UNIVERSIDAD APEC
UNAPEC

DECANATO DE INGENIERIA E INFORMATICA

PLAN DE RECUPERACIÓN ANTE DESASTRES PARA TECNOLOGÍA DE INFORMACIÓN DEL CENTRO DE IMÁGENES CEMADOJA.

Sustentantes:

LUIS RICARDO RODRÍGUEZ CUESTA	**2002-0359**
EUGENIO POLANCO BERROA	**2003-1483**
SILVANO SAÚL ESTÉVEZ GÓMEZ	**2004-0155**

Asesores:

ING. JACQUELINE J. VEGA
ING. RAMÓN GÓMEZ

Monografía para optar por el título de:
INGENIERO EN SISTEMAS COMPUTACIONALES.

Santo Domingo, D. N.
Agosto, 2009

PLAN DE RECUPERACIÓN ANTE DESASTRES PARA TECNOLOGÍA DE INFORMACIÓN DEL CENTRO DE IMÁGENES CEMADOJA.

Dedicatorias

DEDICATORIAS

Sonia Margarita Cuesta (Mi Madre):

Que además de darme la vida, ha formado la persona que soy ahora; siempre siendo para mí: madre, padre y amiga.

Esther Matos Cornelio (Novia):

Por apoyarme en todo momento y estar a mi lado mostrándome una forma positiva de ver las cosas.

Melissa Estrella (Hermana):

Que siempre es una gran amiga con la que puedo contar en cualquier situación, dándome su apoyo incondicional.

Guillermo Rodríguez (Abuelo):

Por ser para mí el modelo a seguir de una persona que cuenta con los valores necesarios para ser un Gran Hombre (Que en paz descanse).

Luís Ricardo Rodríguez Cuesta

DEDICATORIAS

A mi Dios:

Por permitirme lograr la mayor parte de mis metas.

A mi Madre:

Clara lidia (mi madre) por apoyarme y darme su amor incondicional y creer que podría lograr todas mis metas y esta es una de ellas.

A mi Padre:

Eugenio Polanco Rivera (mi padre) por ayudarme en cada momento que necesite de su ayuda y por sus grandes consejos.

A mi Novia:

A Ivonne por brindarme su amor y ayudarme a comprender que cada cosa viene a su debido tiempo.

A mis Amigos:

Mis amigos Juancito, Gustavo y Ricardo por a verme apoyado tanto en lo personal como en lo laboral los quiero mucho.

Eugenio Polanco Berroa.

DEDICATORIAS

A Mi Dios:

Las gracias por darme la vida, la sabiduría y entendimiento durante mi vida como estudiante y no permitir rendirme en los momentos difíciles de mi carrera.

A Mis Padres:

Colombia Gómez y Silvano Estévez por ser los mejores padres del mundo, gracias por todo su esfuerzo, su apoyo y por la confianza depositada en mi, gracias por estar siempre a mi lado. Los Amo.

A Mi Novia:

Cesarina Ortiz por ser para mí una fuente de inspiración y confianza, por darme el amor y el apoyo que necesite en cada momento. Por enseñarme que la desesperación es parte del fracaso, gracias porque sin ti no hubiera logrado mis metas, Te Amo mi Reyna.

A Mis Hermanas:

Silvana Matilde y Matilde Silvana porque a pesar de los buenos y malos momentos siempre se mantuvieron cerca de mí. Y me brindaron su amor, apoyo y cariño, Ah y También las Amo Mis Manitas.

A Mis Amigos (as): Pablo Torres, Eugenio Polanco, Luís Rodríguez, Laura Cruz, los cuales me sirvieron de ayuda y apoyo a lo largo de mi carrera.

Silvano Saúl Estévez Gómez

Agradecimientos

AGRADECIMIENTOS

A Dios:

Por mostrarme cada día que lo que puedo alcanzar a ver a través de mis ojos es insignificante relacionado con lo que puedo alcanzar a través del espíritu.

Sonia Margarita Cuesta:

Que siempre ha estado para aconsejarme, guiarme y apoyarme.

Esther Matos Cornelio:

Que me ha ayudado y apoyado en todo lo que he necesitado.

Luís Ricardo Rodríguez Cuesta

AGRADECIMIENTOS

A Mi Dios:

Por ofrecerme su fe y que siempre estuvo a mi lado en los momentos difíciles.

A Mi Familia:

Le agradezco a mi familia porque siempre estuvieron a mi lado me ayudaron a formarme como profesional, Gracias por todo.

A Mi Novia:

Porque fuiste una fuente de inspiración por el gran amor que me brindaste a lo largo de toda mi carrera, Te Amo Lobita.

A Mis Profesores:

Por ser nuestro guía en todo el transcurso de nuestra carrera y ser parte de nuestras vidas como maestros impulsadores del progreso.

Eugenio Polanco Berroa.

AGRADECIMIENTOS

A Mi Dios:

Por hacerme ver que cada día existe la esperanza de un mañana. Por ayudarme en todas las etapas de mi vida y hacer posible este momento.

A Mi Familia:

Por brindarme su apoyo y guiarme siempre por el camino al triunfo. Gracias!

A Mi Novia:

Porque aunque llegaste en la etapa final de mi carrera fuiste la fuente de inspiración y de esfuerzo para lograr mi gran apreciada meta, gracias mi Amor.

A Mis Profesores:

Por las sugerencias y ayudas que nos brindaron en los momentos necesarios, que impulsaron el desarrollo de nuestro proyecto y por orientarnos en todo momento en lo que necesitábamos.

Silvano Saúl Estévez Gómez

Índice

ÍNDICE

Introducción

INTRODUCCION

En la actualidad es de gran importancia para las organizaciones estar preparadas para asegurar sus ingresos ante cualquier impacto de cualquier amenaza producida en su entorno. El alto índice de incidentes ocurridos en una organización podría trastornar de mayor forma el desempeño de la misma.

Si bien es posible calcular las pérdidas económicas que pudiera generar una interrupción, generalmente no se puede calcular el daño que se refleja en una pérdida de imagen o confianza por un incidente mal manejado por la misma organización.

La gestión de continuidad de negocios busca mejorar la capacidad de recuperación de las organizaciones ante un desastre. Registrando un análisis de las posibles amenazas, vulnerabilidades y riesgos que pudieran afectar de forma negativa o circunstancial las operaciones de una organización, haciendo así posible establecer prioridades en la implementación de controles que ayuden a mitigar el daño causado por cualquier incidente.

El presente documento constituye la formulación del Plan de Recuperación Ante Desastres para el Centro de Educación Medica de Amistad Dominico – Japonesa CEMADOJA, el cual tiene como propósito definir los lineamientos de

políticas y los principios básicos que debe desarrollar la institución para la ejecución de programas y acciones que garanticen las mejores condiciones de seguridad y protección de los recursos del centro.

El Plan de Recuperación define los puntos de orientación, procesos y medidas a tomar en el corto, mediano y largo plazo. El mismo incluye una serie de programas para organizar el conjunto de acciones para que el departamento desarrolle para alcanzar los mayores niveles de seguridad frente a cualquier amenaza o riesgo existente y a su vez contribuir al mejoramiento y bienestar de cada área de la organización.

Capitulo I
Antecedentes Históricos

CAPITULO I
ANTECEDENTES HISTÓRICOS

1.1 Reseña Histórica de CEMADOJA

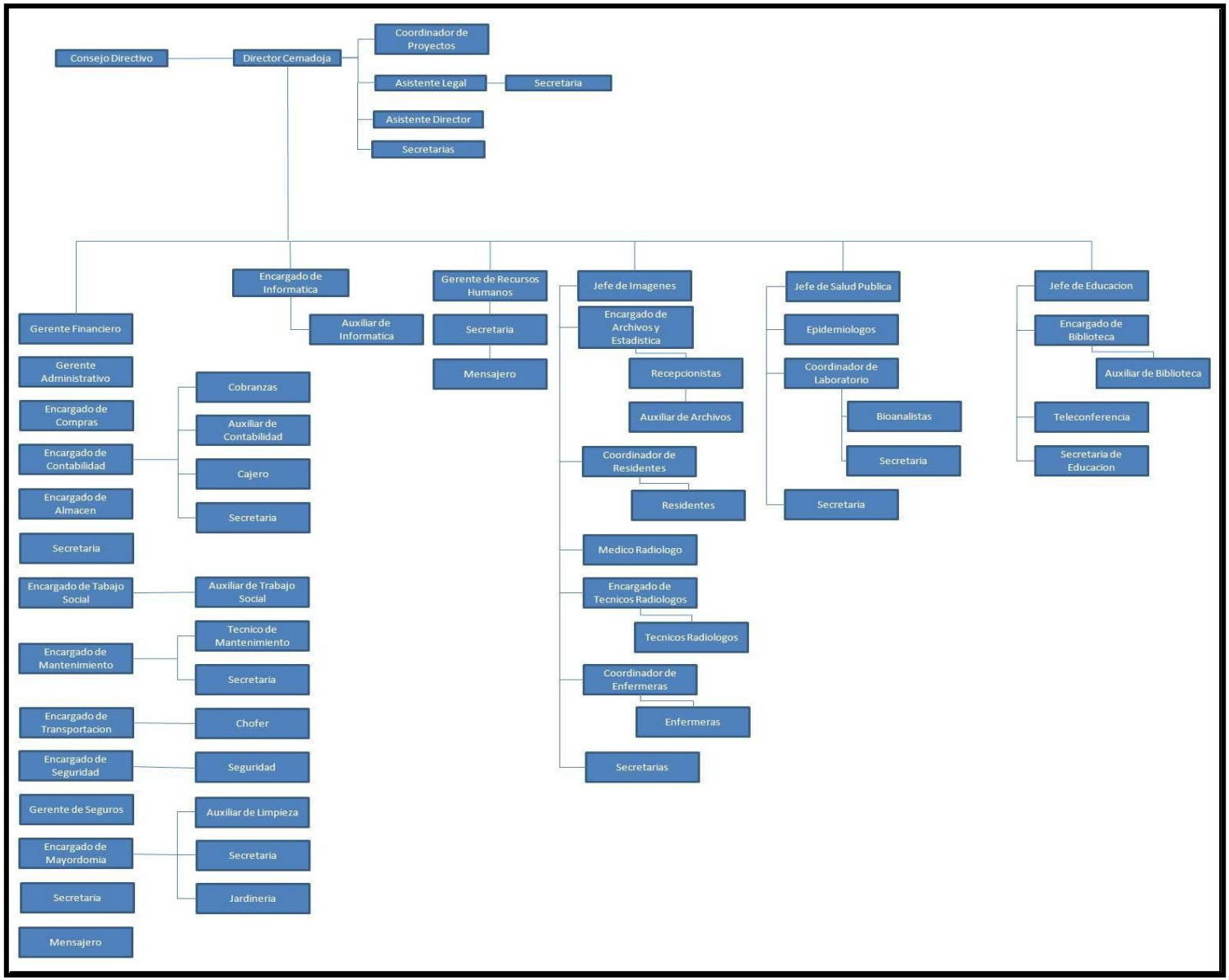
La SESPAS, para contribuir al sector salud y satisfacer las necesidades de una gran mayoría de la población Dominicana, solicitó al gobierno del Japón la construcción de un Centro de Educación Médica y Entrenamiento en la Ciudad Sanitaria Dr. Luís E. Aybar, mediante la Cooperación Financiera No Reembolsable del gobierno de Japón. En Respuesta a la solicitud del Gobierno Dominicano y luego de varios estudios de factibilidad realizados por la JICA, el gobierno de Japón construyó el CEMADOJA, el cual inicio sus actividades el 8 de octubre de 1999 bajo la coordinación y supervisión directa de la JICA. El Centro de Educación Medica de Amistad Dominico – Japonesa, es un centro de docencia, capacitación, formación e investigación para el desarrollo nacional de educación médica especializada y continua,

Brinda atención médica ambulatoria y de urgencia las 24 horas, en servicios de imágenes diagnosticas de alta tecnología. Cuenta con los cuidados de enfermeras y servicio de apoyo para formular el diagnóstico clínico del paciente. El CEMADOJA está ubicado dentro de la ciudad sanitaria Dr. Luís E. Aybar, en la cual se encuentra además las siguientes áreas: Hospital Dr. Luís E. Aybar, Centro de Gastroenterología Dominico –japonés, Unidad de Quemados Pearl E. Ort. Y Centro de Cardio-Neuro Oftalmológico y Trasplante (CECANOT).

1.2 Directiva Principal

La directiva administrativa de CEMADOJA Está constituida por un consejo directivo que es la autoridad suprema, una Dirección Ejecutiva, un coordinador de proyecto, 8 gerentes administrativos, siendo estos: Gerente financiero, Gerente administrativo, Gerente de informática, Gerente de Recursos Humanos, Gerente de Imágenes, Gerente de Salud Pública y Gerente de Educación, Gerente de Seguros, Dependiendo de estas gerencias están los Departamentos con sus respectivos encargados, Subdivisiones y secretarias.

1.3 Organigrama General



1.4 Servicios

Los Servicios Ofrecidos por el Centro de Imágenes se clasifican en los siguientes:

Imágenes:

- Mamografía
- Rayos X Convencional
- Resonancia Magnética
- Tomografía
- Sonografía
- Drenajes
- Biopsias Sondirigidas
- Biopsias Tomodirigidas
- Fluoroscopio
- Urografía
- Electrocardiograma
- Desintometría Ósea

Salud Pública y Epidemiología:

- Docencias a los residentes de diferentes especialidades
- Practica de los rotantes por el laboratorio
- Área de microscopia con microscopio triocular e inmunofluorescencia
- Equipo de PCR para la reacción en cadena de la polimerasa
- Equipos para cultivo celular de virus
- Equipo de Elisa para pruebas inmunológicas

Educación Médica

- Residentes rotantes en medicina
- Seminarios y congresos
- Informe de la evaluación de los médicos
- Actividades docentes
- Seguimiento de las actividades académicas
- Biblioteca
- Elaboración de revistas científicas
- Investigaciones Científicas

1.5 Misión y Visión

Misión:

Proporcionar diagnósticos por imágenes con los más altos estándares de calidad, así como formar médicos en imgeonología y epidemiología a través de la educación como un servicio socialmente responsable en la mejora de la salud pública.

Visión:

El personal del Centro comparte una visión del futuro que ha sido planteada en los siguientes términos: “Somos el Centro modelo de referencia internacional en educación en imagenología y epidemiología, con prestación de servicios en imágenes, con alta calidad humana y tecnológica”.

1.6 Situación Actual de la Empresa

Las situaciones de desastres tanto en la empresa con en el área de tecnología ocurren a menudo por desconocimiento de la empresa, por la Dirección de Tecnología o por alguna catástrofe sobrenatural. La República Dominicana está expuesta a varias amenazas meteorológicas, geológicas, y antrópicas, como huracanes, tormentas, inundaciones y riesgos tecnológicos.

Desde el año 2007 el Departamento de TI del Centro de Educación Medica de Amistad Dominico – Japonesa (CEMADOJA) ha venido desarrollando cambios muy significativo en su plataforma informática y en su estructura física, pero

estos a su vez no tienen elaborado un plan de contingencia para mitigar los efectos ante cualquier evento catastrófico que ponga en peligro la Institución, y se llegue a suspender las actividades diarias de la institución.

Actualmente el departamento de TI presenta problemas de almacenamiento de backup, ya que las cintas magnéticas que Utilizan son almacenadas en la misma área de trabajo y no tienen la debida protección necesaria. Por otro lado, no existe un software que realice los backup de aquellas informaciones almacenadas en las PC de cada usuario, por tal razón no hay forma de asegurar la información de uso diario en caso de algún desastre. Por otro lado, es necesario implementar controles de acceso físico al área al departamento de TI para así asegurar de una manera eficaz su data.

Otro gran problema que tiene el departamento de TI es la poca distribución de espacio para la correcta protección de los equipos informáticos que se encuentran expuestos a diferentes amenazas, como son; perdidas de equipos, desorden en el cableado. Esto conllevaría a realizar una reestructuración dentro de la institución y así buscar una mejor forma de salvaguardar las informaciones, equipos y demás dispositivos de dicho departamento.

CEMADOJA requiere un plan de contingencia, el cual le permita seguir sus operaciones y la producción no sea detenida de forma temporal o permanente. El área de TI requiere mayor disponibilidad de espacio y recursos que permitan contrarrestar una situación de desastres, ya que esta es el área primordial para

el desenvolvimiento de las funciones de dicha institución. Actualmente las informaciones de cada usuario y del servidor son sumamente valiosas, por lo que la perdida de estas llevaría a la institución a frenar sus operaciones por una largo tiempo.

1.7 Descripción de la Infraestructura de TI

Una infraestructura de tecnología de información (TI) funcionando adecuadamente es esencial para la calidad y continuidad de los procesos de negocios dentro de una organización. Esto ejerce presión en el departamento de TI para responder a preguntas rápidamente, resolver problemas inmediatamente y encontrar formas de prevenir problemas en el futuro.

Por lo que es necesario analizar cómo está la infraestructura de TI de la empresa.

- **Área de las Secretarias del Departamento.**
- **Oficina del Gerente de Informática.**
- **Área de Soporte Técnico.**
- **Área de Helpdesk.**
- **Área de almacenamiento de los backup (cintas magnéticas).**
- **Sistemas** – hardware, software y los datos.
- **Red** - comunicación de voz y datos.

1.8 Organigrama del Departamento de TI

Capítulo II
Conceptos Generales

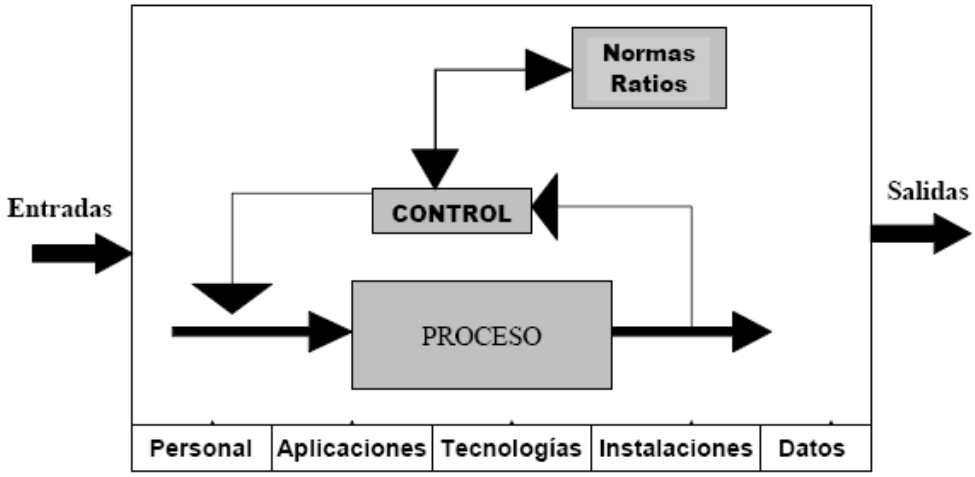
CAPITULO II
CONCEPTOS GENERALES

2.1 Que es un sistema de información

Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tan simples como en el que una persona tiene una computadora y le introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Sin embargo la mayor parte de los sistemas son mas complejos que el enunciando anteriormente. Normalmente una organización tiene más de un sistema de computadoras para soportar las diferentes funciones de la organización, ya sean de ventas, recursos humanos, contabilidad, producción, inventario, etc.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.



La figura anterior nos muestra en un sentido amplio que se puede considerar un Sistema de Información (**SI**) como un conjunto de componentes que interactúan para que la empresa pueda alcanzar sus objetivos satisfactoriamente. Los componentes o recursos de un SI son los siguientes:

- **Datos:** En general se consideran datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- **Aplicaciones:** Se incluyen los manuales y las aplicaciones informáticas.
- **Tecnología:** El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- **Instalaciones:** En ellas se ubican y se mantienen los sistemas de información.
- **Personal:** Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos.

2.2 Aspectos Generales de la seguridad física de la información

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación a la cronología del fallo.

Antes

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que de él se puedan derivar. Es un concepto aplicable a cualquier actividad, no sólo a la informática, en la que las personas hagan uso particular o profesional de entornos físicos.

- Ubicación del edificio.
- Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- Compartimentación.
- Elementos de la construcción.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

Durante

Se debe de ejecutar un plan de contingencia adecuado. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización. Por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que junto con el Centro Alternativo de Proceso de Datos, constituye el plan de contingencia que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

Son puntos imprescindibles del plan de contingencia:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas
- Establecer un periodo crítico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.

- Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en el que el centro alternativo puede procesar las aplicaciones críticas.
- Designar entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la capacidad de las comunicaciones.
- Asegurar la capacidad de los servidores back-up.

Después

Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar para el centro de proceso de datos una vez detectado y corregido el fallo. De la gama de seguros existentes, se pueden indicar los siguientes:

Centros de proceso y equipamiento: se contrata la cobertura sobre el daño físico en el CPD (Centro de Procesamiento de Datos) y el equipo contenido en el.

Reconstrucción de medios de software: cubre el daño producido sobre medio software tanto los que son de propiedad del tomador de seguro como aquellos que constituyen su responsabilidad.

Gastos extra: cubre los gastos extra que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos.

Interrupción del negocio: cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.

Documentos y registros valiosos: Se contrata para obtener una compensación en el valor metálico real por la pérdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de reconstrucción de medio software.

Errores y omisiones: proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida financiera a un cliente.

Cobertura de fidelidad: cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.

Transporte de medios: proporciona cobertura ante pérdidas o daños a los medios transportados.

Contratos con proveedores y de mantenimiento: proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

2.3 Seguridad integral de la información

La función del procesamiento de datos es un servicio de toda la institución, que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales. La Seguridad un aspecto de mucha importancia en la correcta Administración Informática, lo es también de toda la Institución.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren. En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

2.4 Concepto de Desastre

Es un hecho natural o provocado por el hombre que afecta negativamente a la vida, al sustento o industria desembocando con frecuencia en cambios permanentes en las sociedades humanas, ecosistemas y medio ambiente. Los

desastres ponen de manifiesto la vulnerabilidad del equilibrio necesario para sobrevivir y prosperar. Que Implica:

1. Implica la pérdida de la capacidad operativa de una organización, una localidad, región o país. Necesita para su resolución la participación cooperativa de varios grupos que normalmente no necesitan trabajar codo con codo para controlar emergencias.
2. Requiere que las partes implicadas renuncien a la autonomía y libertad tradicional para producir respuestas en conjunto y organizadas. Siguiendo un comando o estructura predefinida.
3. Cambia el desarrollo habitual de las medidas, y
4. Es necesario un acercamiento entre organizaciones públicas y privadas en las operaciones.

Según la magnitud del desastre, puede ocurrir:

1. Destruye a la mayor parte de una comunidad.
2. Impide a los servicios locales hacer sus deberes.
3. Provoca un cese en la mayoría de las funciones de la comunidad, e
4. Impide a las comunidades adyacentes el envío de ayuda.

Conceptos asociados:

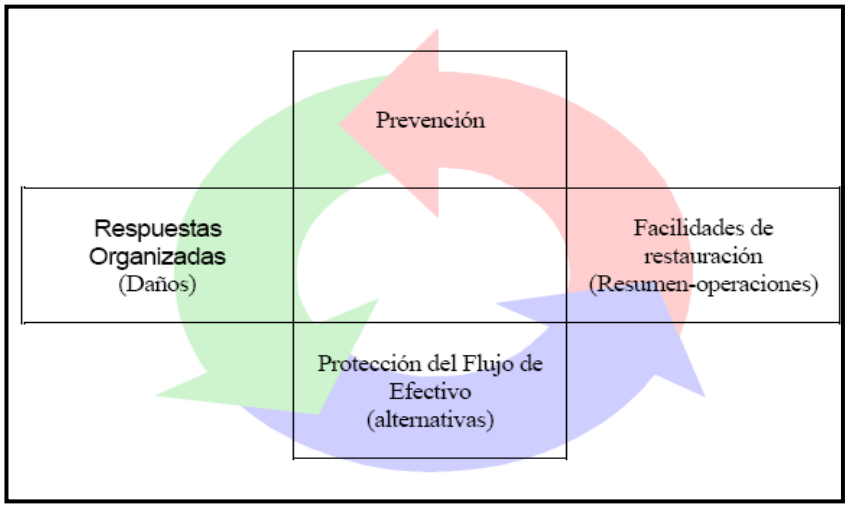
Emergencia ordinaria: Un acontecimiento que puede ser controlado localmente sin necesidad de añadir medidas o cambios en el procedimiento de atención

Catástrofe: Algunos conceptúan erróneamente que implica un mayor grado destructivo que un desastre. La acepción verdadera se entiende mejor si se considera la catástrofe como el "hecho" y el desastre como la consecuencia.

2.5 Ciclo de Vida de los Desastres

En la decisión de que es lo que debería incluirse en el plan, esto nos ayuda a entender las diferentes fases de un desastre. El ciclo de vida de un desastre consta de cuatro periodos de tiempo:

1. Operaciones normales
2. Respuestas de emergencia
3. Procesamiento interno
4. Restauración



Operaciones Normales

Las operaciones normales indican el periodo de tiempo antes de que ocurra un desastre. Esta fase del plan debe incluir la práctica de las operaciones que pretenden prevenir un desastre desde que principia, y de aquellas que ayudan a mitigar el impacto del mismo, prever lo que podría ocurrir.

Respuestas de Emergencia

Las respuestas derivadas de una situación de emergencia ocurren durante las pocas horas que siguen inmediatamente a un desastre. Esta fase de un plan identifica las actividades que pueden necesitar mayor atención durante este periodo, con la finalidad de asegurar una respuesta a la organización y proporcionar una lista de verificación de las emisiones importantes que pueden pasar inadvertidas durante la confusión que acompaña a los desastres.

Procesamiento Interno

El procesamiento interno es un procedimiento alternativo que representa el tiempo de duración de la contingencia en relación con el soporte de las funciones esenciales de la empresa hasta que la capacidad de procesamiento normal sea restaurada. Estos procedimientos alternativos, deberían ser desarrollados por un departamento funcional dividido en tres fases:

Inicio:

Esta sección identifica la necesidad de una preparación específica para asegurar las transiciones desde “el negocio como usual” hasta una modalidad de procesamiento interno.

Soporte de las funciones esenciales del negocio:

Esta sección describe los departamentos funcionales que están de acuerdo en el soporte de las funciones vitales del negocio durante el periodo de recuperación de desastres.

Recuperación de datos:

En esta sección, el plan cubre las responsabilidades funcionales para retener los datos transaccionales que ocurren durante el periodo de procesamiento interno, así que los archivos y bases de datos pueden ser actualizados cuando la capacidad de procesamiento normal sea restaurada.

Restauración

La restauración indica el periodo de tiempo destinado a aquellas actividades que se necesita realizar para recuperar una condición o capacidad de procesamiento en su operación normal. La restauración involucra necesariamente los pasos de la planeación, organización y control de tales actividades. Cuando el clima económico es favorable, los planes de contingencia están al final de la lista de las cosas que se necesitan hacer; cuando los beneficios son bajos, los planes de

contingencia forman parte de las actividades prioritarias de la empresa ya que se trata de asegurar el negocio, Además mientras mayor sea el costo en los proyectos del plan de contingencias, mayor será su plazo.

2.6 Concepto e Importancia de una Continuidad de Negocios

La Continuidad de Negocio es un proceso integral de gestión que identifica los posibles impactos que amenazan a una organización y ofrece un marco para proporcionar robustez y disponer de una respuesta efectiva que salvaguarde los intereses de los principales clientes, proveedores y demás partes interesadas, además de la reputación de la organización, su marca y las actividades creadoras de valor.

La Continuidad Negocios se centra particularmente en desarrollar una capacidad de recuperación que sea conjunta para toda la organización y le permita sobrevivir a la pérdida total o parcial de su capacidad operativa. Al identificar por adelantado los posibles impactos de una amplia gama de incidencias que trastornarían de forma súbita el éxito de la organización, la Continuidad Negocios aspira a mejorar la capacidad de recuperación de una organización.

El factor determinante de esta robustez en toda la organización se sustenta en la responsabilidad de la alta dirección de proteger los intereses a largo plazo del personal, clientes y todos aquellos que dependen de algún modo de la organización. Si bien se pueden calcular las pérdidas financieras ocasionadas por una interrupción, generalmente el mayor daño suele reflejarse en una

pérdida de imagen o de confianza fruto de un incidente mal gestionado. Del mismo modo, un incidente bien gestionado puede mejorar la imagen de la organización y su equipo de gestión.

Para que la Continuidad de Negocios sea efectiva tiene que ser asimilada y totalmente integrada en la organización como uno más entre sus procesos de gestión. Si bien las bombas, incendios e inundaciones acaparan los titulares de los medios de comunicación, el 90% de las incidencias que ponen en riesgo el negocio son "catástrofes silenciosas" que no figuran en los medios pero que pueden tener un efecto devastador para el buen funcionamiento de una organización. Muchas de las causas son ajenas al control de la organización y suelen estar a merced de los servicios de emergencias o de proveedores que marcan los plazos de la interrupción.

¿Cómo beneficiará la organización?

Planear para interrupciones es tan importante como planear cualquier otro proceso del negocio. Cuando los factores de la continuidad de negocios son integrados dentro de un plan central de la organización, la empresa puede responder antes escenarios no previstos de una manera confiable y ordenada.

La Continuidad de Negocios beneficia todos los tipos de organizaciones por igual, lo único que cambia es el enfoque de los procesos de acuerdo al tamaño y complejidad de la organización. Estos son algunos de los beneficios de orientar una organización a una cultura de Continuidad de Negocios:

Beneficios Organizacionales

- Mantenimiento de la salud y seguridad de los empleados.
- Restauración de los procesos críticos de una manera mas rápida
- Incrementación de la confianza y seguridad de los clientes.
- Reducción de los daños a la imagen, reputación y la marca.
- Manejo y control de los costos durante un periodo de restauración.

Beneficios Adicionales

- Promueve el trabajo en equipo y el intercambio de experiencia entre los empleados.
- Presenta una oportunidad de revisar la manera en que la organización realiza los procesos.

2.7 Concepto de Disaster Recovery Plan (DRP)

Es el proceso, políticas y procedimientos relacionados a la preparación para la recuperación o continuación del departamento de Tecnología de Información de una organización, luego de la ocurrencia de un desastre ya sea natural o inducida por seres humanos. El plan de recuperación de desastres (DRP por sus siglas en ingles) es parte de un proceso más grande conocido como Continuidad de Negocios.

Un DRP debe incluir la planeación para reanudación de aplicaciones, datos, hardware, redes de comunicación y otras infraestructuras de TI. El objetivo primordial es permitir a la organización la sobrevivencia ante un desastre y continuar con las operaciones del negocio de la manera más normal posible.

Para poder sobrevivir, la organización debe asegurar que las operaciones críticas se pueden reanudar para continuar con su procesamiento normal. El plan establece líneas claras de autoridad y prioriza los esfuerzos del trabajo.

Los objetivos claves en un plan de contingencia deben ser:

- Proveer seguridad y bienestar para las personas en la ocurrencia de un desastre.
- Continuar con las operaciones críticas del negocio
- Minimizar la duración de una interrupción critica para las operaciones y los recursos.
- Minimizar los daños y pérdidas inmediatas.
- Facilitar una coordinación efectiva de las tareas de recuperación.
- Reducir la complejidad de un esfuerzo de recuperación.
- Identificar las líneas críticas entre el negocio y las funciones que le sirven de soporte.

Los continuos avances de la misma tecnología y de las necesidades particulares de cada empresa, hace que el modelo del DRP sea un proceso cíclico con continuos ajustes y revisiones.

Capítulo III
Análisis de Riesgos

CAPITULO III
ANÁLISIS DE RIESGOS

3.1 ¿Que son los Riesgos?

Definiciones:

Es la probabilidad de que suceda un evento, impacto o consecuencia adversos. Se entiende también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento.

Es una medida de potencial de pérdida económica o lesión en términos de la probabilidad de ocurrencia de un evento no deseado junto con la magnitud de las consecuencias.

3.2 Objetivos de la evaluación de Riesgos

El objetivo es poder analizas los diferentes tipos de riesgos y relacionarlos con los cuales pueden causarle daños a la empresa. Mediante esto tendremos los datos suficientes para poder realizar un plan que disminuya la posibilidad de que ocurra.

3.3 Evaluación de Riesgos

En esta etapa se analizan los riesgos presentes en el entorno, para determinar que riesgos se pueden mitigar, cuales se pueden transferir y cuales se deben asumir.

No es posible eliminar todos los riesgos sino que se pueden mitigar (empleando medidas para reducirlos), transferir (cede su responsabilidad a otra persona) o asumir (cuando se decide correr el riesgo con sus posibles consecuencias).

Sin embargo, siempre existen riesgos remanentes y desconocidos.

Es más, constantemente surgen nuevos riesgos a medida que la tecnología avanza y los sistemas cambian. Los entornos informatizados suelen acompañar estos cambios adaptándose a los requerimientos tecnológicos del momento. Es por eso que surgen nuevos riesgos día a día.

Los riesgos pueden ser:

- Tecnológicos: si tienen origen o afectan aspectos técnicos del entorno (como deterioro de equipamientos, falta de disponibilidad de recursos, etc.).

- Funcionales: si tienen origen o afectan aspectos funcionales del entorno (como posible descubrimiento de información por la existencia de usuarios con contraseña por default, o el acceso no autorizado a los recursos por una pobre autenticación de usuarios).

Todos los entornos están expuestos a amenazas. Todos los entornos tienen vulnerabilidades, algunas conocidas, otras no, pero están presentes, esperando ser usadas por un atacante para penetrar las barreras de seguridad y apoderarse de información, denegar servicios, o provocar toda clase de daño.

No importa la plataforma tecnológica, no importa la marca de software que se usa. Tampoco importa la infraestructura edilicia, los equipos, el cableado. Siempre existen riesgos.

Existe una relación entre tipo de desastre y sus efectos, y su probabilidad de ocurrencia. Los riesgos reales y potenciales son variables en el tiempo y en el lugar.

3.4 Evaluación de riesgos de la empresa
3.4.1 Identificación de activos

Recursos Críticos

1) Servidores
2) Computadoras
3) Base de Datos
4) Personal
5) Backups Almacenados

3.4.2 Identificación de las amenazas y Vulnerabilidades

Matriz de Amenazas

Amenazas	Probabilidad
Virus	4
Hackers	4
Falla Eléctrica	2
Huracanes	1
Incendios	2
Sismos	1
Vandalismo	3

Matriz de Vulnerabilidades

Vulnerabilidades	Probabilidad
Ubicación inadecuada	1
Espacio insuficiente	2
Cableado defectuoso	2
Password inseguros	3
Falta de Actualizaciones	3
Falta de equipos de seguridad	3
Falta de Protección a los sistemas	3

3.4.3 Calculo del Riesgo

Matriz de Priorizacion Riesgos TI						
Activo	Amenazas	Vulnerabilidades	Impacto Economico	Probabilidad de Ocurrencia	Medicion del Riesgo	Priorizacion
Base de datos	Personal no Autorizado	Falta de proteccion en las areas	3	1	3	Alta
	Virus	Antivirus Desactualizado				
Computadoras	Virus	Antivirus Desactualizado	1	3	2	Media
	Falla Electrica	Falta de capacidad en planta electrica				
	Vandalismo	Personal Desmotivado				
Servidores	Falla Electrica	Falta de capacidad en planta electrica	3	1	3	Alta
	Virus	Antivirus Desactualizado				
	Hackers	Sistemas Desactualizados				
Redes	Hackers	Redes desprotegidas	2	3	3	Alta
	Desconeccion	Mala estructura				

Leyenda: 1= Baja 2= Media 3= Alta

Capítulo IV

Análisis de Impacto de la Empresa

CAPITULO IV
ANÁLISIS DE IMPACTO DE LA EMPRESA

4.1 Propósito del Análisis de Impacto (BIA)

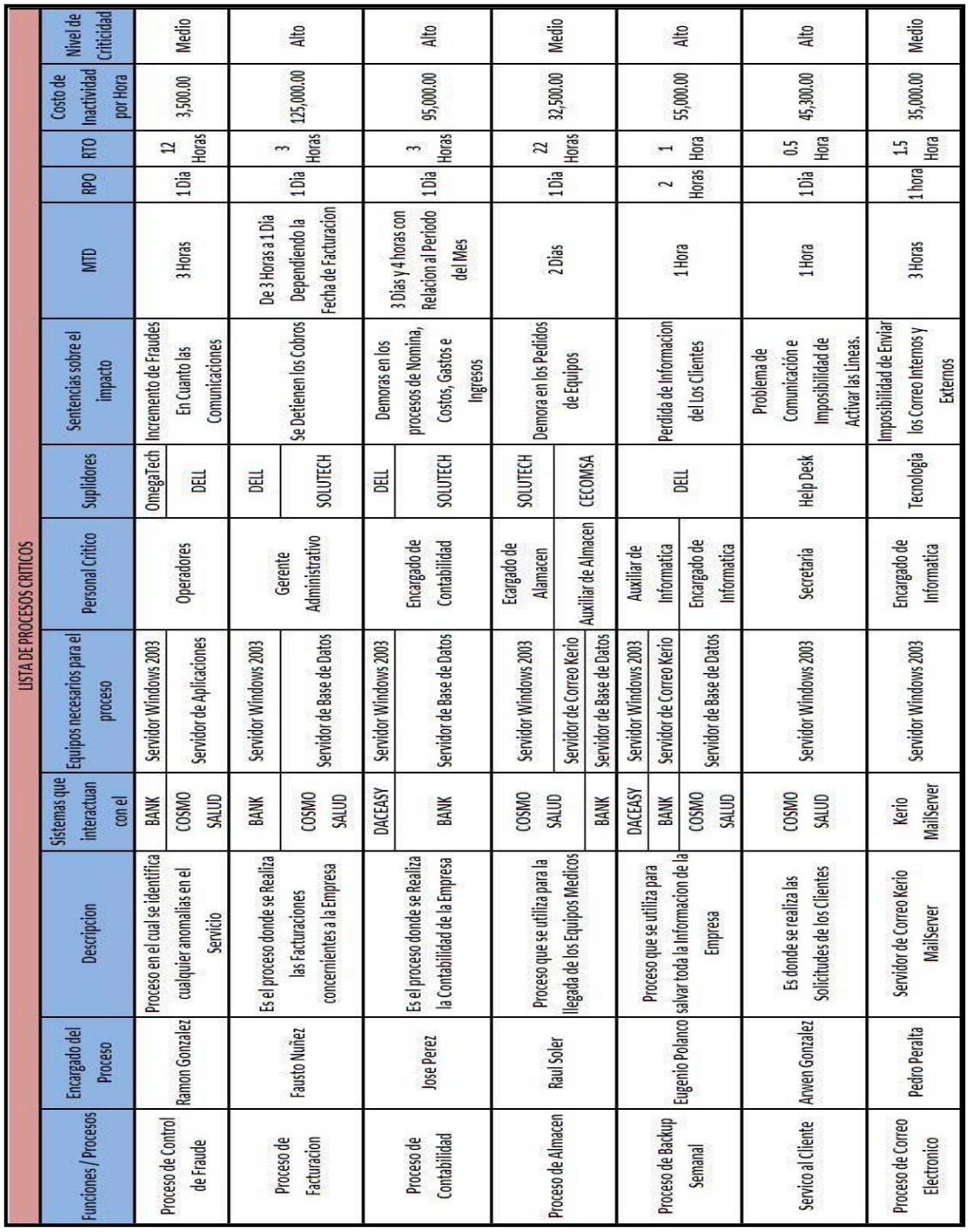
Esta fase ayuda a reconocer qué procesos son los que deben mantenerse activos ante cualquier eventualidad y les da prioridad ante la contingencia.

El análisis del impacto al negocio BIA es un paso crítico para desarrollar el plan de continuidad del negocio. Esta etapa implica identificar los diversos eventos que podrían tener un impacto sobre la continuidad de las operaciones y su impacto financiero, legal y de reputación sobre la organización.

Para ejecutar esta etapa con éxito, se debe lograr un entendimiento de la organización, de los procesos claves del negocio y los recursos de SI (Sistemas de Información) utilizados para soportarlos. Esta etapa requiere un elevado nivel de soporte por parte de la alta gerencia y la total participación del personal tanto de Tecnología de la Información (TI) como de los usuarios finales.

Se debe establecer la criticidad de los recursos de información (por ejemplo, aplicaciones, datos, redes, software de sistema, instalaciones, etc.) que dan soporte a los procesos críticos del negocio de una organización con la aprobación de la alta gerencia. Es importante incluir todos los tipos de recursos de información y mirar más allá de los tradicionales para que se puedan incluir en la planeación de la continuidad del negocio.

4.2 Identificación de los Procesos Críticos



LISTA DE PROCESOS CRITICOS												
Funciones / Procesos	Encargado del Proceso	Descripcion	Sistemas que interactuan con el	Equipos necesarios para el proceso	Personal Critico	Suplidores	Sentencias sobre el impacto	MTD	RPO	RTO	Costo de Inactividad por Hora	Nivel de Criticidad
Proceso de Control de Fraude	Ramon Gonzalez	Proceso en el cual se identifica cualquier anomalias en el Servicio	BANK	Servidor Windows 2003	Operadores	OmegaTech	Incremento de Fraudes	3 Horas	1 Dia	12 Horas	3,500.00	Medio
			COSMO SALUD	Servidor de Aplicaciones		DELL	En Cuanto las Comunicaciones					
Proceso de Facturacion	Fausto Nuñez	Es el proceso donde se Realiza las Facturaciones concernientes a la Empresa	BANK	Servidor Windows 2003	Gerente Administrativo	DELL	Se Detienen los Cobros	De 3 Horas a 1 Dia Dependiendo la Fecha de Facturacion	1 Dia	3 Horas	125,000.00	Alto
			COSMO SALUD	Servidor de Base de Datos		SOLUTECH						
Proceso de Contabilidad	Jose Perez	Es el proceso donde se Realiza la Contabilidad de la Empresa	DACEASY	Servidor Windows 2003	Encargado de Contabilidad	DELL	Demoras en los procesos de Nomina, Costos, Gastos e Ingresos	3 Dias y 4 horas con Relacion al Periodo del Mes	1 Dia	3 Horas	95,000.00	Alto
			BANK	Servidor de Base de Datos		SOLUTECH						
Proceso de Almacen	Raul Soler	Proceso que se utiliza para la llegada de los Equipos Medicos	COSMO SALUD	Servidor Windows 2003	Ecargado de Alamacen	SOLUTECH	Demora en los Pedidos de Equipos	2 Dias	1 Dia	22 Horas	32,500.00	Medio
				Servidor de Correo Kerio	Auxiliar de Almacen	CECOMSA						
			BANK	Servidor de Base de Datos								
Proceso de Backup Semanal	Eugenio Polanco	Proceso que se utiliza para salvar toda la Informacion de la Empresa	DACEASY	Servidor Windows 2003	Auxiliar de Informatica	DELL	Perdida de Informacion del Los Clientes	1 Hora	2 Horas	1 Hora	55,000.00	Alto
			BANK	Servidor de Correo Kerio	Encargado de Informatica							
			COSMO SALUD	Servidor de Base de Datos								
Servico al Cliente	Arwen Gonzalez	Es donde se realiza las Solicitudes de los Clientes	COSMO SALUD	Servidor Windows 2003	Secretaria	Help Desk	Problema de Comunicación e Imposibilidad de Activar las Lineas.	1 Hora	1 Dia	0.5 Hora	45,300.00	Alto
Proceso de Correo Electronico	Pedro Peralta	Servidor de Correo Kerio MailServer	Kerio MailServer	Servidor Windows 2003	Encargado de Informatica	Tecnologia	Imposibilidad de Enviar los Correo Internos y Externos	3 Horas	1 hora	1.5 Hora	35,000.00	Medio

Entrevista sobre el análisis de impacto ver Anexo No.2

4.4 Identificación de los Recursos Críticos

1. Computadoras
2. Servidores
3. Base de Datos
4. Personal
5. Backups Almacenados

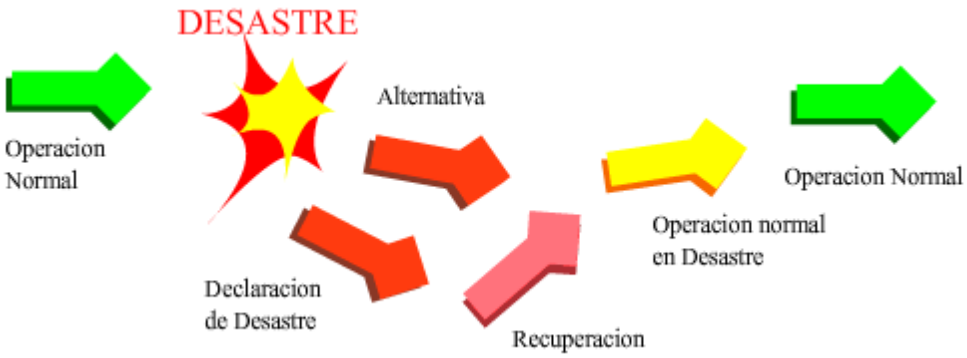
4.5 Matriz Sistemas Críticos

MATRIZ DE SISTEMA CRITICO	
DEPARTAMENTO	SISTEMA CRITICO
DEPARTAMENTO DE CONTABILIDAD	Bank (Sistema de Cobros)
	Sistema de Nomina
	Cosmo Salud
	DacEasy (Sistema de Contabilidad)
DEPARTAMENTO TI	Isa server (Servidor de Internet)
	Kerio Mail Server (Servidor de Correo)
DEPARTAMENTO DE ALMACEN	Sistema de Alamacen
	Sistema de Llegada de Productos

Capítulo V
Desarrollo de Estrategias

CAPITULO V
DESARROLLO DE ESTRATEGIAS

5.1 Escenario del Plan de contingencia



5.1.1 Operación Normal

Es la operatoria que se registraba antes de ocurrir el desastre. Asimismo, define las condiciones que se deben alcanzar como objetivo final mediante la ejecución del plan de recuperación ante desastres.

5.1.2 Alternativa

Mientras se trabaja en la recuperación de las prestaciones afectadas por la contingencia, los usuarios deberán utilizar una operatoria alternativa, constituida fundamentalmente por procesos manuales, durante la cual se genera información.

5.1.3 Operación en desastre

Mediante la ejecución de los procedimientos se llega a esta instancia en la cual todos los servicios y aplicaciones han sido recuperados, pero no se encuentran ejecutando en su lugar original o bajo las mismas condiciones en que se encontraban originalmente.

El tiempo desde la declaración de la emergencia hasta que se alcanza la operación normal en desastre no debe ser superior a los tiempos máximos tolerables de suspensión definido para cada una de las prestaciones.

5.1.4 Operación Normal Restablecida

Mediante la ejecución de los procedimientos se alcanza esta última instancia, en la cual todos los servicios y aplicaciones se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaba antes de la contingencia. Para alcanzar este tipo de operaciones, es posible que haya que considerar una suspensión programada de alcance total o parcial de las prestaciones, para lo cual es necesario acotar el tiempo de interrupción al mínimo indispensable, y que preferentemente sea imperceptible por los usuarios.

5.2 CheckList del Desarrollo de las Estrategias

Falla Eléctrica

En caso de una falla eléctrica que afecte directamente al centro de cómputos principal (servidores, dispositivos de Red), el centro de cómputos contara con un sistema redundante en alimentación, distribución, transformación, NO-BREAK'S y Plantas de emergencia. Además el centro de cómputos será independiente del sistema de alimentación del resto de las instalaciones.

Checklist No.1

#	Acción	Responsable
1	Fecha y hora de la interrupción	CEMADOJA/ Eugenio Polanco
2	Verificar que el sistema redundante se haya activado de inmediato y sin problemas	
3	Activación de la planta de emergencia	
4	Verificar que los servidores principales sigan funcionando correctamente	CEMADOJA/ Jorge Cespedes
5	Verificar el funcionamiento de los dispositivos de red LAN y WAN	
6	Verificar la conexión con los demás departamentos ubicados en la organización	
7	Documentar el problema	

Falla del Servidor Windows 2003

En caso de que el servidor Windows 2003, el cual sostiene el sistema BANK Y COSMO SALUD falle, la empresa contara con un hot site que se actualiza de forma general cada 24 horas y de manera diferencial cada 1 hora (se restaura una copia de la base de datos del sistema solo con los cambios que han transcurrido durante una hora).

Checklist No.2

#	Acción	Responsable
1	Fecha y hora de la interrupción	CEMADOJA/ Socrates Martínez
2	Sacar de línea el servidor averiado	
3	Switching al servidor de Base de Datos y Windows 2003 en el hot site	
4	Verificar que se haya restaurado el último backup diferencial de la base de datos	CEMADOJA/ Eugenio Polanco
5	Verificar que el sistema BANK y COSMO SALUD se está ejecutando correctamente en el hot site	
6	Poner en línea servidor de Base de Datos del hot site	
7	Verificar la disponibilidad de la red LAN y WAN	CEMADOJA/ Juan Francisco García
8	Detectar y corregir el problema en el servidor de Base de Datos local	
9	Poner en marcha el servidor local y restaurar el backup general y el último backup diferencial realizado en el servidor del hot site	
10	Switching al servidor local	
11	Verificar la disponibilidad de la red LAN y WAN	
12	Verificar los enlaces con cada departamento de la organización	
13	Documentar el Problema	CEMADOJA/ Edwin Pérez

Falla de Servidor de Correo Kerio Mail Server

En caso de que el servidor de Correo Kerio Mail Server (correo electrónico) falle, la empresa contara con un servicio de correo electrónico en línea bajo el dominio **cemadoja.net**. Todos las cuentas de correo electrónico local de **cemadoja.com** están replicadas en el servidor de correo electrónico en línea y cada estación de trabajo tiene la capacidad de enviar correos utilizando ambas direcciones, obviamente la dirección predeterminada es cemadoja.com. Un backup general de las configuraciones y cuentas de correo local será realizado todas las semanas.

Checklist No.3

#	Acción	Responsable
1	Fecha & hora de la interrupción	CEMADOJA/ Socrates Martínez
2	Sacar de línea el servidor averiado	
3	Notificar a todos los usuarios que deben configurar cemadoja.net como el servidor de correo predeterminado y que deben enviar todos sus correos a través de este servidor	
4	Detectar y corregir el problema en el servidor Kerio Mail Server	
5	Poner en marcha el servidor de correo Kerio Mail Server y de ser necesario, restaurar el último backup de la configuración de correo electrónico de la empresa y todas las cuentas de usuarios	
6	Notificar a todos los usuarios que el servidor de correo Kerio Mail Server está arriba y que utilicen erdosa.com como el servidor de correo predeterminado.	
7	Documentar el problema	CEMADOJA/ Edwin Pérez

Falla en el Servidor de Base de Datos

La base de datos del sistema Bank y Cosmo Salud contara con la generación de un backup total diariamente y un backup diferencial cada una hora (se guardan solos los cambios transcurridos durante esa hora en un archivo de backup independiente). De esta forma, si la base de datos falla, se corrompe, entra en estado “suspect” o se produce una falla eléctrica que ocasiona perdida de datos, se procederá a restaurar el backup general diario, seguido de los backups diferenciales que se han generado en el transcurso del día y lo máximo que se perdería seria una hora de datos.

Checklist No.4

#	Acción	Responsable
1	Sacar de línea el servidor Widnows 2003 durante el máximo MTD	CEMADOJA/ Edwin Grullón
2	Bajar los servicios del gestor de base de datos	
3	Ejecutar las rutinas de reparación de los archivos de base de datos corruptos	
4	Si la base de datos no pudo ser reparada, proceder a restaurar los backups general y diferenciales	
5	Subir los servicios del gestor	
6	Realizar consultas menores a la base de datos y determinar el volumen de pérdida de datos	
7	Poner en línea el servidor Windows 2003 y verificar los enlaces correspondientes	
8	Documentar el problema	CEMADOJA/ Edwin Pérez

Inundaciones Parciales y Totales

Inundación Parcial		
#	Accion	Responsable
1	Verificar que ningún equipo este afectado	CEMADOJA / Socrates Martinez
2	Si hay algún equipo afectado, realizar el cambio del mismo	
3	Contactar el equipo de limpieza para limpiar el área afectada	
4	Documentar el incidente	CEMADOJA / Edwin Perez

Inundación Total		
#	Acción	Responsable
1	Se desconectara de la energía del Cuarto de Equipos	CEMADOJA / Socrates Martinez
2	Se enruteará el trafico para el HotSite	
3	Contactar el equipo de limpieza para limpiar el área	
4	Verificar los equipos que estén afectados para realizar el cambio de estos	
5	Restaurar la energía	
6	Verificar el Correo electrónico	
7	Restaurar el Backup del HotSite	CEMADOJA / Francisco Garcia
8	Verificar la disponibilidad de la Red LAN/WAN	
9	Verificar el funcionamiento de los equipos	
10	Verificar las aplicaciones COSMO Y BANK	CEMADOJA / Eugenio Polanco
11	Restaurar las operaciones normales en el site principal	
12	Documentar el incidente	CEMADOJA / Edwin Perez

Situación de Incendios

Fuego		
#	Accion	Responsable
1	Se desconectara de la energía del Cuarto de Equipos	CEMADOJA / Socrates Martinez
2	Se enruteará el trafico para el HotSite	
3	Contactar el equipo de limpieza para limpiar el área	

4	Verificar los equipos que estén afectados para realizar el cambio de estos	
5	Se repara la causa del incendio	
6	Restaurar la energía	
7	Restaurar el Backup del HotSite	
8	Verificar el Correo electrónico	
9	Verificar la disponibilidad de la Red LAN/WAN	CEMADOJA / Francisco Garcia
10	Verificar el funcionamiento de los equipos	
11	Verificar las aplicaciones COSMO Y BANK	CEMADOJA / Eugenio Polanco
12	Restaurar las operaciones normales en el site principal	
13	Documentar el incidente	CEMADOJA / Edwin Perez

- **Detección de Virus en los Procesos**

Virus		
#	Accion	Responsable
1	Desconectar de la red el área afectada	CEMADOJA / Socrates Martinez
2	Enrutar el trafico al HotSite	
3	Comprobar ultimas actualizaciones del antivirus	
4	Buscar información sobre el virus	
5	Proceder con los pasos encontrados de eliminar el virus	
6	Verificar todos los equipos para comprobar que el virus no se haya propagado	
7	Notificar del evento a todos los usuarios para que reporten cualquier anomalía	
8	Restaurar las operaciones en el site principal	
9	Documentar incidente	CEMADOJA / Edwin Perez

- **Manipulación de Datos mediante un Hacker**

Hacker		
#	Accion	Responsable
1	Cambiar la configuración en el Router para bloquear la IP del Atacante	CEMADOJA / Socrates Martinez
2	Verificar en los logs del sistema para comprobar como se ha introducido	
3	Corregir las vulnerabilidades que ha utilizado el intruso	
4	Comprobar la integridad de los datos	
5	Contactar a codetel para informar lo ocurrido y proveerles la información del hacker	
6	Documentar el incidente	CEMADOJA / Edwin Perez

Desastre Total

Desastre total no espesificado		
#	Accion	Responsable
1	Verificar el tiempo en restaurar el site principal	CEMADOJA / Socrates Martinez
2	Si no se podrá restaurar de inmediato, enrutar el trafico al HotSite	
3	Reparar equipos afectados	
4	Verificar el Correo electrónico	
5	Verificar la disponibilidad de la red	CEMADOJA / Francisco Garcia
6	Verificar el Funcionamiento de las aplicaciones COSMO Y BANK	CEMADOJA / Eugenio Polanco
7	Restaurar las operaciones en el site principal	
8	Documentar el incidente	CEMADOJA / Edwin Perez

Capítulo VI
Desarrollo del Plan de Recuperación de Desastres

CAPITULO VI
DESARROLLO DEL PLAN DE RECUPERACIÓN DE DESASTRES

6.1 Objetivos del Proyecto:

- Preparar un Plan de recuperación ante desastres para mantener la existencia de CEMADOJA ante cualquier situación que la ponga en peligro.
- Mantener los activos de la empresa.
- Reducir el riesgo de pérdida de datos, daños de hardware, daños de software, etc.

6.1.1 Objetivos Generales

Con este plan de recuperación ante desastres, se desea proteger la empresa ante cualquier evento que pueda poner en peligro su existencia.

Poder también mantener los activos ante cualquier riesgo que pueda causar la perdida de estos, o lograr reducir al mínimo los costos necesarios para restablecer la empresa.

Establecer los controles que puedan evitar las fallas o pérdidas de información en los diferentes sistemas.

Que todo el personal tenga conciencia de cuál será su función ante cualquier evento que pueda poner en peligro la empresa

6.1.2 Específicos

- Proteger los datos ante cualquier virus, spyware o alguna otra amenaza, para poder mantener la integridad de la información a la hora del backup.
- Almacenar los backup en lugares de condiciones óptimas para su preservación y posterior uso en caso de desastres.
- Establecer seguridad física y lógica de cada una de las estaciones de trabajo, teniendo el debido control para su protección.
- Evaluar las estructuras y los espacios donde están guardados los equipos y el servidor.

6.2 Plan de Acción

Los encargados del Plan de Contingencia declararan la emergencia y contactarán al Consejo Directivo para activar el Plan de Recuperación de Desastre

6.3 Las 4 Fases del Plan de Recuperación

Respuesta:

Procesos a realizar	Inundaciones	Incendio	Falla Eléctrica
Presencia inmediata en el lugar de incidentes	⊗	⊗	⊗
Llamar a las personas responsables	⊗	⊗	⊗
Activar el plan de emergencia	⊗	⊗	⊗

Llamar a los bomberos o Defensa Civil	⊗	⊗	⊗
Activar centro de computo alterno (Redundante)	⊗	⊗	⊗
Detectar la persona responsable del error	⊗	⊗	⊗
Verificar las operaciones en cada sucursal	⊗	⊗	⊗

Reanudación:

Procesos a realizar	Inundaciones	Incendio	Falla Eléctrica
Verificar la magnitud del incidente	⊗	⊗	⊗
Activar alarma	⊗	⊗	⊗
Evacuar personas	⊗	⊗	⊗
Investigación del personal del área	⊗	⊗	⊗
Asegurar las áreas tanto internas como externas	⊗	⊗	⊗

Recuperación:

Procesos a realizar	Inundaciones	Incendio	Falla Eléctrica
Reordenar el Centro de Cómputos	⊗	⊗	⊗
Llamar a los proveedores de servicios	⊗	⊗	⊗
Evaluar los daños ocasionados			
Reemplazar los equipos afectados	⊗	⊗	⊗
Activar fuentes de energía de respaldo	⊗	⊗	⊗
Restauración del Centro alterno	⊗	⊗	⊗
Utilizar estrategias de recuperación	⊗	⊗	⊗

Restauración:

Procesos a realizar	Inundaciones	Incendio	Falla Eléctrica
Tomar el Backup	⊗	⊗	⊗
Contactar al encargado de TI	⊗	⊗	⊗
Llamar a el transporte encargado de mover los equipos	⊗	⊗	⊗

Capitulo VII
Plan de Mantenimiento y Pruebas

CAPITULO VII
PLAN DE MANTENIMIENTO Y PRUEBAS

Una de las últimas etapas son las pruebas. El plan debe dar probado en su totalidad al menos una vez al año, según las mejores prácticas y regulaciones internacionales, y probado parcialmente en distintas oportunidades para obtener mejoras y poder dar una revisión, que contribuyan al mantenimiento vigente del plan a lo largo del tiempo y garanticen la recuperación de las prestaciones en un futuro. A continuación le presentaremos los simulacros en cuanto el plan de Mantenimientos y Pruebas, mas el cuadro de prueba de plan que se encuentra en el **Anexo No. 4** del proyecto.

7.1 Simulacros

7.1.1 El programa de simulacros anunciados.

Una vez al año los días 12 de noviembre se efectuará un simulacro anunciado para poner en práctica el plan en el lugar alterno. Estas actividades se llevarán a cabo en el horario determinado en el acuerdo entre la CEMADOJA y el lugar alterno. Los directores de cada una de las oficinas mencionadas serán responsables de lograr que un representante idóneo participe en el simulacro.

7.1.2 El programa de simulacros no anunciados.

Una vez al año se efectuará un simulacro de desastre que se anuncia por la mañana del día en que se va a efectuar. Los Coordinadores de Contingencias y de Emergencias de CEMADOJA serán responsables de determinará al fecha de

los simulacros (anunciado y no anunciado); velar por su ejecución y que se tomen medidas correctivas para los problemas que se detecten en ellos. Estas actividades también se llevarán a cabo en el horario determinado en el acuerdo entre la CEMADOJA y el lugar alterno.

Capítulo VIII
Plan De Comunicación Ante Crisis

CAPITULO VIII
PLAN DE COMUNICACIÓN ANTE CRISIS

La crisis es una serie de acontecimientos, que afecta de forma diversa a la integridad del producto, la reputación o a la estabilidad financiera de la empresa; o a la salud y bienestar de los trabajadores, o del público en general.

No todas las crisis tienen orígenes similares y, por tanto, cada una tiene una forma diferente de manejarlas.

Para enfrentar una crisis, una empresa debe contar con un "comité", en el que se integra la alta dirección y los responsables de diversas áreas, dependiendo del tipo de empresa que se trate: legal, producción, finanzas, logística, recursos humanos y, por supuesto, comunicación.

Las empresas se enfrentan con algunas dificultades que pueden originar crisis internas muy graves, pero con menor notoriedad en el exterior. Otras pueden tener un alcance muy importante en la opinión pública, aunque puedan no tener un impacto directo en el negocio de la compañía.

8. 1 Cómo actuar frente a una crisis

Las compañías deben tener un manual de crisis en el que se establecen las metodologías para manejar situaciones inmediatamente después de ocurrido un desastre.

Responsabilidades de un Encargado ante Crisis:

1. Reunir toda la información posible.
2. Evitar los vacíos de información comunicando lo antes posible.
3. No apresurarse a comunicar por la presión de los periodistas u otros grupos.
4. Determinar el formato de la comunicación.
5. Establecer un mecanismo de monitoreo inmediato en todos los medios para comprobar el alcance de la crisis.
6. Determinar la secuencia y la coherencia de la comunicación, en caso de que se trate de una crisis con extensión en el tiempo.
7. Aconsejar sobre la política de la compañía en cuanto a rumores e imprecisiones aparecidos en los medios de comunicación.

Los encargados de comunicar la crisis deben estar preparados en el momento de actuar ante una crisis.

Aunque haya una infinidad de variables de riesgo, es posible prepararse para enfrentarse a posibles crisis y, de esta manera, lograr sobrellevarla con más posibilidades de éxito.

Capitulo IX
Programas de Concientización, Capacitación y Difusión del Plan.

CAPITULO IX
PROGRAMAS DE CONCIENTIZACIÓN, CAPACITACIÓN Y DIFUSIÓN DEL PLAN.

La tecnología facilita el desarrollo de las actividades en la empresa, pero las personas y los procesos son esenciales para reducir exitosamente los riesgos. Asegurar que las personas estén conscientes de los riesgos, tengan la capacidad de identificar los problemas y estén debidamente entrenadas para responder a los diversos retos, es primordial para el exitoso desempeño del Plan de Recuperación de Desastres.

Debido a la necesidad de contar con empleados preparados para actuar en eventualidades que se presenten en nuestro centro de trabajo, hemos elaborado un programa de capacitación sobre seguridad y protección, para que cualquier trabajador sepa que hacer en caso de emergencia.

El objetivo de este programa es concienciar a los empleados y directivas de CEMADOJA, sobre el hecho de que los desastres e interrupciones imprevistas ocurren. También lograr una cultura en el personal de la empresa a través de actividades que involucren la participación activa de cada departamento. (Ver programa en anexos No. 3 del Plan).

Recomendaciones

RECOMENDACIONES

Toda organización debe estar preparada ante cualquier impacto dentro de una situación inusual que se le pueda presentar, por lo que se le recomienda elaborar un Plan de Recuperación ante Desastres (DRP) que le permita mantener de forma normal el funcionamiento de todas sus operaciones.

Toda organización debe de tener en la estructura un plan de Recuperación Las instituciones deben de tener en sus estructuras un Plan de Recuperación ante Desastre, en el que este seria evaluado periódicamente para su mejor rendimiento o cambios convenientes.

Cada institución debe tener una unidad de seguridad que se encargue de efectuar y velar este Plan, de una forma adecuada en todas las áreas de la institución para que el Plan sea válido en cada funcionamiento de los procesos de la misma.

Y por último que esto nunca se queda es de instruir cada personal de la organización sobre la existencia de este plan y tomar las medidas preventivas en caso de cualquier situación de amenaza o riesgo que se pueda presentar.

Conclusión

CONCLUSIÓN

Los planes de contingencia para una empresa muestran un nivel de competitividad por su alto rendimiento en la eficiencia administrativa, lo cual concentra en la recuperación de eventos únicos que producen una interrupción prolongada de los servicios que puedan ofrecer dichas organizaciones.

En la Actualidad las infraestructuras del edificio y del Departamento de TI se encuentran en un estado de remodelación y cambios de equipos, pero con las medidas debidamente tomadas en el plan de recuperación ante desastre se pueden obtener resultados favorables y a su vez exitosos.

Se espera que este proyecto satisfaga los propósitos y expectativas creadas, y que sea a la vez un gran aporte de conocimientos para la Universidad, y para el Centro de Imágenes CEMADOJA, y para todas las personas que deseen enriquecer sus conocimientos con respecto a un plan como este pues le puede sacar el mayor provecho.

Bibliografía

BIBLIOGRAFÍA

- **Administración Profesional de Proyectos LA GUIA, Autor:** Yamal Chamoun, Editora McGraw Hill.
- **Enciclopedia Interactiva de los Conocimientos**, **Editora:** MM Océano Grupo Editorial, S. A.
- **Glosario de Términos Informáticos, Autor:** Guido J. Pace, año 2003.
- **Diccionario Pequeño Larousse**, Edición 2005.
- **Análisis y Diseño de Sistemas de Información**, Tercera Edición, **Autores:** Jeffrey L Whitten, Lonnie D. Bentley, Víctor M. Barlow.
- **Manual de Preparación CISA 2008**, impreso en los Estados Unidos de América.

Internet

- www.ongei.gob.pe/seguridad/seguridad2_archivos/Lib5131/Libro.pdf
- personal2.iddeo.es/alcazaba/normas/planseguridadinformatico.pdf
- www.hacienda.go.cr/centro/datos/Articulo/Plan%20de%20Contingencia.doc
- http://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres_(inform%C3%A1tica)Poner la fuente
- Htttp://www.comunidadbcm.com
- http://www.bdaglobal.com/es/services/continuity.php
- http://www.monografias.com/trabajos14/recursos-humanos/recursos-humanos.shtml

Anexos

UNIVERSIDAD APEC
Fundada en 1965

Decanato de Informática
Facultad de Humanidades y Ciencias.

Implementación del plan de contingencia ante desastre para la continuidad de los sistemas automatizados en el periodo mayo-agosto 2009 del Centro de Estudio de Imágenes CEMADOJA.

Sustentantes:

Luis Ricardo Rodríguez Cuesta	**2002-0359**
Eugenio Polanco Berroa	**2003-1483**
Silvano Saúl Estévez Gómez	**2004-0155**

Módulo:
Continuidad de Negocios

Asesores:
Ing. Jacqueline J. Vega
Ing. Ramón Gómez

Anteproyecto de la monografía para optar por el título de Ingeniero en Sistemas Computacionales.

Distrito Nacional, República Dominicana
2009

I. Selección del Tema

Implementación del plan de contingencia ante desastre para la continuidad de los sistemas automatizados en el periodo mayo-agosto 2009 del centro de estudio de imágenes CEMADOJA.

II. Definición del Tema

En este proyecto realizaremos un plan de contingencia con la finalidad de asegurar que los sistemas informáticos de la empresa continúen su funcionamiento ante cualquier posible desastre que pueda ocurrir. Los datos son una parte importante en la empresa y también está contemplada la recuperación de estos a la mayor brevedad.

III. Planteamiento del Problema

Uno de los recursos más importantes hoy en día en una empresa son sus sistemas informáticos, de tal manera que cualquier daño a este causaría grandes pérdidas incalculables de dinero. Sin embargo existen situaciones que no siempre pueden ser controladas ni ser evitadas a tiempo como los desastres naturales o los causados por el hombre.

Para prevenir que los mismos afecten la empresa, es de gran importancia implementar un plan de contingencia con las medidas necesarias para la continuidad de la empresa.

IV. Objetivos Generales

El objetivo general de este proyecto es de proveer de un plan adecuado para reducir riesgos por fallas o mal funcionamiento de los elementos que conforman un sistema de información, y así garantizar la continuidad de la empresa y sus activos mediante un buen plan de contingencia.

4.1 Objetivos Específicos

- Asegurar la Estabilidad de la Empresa
- Proteger los activos de la empresa de riesgos, desastres naturales y robo de los mismos.
- Reducir al mínimo las probabilidades de pérdidas a un costo razonable y asegurar la pronta recuperación.
- Informarle a todo el personal de la empresa los procedimientos a seguir en caso de cualquier riesgo o desastre que ocurra en la empresa.
- Identificar las estrategias para la continuidad de los sistemas automatizados de la empresa.
- Proveer un manejo centralizado del plan ante cualquier desastre.

V. Justificación de la Investigación

5.1 Justificación Teórica

Implementar un plan de contingencia es de mucha importancia para la empresa, debido a que con este se asegura que la institución siga en funcionamiento ante cualquier situación.

Este trabajo de grado le proporcionara a CEMADOJA una visión de las vulnerabilidades que tienen ante cualquier posible amenaza y como estar preparados ante estas. Proporcionándoles una forma de enfrentarlas y mantener en todo momento la integridad de la información.

5.2 Justificación Metodológica

El plan de contingencia contara con las diferentes prácticas que se deben poner en funcionamiento para garantizar la continuidad de los sistemas de información. Ese cuenta con los procesos que hay que seguir, las medidas a tomar, la capacitación del personal, entre otros.

Al estar establecido los pasos a tomar ante cualquier situación que le pueda causar un daño a la empresa, no se perderá tiempo en especulación y se tomaran de inmediato las acciones que con anticipación se analizaron como soluciones. Permitiendo que los ojos del cliente no perciban las dificultadas que se puedan presentar.

5.3 Justificación Practica

Al haber realizado previamente un análisis de los procesos actuales en CEMADOJA, hemos visto la existencia de mucho puntos débiles y podemos garantizar que con las herramientas necesarias y la disposición del personal, estos pueden ser cubiertos.

VI. Tipo de Investigación

Dentro de los Tipos de Investigación que existen hemos elegido las que más se adaptan a nuestra metodología de investigación siendo estas las siguientes:

- Documental
- Explicativa
- Descriptiva

VII. Marcos de Referencia

7.1 Marco Teórico

Hoy en día, la mayoría de las empresas requieren un nivel de disponibilidad más alto y otras incluso necesitan un nivel continuo de disponibilidad, ya que le resulta difícil funcionar sin los Recursos Informáticos.

Un Plan de Contingencia seria para cualquier empresa como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

El Plan de contingencia en el caso particular aplicado en el área de tecnología de la información o en cualquier otro departamento es de sentido relevante aplicarlo para el beneficio de la organización completa.

7.2 Marco Conceptual

7.2.1 Plan de Continuidad del Negocio

Un BCP es el resultado de la aplicación de una metodología interdisciplinaria, llamada Cultura BCM, usada para crear y validar planes logísticos para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción o desastre. Estos planes son llamados Planes de Continuidad del Negocio. El plan logístico que se denomina un Plan de Continuidad de Negocios.

7.2.2 Riesgo

Riesgo es la contingencia de un daño. A su vez contingencia significa que el daño en cualquier momento puede materializarse o no hacerlo nunca. Cualquier cosa que pueda provocar daños, cualquier tipo de daño, es un riesgo.

7.2.3 Desastre

Es un hecho natural o provocado por el hombre que afecta negativamente a la vida, al sustento o industria desembocando con frecuencia en cambios permanentes en las sociedades humanas, ecosistemas y medio ambiente. Los desastres ponen de manifiesto la vulnerabilidad del equilibrio necesario para sobrevivir y prosperar.

7.2.4 Amenaza

Riesgo es la contingencia de un daño. A su vez contingencia significa que el daño en cualquier momento puede materializarse o no hacerlo nunca.

7.2.5 Contingencia

Son los procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir el normal funcionamiento de esta, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo de la misma.

7.2.6 Seguridad Informática

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

7.2.7 Backup

son un proceso que se utiliza para salvar toda la información, es decir, un usuario, quiere guardar toda la información, o parte de la información, de la que dispone en el PC hasta este momento, realizará una copia de seguridad de tal manera, que lo almacenará en algún medio de almacenamiento tecnológicamente disponible hasta el momento como por ejemplo cinta, DVD, BluRay, en discos virtuales que proporciona Internet o simplemente en otro Disco Duro, para posteriormente si pierde la información, poder restaurar el sistema.

7.3 Marco Espacial

Esta propuesta está delimitada a la Empresa CEMADOJA, Centro de Estudio de Imágenes. Con el Objetivo de realizar un plan de contingencia que le permita el seguimiento de los procesos de los sistemas automatizados de la misma.

7.4 Marco Temporal

Esta propuesta se trabajara durante el segundo periodo de estudio del 2009, dependiendo en si también del tiempo que se tomen los empresarios de la empresa para su aprobación.

VIII. Métodos, Procedimientos y Técnicas de la Investigación

8.1 Método

Para este proyecto se utilizara como metodología para la investigación el método de observación y análisis. El motivo para utilizar estos métodos es porque los mismos sirven para analizar y determinar el comportamiento de objeto de estudio, para luego así aplicarlo a los procedimientos de la empresa, para su implementación.

8.2 Procedimiento

Para ser posible este proyecto de plan de Contingencia del Centro de Imágenes CEMADOJA, la metodología general de trabajo está orientada a los diferentes sistemas y a los tipos de información utilizados por el laboratorio y las demás operaciones del mismo.

La presente metodología de trabajo permite que el proyecto esté lo suficientemente documentado y manejado para la utilización del mismo.-

8.3 Técnica

Las Técnicas de investigación a utilizar en el proyecto para la realización del plan de contingencia, consiste en la observación de todos los procedimientos internos y externos de la empresa, encuestas y entrevistas al personal de la empresa sobre el funcionamiento de todos los sistemas automatizados y una evaluación de los recursos que dispone la empresa.

IX. Tabla de Contenido

6.3.6 Fuegos

6.3.7 Falla de Electricidad en el Centro de Cómputos

6.3.8 Falla de Electricidad en CEMADOJA

6.4 Desastre Total

7. Plan de Mantenimiento de Pruebas

7.1 Simulacros

7.1.1 El Programa de Simulacros Anunciados

7.1.2 El Programa de Simulacros no Anunciados

7. Programas Concientización, Capacitación y Difusión del Plan

Fuentes de Información

Internet
http://es.wikipedia.org/wiki/copia_de_seguridad
http://es.wikipedia.org/wiki/plan_de_contingencia
http://es.wikipedia.org/wiki/seguridad_de_la_informaci%C3%B3n
http://www.conida.gob.pe/tranparencia/PDF/INFO_GEN/pc.pdf
http://google.com.do
http://monografias.com

Libros

Autor: Juan Gaspar Hernández. Año: 2006. Titulo: Planes de Contingencia. La Continuidad de Negocios en las Organizaciones. Casa Editora: Editorial Díaz de Santos.
Autor: Gregory, Peter. Año: 2008. Titulo: IT Disaster Recovery Planning for Dummies. Casa Editora: Wiley Publishing, Inc.

Autor: Instituto Nacional de Estadística e Informática (IENI). Año: 2001.
Titulo: Guía Práctica para el desarrollo de Planes de Contingencia de Sistema de Información. Casa Editora: Lima, Perú

Anexo 2. Entrevista para la elaboración del Análisis de Impacto (BIA)

CEMADOJA Centro de Educación Médica de Amistad Domínico-Japonesa	Analisis de Impacto de Negocios Fecha de Entrevista: Realizado Por:

El análisis de impacto al negocio tiene como objetivo identificar, cuantificar y calificar el impacto al negocio por pérdida o interrupción de las operaciones y provee la información con base en la cual se determinan las estrategias de recuperación mas apropiadas. La información para la construcción del BIA es suministrada por varios departamentos dentro la organización. El análisis puede proporcionar información sobre el corto y largo plazo de los efectos de un desastre.

Esta información es necesaria para desarrollar una estrategia de continuidad de la empresa. Por favor, rellene el cuestionario, su respuesta sera de mucha importancia para el desarrollo del plan.

CUESTIONARIO DE PROCESOS DE LA EMPRESA

Cargo:_____

Departamento:_____

Función del Departamento:_____

_____

Existen Otros Departamentos que Depende de sus Procesos? Si ☐ No ☐

Departamento:_____

Que Procesos depende de su Departamento:_____

Depende usted de otro departamento para cumplir con sus procesos ? Si ☐ No ☐

Departamento:_____

Que Procesos depende de su Departamento:_____

Durante sus Labores cotidianas, Tiene usted un momento critico del dia ☐ ,semana ☐ ,mes ☐ ,año ☐ de que su proceso debe ser completado? (Marque todas las que apliquen)

Cual es el mas critico de sus procesos:_____

Porque este es el mas critico:_____

Como puede ser producido:_____

Que sistema utliza actualmente?:

Equipos Fisicos (Hardware):

Programas Informaticos (Software):

Cuanto Tiempo puede funcionar su departamento manualmente sin ningun equipo de apoyo?

_____

Cuanto Tiempo puede tardarse en hacerse un impacto critico sobre la organizacion un corte de luz?

2 Hrs ☐ 4Hrs ☐ 8Hrs ☐ 2 a 5 Dias ☐ 6 a 10 Dias ☐

Otras:

Comente sobre este impacto que puede tener:

Como realiza su respaldo del sistema que utiliza:

Cinta ☐ Site Alterno ☐ USB ☐ No Tengo Conocimiento ☐

Otro medio:_____

Frecuencia con que lo Hacen:_____

Donde los Almacenan:_____

Tiempo que toman para la recuperacion de su Respaldo:

Cuantas copias de Seguridad hacen?:_____

Como evita que su sistema sea expuesto por:

Fraudes:_____

Daños causados por terceros:_____

Su departamento como tal ha experimentado un desastre? Si ☐ No ☐

Si su respuesta es afirmativa, de que tipo y como se ha recuperado?_____

_____.

Cual es el objetivo de usted por recuperarlo?_____

_____

_____.

Anexo 3. Programa de Entrenamiento y Capacitación, Cotización y Cultura.

Programa de Entrenamiento y Capacitación

Programa de Entrenamiento y Capacitación							
Taller/Seminario	**Dirigido A**	**Impartido Por**	**Objetivos**	**Duracion**	**Fecha de Inicio/Fin**	**Horario**	**Lugar**
SEMINARIO DE DISASTER RECOVERY PLAN	Gerentes de TI, Administrador de Seguridad, Administrador de Planes de Continuidad de Negocios	Dr. Nashley Estevez	Fundamentalmente comprender la importancia para las organizaciones de poseer un plan de recuperación ante desastres.	2 Dias	11/09/2009 12/09/2009	9:30 am 1:00 pm	Hotel Lina Santo Domingo
Taller de Comunicación de Crisis	Gerentes de Toda la Organización, Area de Seguridad de la Informacion, Miembros de Comité ante Crisis	Ing. Pedro Antonio Gil	1. Promocionar a la empresa tanto interna y externamente para mejorar los servicios de sus empleados y sus clientes. 2. Diseñar y gestionar estrategias ante situaciones de crisis y a la vez adquirir los conocimientos necesarios para elaborar ficheros ante crisis.	4 Dias	15/09/2009 18/09/2009	9:00 am 3:00 pm	Hotel Hitlton Santo Domingo
Planificación ante La Gestión de la Crisis	Todo el Personal	Lic. Cesarina Ortiz	Fundamentalmente utilizar la metodología adecuada para utilizar en medio de un desastre	3 Dias	21/09/2009 23/09/2009	5:00 pm 9:00 pm	Hotel La Hispaniola
Primeros Auxilios	Todo el Personal	Cuerpo de Bomberos de Santo Domingo	Obtener cualquier conocimiento basico que se presente ante una emergencia	3 Dias	25/09/2009 27/09/2009	10:30 am 3:00 pm	Hotel El Embajador
Charla	**Dirigido A**	**Impartido Por**	**Objetivos**	**Duracion**	**Fecha de Inicio/Fin**	**Horario**	**Lugar**
Prevención Contra Incendios	Dirigido a Todo el Personal de la Empresa	Lic. Sugey Palin Cid	Minimizar los Riesgo de Incendio, Como Actuar durante el desastre y saber utilizar los distintos instrumentos que se usan en esa situación	2 Dias	11/09/2009 12/09/2009	9:30 am 1:00 pm	Hotel Jaragua

- **Concientización y Cultura**

Concientización y Cultura			
Actividad	**Dirigido A**	**Objetivos**	**Medio**
Políticas a tomar en Cuenta sobre la Continuidad de la Empresa	Todo el Personal de la Empresa	Que todo el personal de la empresa conozcan y tomen en cuenta las Políticas de Continuidad de la Organización.	* Murales de Informacion *Carteles *Afiches
Señalización en toda la Organización	Todo el Personal de la Empresa	Tener Indicadores para que el personal se concientice en momentos dados	* Murales de Informacion *Carteles *Afiches * Intranet

Anexo 4. Prueba del Plan

Programas de Prueba del Plan					
Que	*Donde*	*Cuando*	*Quien*	*Por Que*	*Como*
Amenazas, Riesgos, Controles	Gerencia General	Cada 1 meses	Departamento de Continuidad	Con Este se mantiene la continuidad de la empresa	A través de lo planteado en el plan de continuidad
Análisis de Impacto (BIA)	Estructura Organizacional Completa	Cada 3 Meses	Departamento de Continuidad y El Encargado de Cada Área de la Empresa	Determinar las Funciones Criticas y Saber que hacer para recuperarla en el mejor tiempo posible	Evaluando en cada Área los Procesos que Podrían Ser Críticos para la empresa
Estrategias	Departamento de Continuidad	Mes Después de Analizar el BIA	Departamento de Continuidad	Preservar la Continuidad de Todos Los Procesos Críticos	Planteando los Riesgo y las Diferentes Amenazas
Desarrollo del Disaster Recovery Plan (DRP)	Departamento Afectado	En el momento del Suceso o Evento	Equipo Autorizado	Así se mantiene el Área Controlada de Cualquier Riesgo Existente	Con la documentación ya establecida para el plan DRP
Prueba del Plan de Continuidad	Departamento de TI	Luego de Desarrollar el Plan de Estrategia	Departamento y Grupo de Cada Área encargado del BCP	Para la Aprobación del Plan	En Base a los Ejercicios de Pruebas Establecidos
Mantenimiento del Plan de Continuidad	Departamento de Continuidad	Cada 6 Meses	Departamento de Continuidad	Para que pueda Resolver a tiempo un nuevo Proceso Critico Añadido a la Empresa	Reestructurando el Plan

Glosario

GLOSARIO

Almacenamiento: almacenamiento de datos, acción de introducir datos en la memoria de un ordenador.

Activos: conjunto de bienes que se posee.

Backup: es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento.

Cintas Magnéticas: tipo de soporte de almacenamiento de información que permite grabar datos en pistas sobre una banda de material magnético.

Catástrofes: suceso desgraciado que altera gravemente el orden regular de las cosas.

Desastres: interrupción prolongada de los recursos informáticos y de comunicación.

Hardware: conjunto de elementos físicos de un sistema informático.

Infraestructura: conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de una actividad o para el funcionamiento de una organización.

Implementación: instalación y puesta en marcha, en una computadora, de un sistema de explotación o de un conjunto de programas de utilidad, destinados a usuarios.

Red: es un sistema de comunicación entre computadoras que permite la transmisión de datos de una maquina a la otra.

Riesgo: posibilidad de que se produzca una desgracia o contratiempo.

Software: conjunto de programas y rutinas que permite a la computadora la realización de ciertas tareas.

Servidor: Sistema informático que presta ciertos servicios y recursos.

Sistema: programa o conjunto de programas que realizan la gestión de los procesos básicos de un sistema informático y permiten la ejecución del resto de programas.

Switch: palabra que significa “conmutador”, es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria.

TI (Tecnología de Información): Es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar y diseminar información por medios de un computador.

Virus: secuencia de instrucciones que se introduce en la memoria de una computadora con objeto de que, al ser procesada, produzca alteraciones graves en el funcionamiento de la maquina.

Usuarios: es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático.