados.
Fallas en los equipos de comunicación de la red.	• Pérdida de información de los procesos operacionales y administrativos. • Pérdida de enlaces de comunicación entre plantas o áreas administrativas.	• Habilitamiento de los equipos alternos de comunicación. • Realizar respaldos de información locales con mayor frecuencia en las plantas o los procesos administrativos que están aislados. •

SOFTWARE		
RIESGOS	**EFECTOS PROBALES**	**ACCIONES DE PREVENCIÓN/MITIGACIÓN**
Fallas en el sistema operativo.	• Daño en aplicaciones críticas. • Daño o interrupción en el procesamiento de información, sin que se llegue a presentar daño en el hardware y software.	• Pruebas de integridad al respaldo del sistema operativo. • Revisión y actualización del procedimiento para realizar el cargado del sistema operativo en los equipos de cómputo.
Fallas en los sistemas operativos para administración de la red.	• Mal funcionamiento de los recursos de la red (impresoras, modems, etc). • Interrupción de transferencia de información. • Respaldos erróneos de información crítica del sistema.	• Pruebas de integridad a los programas controladores de equipo periférico de la red. • Revisión y actualización del procedimiento para realizar el cargado del sistema operativo de administración en los servidores de la red. • Realizar respaldos de la configuración de la red, cada 30 días.
Daño en las bases de datos	• Procesamiento erróneo del sistema de administración. • Procesamiento erróneo del sistema de información de plantas. • Pérdida de información de las aplicaciones del sistema.	• Realizar respaldo, en disco óptico, de la base de datos del sistema de información de plantas PI, sistema de administración SAP y sistema de control avanzado, cada 8 días.

APLICACIONES		
RIESGOS	**EFECTOS PROBABLES**	**ACCIONES DE PREVENCIÓN/MITIGACIÓN**
Fallas en el sistema de administración SAP.	• Daño parcial o total en los procesos administrativos (control de personal, compras, programación de presupuestos, control de inventarios). • Daño parcial o total en los procesos operativos (ordenes de trabajo, programación de mantenimientos preventivos y correctivos).	• Realizar respaldo, en disco óptico, de la base de datos del sistema de administración SAP, cada 8 días. • Habilitar de los respaldos las bases de datos de las aplicaciones en los equipos de cómputo. • Almacenar los respaldos de las aplicaciones en el lugar acordado.
Falla en el sistema de información de plantas PI.	• Funcionamiento incorrecto en los procesos productivos por transferencias erróneas entre plantas. • Suministro incorrecto de información de producción para la toma de decisiones en tiempo real.	• Realizar respaldo, en disco óptico, de la base de datos del sistema de administración SAP, cada 8 días. • Habilitar de los respaldos las bases de datos de las aplicaciones en los equipos de cómputo. • Almacenar los respaldos de las aplicaciones en el lugar acordado.
Falla en el sistema de control avanzado.	• Programación incorrecta de los procesos de optimización de los procesos productivos por transferencias incorrectas de información. • Tomas de decisiones equivocadas debido a información errónea.	• Realizar respaldo, en disco óptico, de la base de datos del sistema de administración SAP, cada 8 días. • Habilitar de los respaldos las bases de datos de las aplicaciones en los equipos de cómputo. • Almacenar los respaldos de las aplicaciones en el lugar acordado.

FACTORES/ SEVICIOS EXTERNOS		
RIESGOS	**EFECTOS PROBABLES**	**ACCIONES DE PREVENCIÓN/MITIGACIÓN**
Falla en el suministro de energía eléctrica.	• Daño al hardware del sistema por variaciones eléctricas. • Interrupción de los servicios de interconexión por falta de energía eléctrica. • Interrupción del procesamiento de información por pérdida de equipos claves. • Interrupción del servicio de aire acondicionado para los equipos electrónicos.	• Pruebas de transferencia de carga al sistema de energía ininterrumpible alterno. • Pruebas de integridad de carga al banco de baterías alterno. • Puesta en operación del sistema ininterrumpible de energía UPS. • Restablecimiento de los equipos de computo caídos por falta de energía eléctrica.
Contaminación Ambiental	• Daño en los equipos electrónicos por elementos corrosivos derivados del procesamiento del gas. • Daño a los sistemas de filtrado de aire.	• Pruebas de hermeticidad en los gabinetes que alojan los componentes electrónicos de los equipos de cómputo. • Remplazo de los filtros de aire cada tres meses. • Remplazo de componentes electrónicos dañados por corrosión, siguiendo el procedimiento de sustitución de componentes electrónicos.

SEGURIDAD LÓGICA		
RIESGOS	**EFECTOS PROBABLES**	**ACCIONES DE PREVENCIÓN/MITIGACIÓN**
Acceso no autorizado a la red.	• Robo de información confidencial del *sistema.* • Alteraciones de los programas de aplicaciones críticas.	• Instalar programas centinelas de verificación de intentos de acceso a la red. • Reconfiguración de los programas de aplicación crítica a condición de solo lectura. • Habilitamiento de los respaldos de los programas de aplicación, una vez detectada la violación a la red.
Errores de operadores.	• Programación errónea de instrucciones de programación de la operación de las plantas de procesamiento. • Destrucción de información por operación *errónea* del sistema.	• Capacitación y entrenamiento cruzado al personal con respecto a los equipos, a los procesos, a las aplicaciones y a las normas y procedimientos. • Habilitamiento de los respaldos de los programas de aplicación, una vez detectado el error.
Virus en la red.	• Operación inestable y errónea de los sistemas críticos. • Alteración en el funcionamiento de las estaciones de trabajo y servidores de la red. • Daño parcial o total de los sistemas de almacenamiento de información (Discos duros, discos flexibles).	• Establecimiento de controles de prevención de virus tales como: no cargar programas de sitios de internet no confiables, no cargar programas desde disketes, usar siempre disketes protegidos, proteger los disketes originales de software. • Aplicación de software antivirus antes de iniciar la carga de un respaldo de un programa de aplicación.

SEGURIDAD FÍSICA		
RIESGOS	**EFECTOS PROBABLES**	**ACCIONES DE PREVENCIÓN/MITIGACIÓN**
Robo de equipo electrónico.	• Desconexión y pérdida de equipo electrónico. • Pérdida de interconexiones entre servidores.	• Instalación de circuitos cerrados de TV para vigilancia. • Instalación de sistemas dactilares de acceso a las instalaciones. • Remplazo inmediato de los equipos que hallan sufrido daño.
Robo de información.	• Pérdida de software de desarrollo y aplicaciones del sistema. • Pérdida de documentación del sistema. • Pérdida de respaldos de información. • Procesamiento de datos erróneos por falta de información y documentación.	• Instalación de sistemas dactilares de acceso a las instalaciones donde se almacenan los originales y respaldos de los programas de aplicación y la documenta-ción del sistema. • Una vez detectado el robo, hacer nuevos respaldos de aplicaciones, sistemas operativos, herramientas de desarrollo y documentación.

7.- Plan de Contingencia.

Area: Servidores y Redes LAN/WAN.
Responsable del proceso: Antonio Ruiz Contreras.
Fecha: junio 2000.

Alcance:
Establecer acciones que permitan prevenir y remediar fallas en los servidores, estaciones de trabajo, equipos de comunicación, programas y sistemas operativos que integran la red LAN/WAN.

Objetivo:
Dar continuidad en el funcionamiento de servidores, estaciones de trabajo, equipos de comunicación, suministro de energía eléctrica, aplicaciones y sistemas operativos integrados a la red.

Areas afectadas:
Plantas de procesamiento de gas.
Recursos materiales.
Sistema de administración SAP.
Sistema de información de plantas PI.
Sistema de control avanzado.
Sistema de nómina.
Sistema de inventarios.

Responsables:

Antonio Ruiz Contreras/Grupo de atención de contingencias – est. 32377.

Antonio Renteria Pineda/Gerente de Tecnología – ext. 32587.

Criterios para invocar el plan:

- Los servidores de la red dejan de operar por más de 15 minutos.
- Los equipos de comunicaciones dejan de operar por más de 15 minutos.
- Las estaciones de trabajo operan inadecuadamente por espacio de 30 minutos.
- No se establece comunicación entre plantas de producción por 30 minutos.
- Los reportes de las aplicaciones son erróneos.
- Se detecta pérdida de información y documentación del sistema.

Procedimiento para invocar el modo de contingencia:

- Notificar a todos y cada uno de los elementos que intervienen en la operación y uso de la red LAN/WAN, que se ha iniciado la ejecución del *plan de contingencia.*
- Avisar al responsable directo de contingencias, en caso de que no *responda al llamado dar aviso al gerente del área.*

Procedimiento para operar en modo de contingencia :

- Conjuntar todos los elementos de hardware y software necesarios para el restablecimiento de los equipos o programas que presenten la falla.
- Aplicar el procedimiento de habilitamiento de programas en equipos de cómputo.
- En caso de que se requiera aplicar los procedimientos de operación manual para las Terminales de Almacenamiento y Distribución.
- Aplicar el procedimiento de remplazo de equipos electrónicos.
- Efectuar pruebas de funcionamiento confiable de programas o equipos de cómputo restablecidos.

Recursos para operar el modo de contingencia

- Personal técnico capacitado para atender fallas en los servidores y equipos de la red LAN/WAN.
- Disponibilidad del servidor alterno.
- Disponibilidad de la estación de trabajo adicional.
- Disponibilidad del cable alterno de interconexión de la red.
- Disponibilidad de los *equipos de comunicación adicionales.*
- Disponibilidad de la fuente ininterrumpible de energía eléctrica.
- Disponibilidad de los respaldos de los programas de aplicación, sistemas operativos, bases de datos, listados de configuración de las plantas de *procesamiento.*
- Computadoras e impresoras para apoyo de los procedimientos manuales de las *terminales de almacenamiento y distribución.*

Criterios para retornar al modo normal de operación:

- Restablecimiento de la operación normal de los programas y equipos de computo que integran la red LAN/WAN.
- Realizar actualización y respaldo de información.

Procedimiento para retornar al modo de operación normal:

- Dar aviso a todos los elementos y usuarios de la red LAN/WAN que el servicio esta operando en modo normal y se ha levantado la fase de contingencia.
- Realizar dos respaldos de los programas de aplicación, sistemas operativos, bases de datos, listados de configuración de las plantas de procesamiento.
- Guardar los respaldos de la información el área destinada para ello en el cuarto de control central.

Conclusiones

El problema de las fallas de los sistemas de cómputo, a pesar de ser de naturaleza técnica, es primordialmente un problema que afecta los negocios de las empresas y muchas organizaciones deben encarar las interrupciones o fallas inducidas por el riesgo de los sistemas en los procesos esenciales de su empresa. Las organizaciones deben reducir el riesgo y el impacto potencial de las fallas sufridas por los sistemas basados en tecnología que afecten los procesos esenciales de la empresa mediante la implementación de una rigurosa planificación de la continuidad de los negocios.

La continuidad en el funcionamiento de los sistemas de cómputo es un factor fundamental en la operación de las plantas industriales. Por ello, es importante que se realice un planeación detallada de las contingencias que se puedan presentar y se implementen planes que garanticen la continua funcionalidad de los equipos, programas y datos que integran el sistema de cómputo, lo cual permitirá a su vez la continuidad en las operaciones de cada una de las plantas industriales.

La planeación de contingencias empleando la técnica de causa - efecto para realizar el análisis sistemático de los posibles escenarios de fallas facilita una más efectiva toma de decisiones, debido a que permite entender a partir de hoy lo que puede suceder en el futuro. Su aplicación también permite que el personal operativo involucrado en el proceso de planeación de contingencias, entiendan la naturaleza dinámica y cambiante de su ambiente y analicen los problemas en forma estratégica, buscando la máxima flexibilidad ante la incertidumbre.

El plan de contingencias para el área de redes LAN/WAN del CPG. Cactus asegura la determinación de caminos alternativo para dar continuidad a su funcionamiento, permitiendo reconocer con mayor efectividad las causa u efectos de las fallas, para evitar sorpresas. También ayuda al grupo de contingencias a adaptarse y actuar efectivamente ante la presencia de contingencias en los sistemas de cómputo, dándose la viabilidad de su operación continúa.

Los lineamientos para los planes de contingencias cumplen con la finalidad de que los responsables de los sistemas de cómputo de los CPG´s de PGPB cuenten y hagan uso de esta herramienta para elaborar sus correspondientes planes de contingencias.

Debe considerarse que el plan de contingencia para los sistemas basados en tecnología ha de ser una preocupación constante de la organización, a un nivel suficientemente alto, que no es un problema exclusivamente técnico y de los técnicos, y que se trata de un camino alternativo para el que puede haber indicaciones, pero que será diferente según la entidad y el momento.

Por lo anterior es preciso no concentrarse exclusivamente en los problemas de tipo técnico, sino en los impactos a la organización de la empresa e incluso al exterior. Los planes de contingencia, deben comprender, en consecuencia las acciones técnicas y organizativas, necesarias para garantizar la continuidad de las operaciones de la empresa.

Por último podemos decir que, siendo la tecnología un activo estratégico, un plan de contingencia, es la culminación de la seguridad, si bien puede suponer cierta complejidad y un costo adicional, pero es necesario para que la empresa pueda asegurar la continuidad de sus operaciones cuando ocurra una falla en los sistemas basados en tecnología.

Bibliografía

1.- Planeación de la Recuperación
IBM de México. 1994.

2.- Disaster Backup/Planning Presentation
Wayne P. Lambert
Sperry-Eagan, Mn.

3.- Contingency and Disaster Planning and Disaster Recovery
Laurence W. Olson
Unisys, Chicago, Il.

4.- Guía del Planeamiento para la Continuidad de los Negocios.
Strohl Systems
Gulph, Boston, 1999.

5.- Lineamientos Metodológicos para afrontar Problemas Informáticos.
Instituto Nacional de Estadística e Informática.
México, 1998.

6.- Guía para la elaboración de Planes de Contingencia para el Y2K.
Programa infoDev.
Banco Mundial, 1999.

7.- Plan Estratégico de Pemex Gas y Petroquímica Básica.
PGPB, México, 1997.

8.- Técnicas Heurísticas.
Gabriel de las Nieves Sánchez Guerrero.
UNAM.

ARTÍCULOS DE INTERNET:

U.S. Army Contingency Planning Resources
http:/www.army.mil/army-Y2

Contingency Planning. SEC Reporting Requirements for Investment Companies.
http:/www.whistlepig.com/wpinternet/y2kinvest.htm

Contingency Plan Guidelines.
http:/www.mitre.org/research/y2k/docs/contingency_guidelines.html

Manual de Contingencias.
http:/www.bancunal.com.co/contingencias/manualcontingencias.htm

Plan de Contingencias y Seguridad de laInformación.
http:/www.inei.gob.pe/cpi/bancopub/libfree/lib611/121.htm

Problema Y2K.
http:/members.es.tripot.de/Contaduria/2004.html.

Contingencias
http:/www.bancunal.com.co/Contingencias/ManualContingencias.html.

Year 2000 Contingency Planning
http:/www.bancunal.com.co/Contingencias/y2k3.html.