Comisión de Política Informática
Comisión Nacional de Emergencias

NORMA PARA LA ELABORACION DE PLANES DE CONTINGENCIA CONTRA DESASTRES EN CENTROS DE PROCESAMIENTO ELECTRONICO DE DATOS.

Costa Rica
Marzo 1990

PRESENTACION

Este documento es fruto de un esfuerzo conjunto con objetivos específicos, entre las siguientes instituciones públicas del país:

Banco de Costa Rica
Banco Nacional de Costa Rica
Comisión de Política Informática
Comisión Nacional de Emergencias
Instituto Costarricense de Electricidad. ICE
Instituto Nacional de Seguros
Ministerio de Ciencia y Técnología
Radiográfica Costarricense
Refinadora Costarricense de Petróleo
Universidad de Costa Rica

Por significativo, debe destacarse la labor de concertación que la tanto la Secretaría Ejecutiva de la COPOIN, como la Comisión Nacional de Emergencias, han realizado en procura del concenso para la puesta en marcha de este proyecto, congruentes con la política del gobierno. Debe destacarse por cuanto en proyectos de esta naturaleza,las instituciones públicas del país tienen que percatarse de la necesidad de unir esfuerzos para formar un frente común, más fuerte al tiempo y la adversidad, que conduzca al logro de los objetivos propuestos.

Para un país tan pequeño y de escasos recursos como Costa Rica, la cooperación entre sus ciudadanos es vitalpara el desarrollo de ideas y la consagración de objetivos.

Se espera que este documento sirva de base para que nuestras instituciones, y nuestra sociedad, encuentren en él los elementos necesarios para desarrollar acciones concretas en torno a la elaboración y puesta en ejecución de **Planes de Contingencia**.

AGRADECIMIENTO

Deseamos agradecer a las instituciones para las cuales laboramos, por la oportunidad de trabajar para el bienestar del país en la investigación y el desarrollo de ideas en torno a untema de tanta trascendencia.

De igual manera, deseamos expresar nuestro agradecimiento al grupo de apoyo de la Comisión Nacional de Emergencias, específicamente de la Dirección de Sectoriales, por las facilidades brindadas en todo momento. Muy especial el agradecimiento a la Sra. Gladys Hidalgo, Auxiliar de Computación e Informática del Centro de Informática de la Universidad de Costa Rica, por su colaboración en la preparación de este documento.

Y a todas aquellas personas que nos han dado su apoyo, ¡muchas gracias!.

Grupo Técnico del Proyecto

INDICE

CAPITULO 1: INTRODUCCION

Alrededor de la información giran la actividad del centro de procesamiento electrónico de datos (centro PED) y de la organización misma. De esta forma, los computadores y toda la infraestructura necesaria para su funcionamiento se convierten en factores clave que merecen un estudio cuidadoso, a efectos de garantizar los niveles mínimos que aseguren a la organización, la información vital requerida en los diferentes niveles de su estructura organizativa para el cumplimiento de sus funciones.

"El planeamiento para enfrentar situaciones de emergencia en los centros de procesamiento de datos, es una tarea necesaria, a fin de minimizar el daño causado por los acontecimientos inesperados e indeseados que afectan el procesamiento de información. La destrucción o la sola demora en el flujo de la información, pueden acarrear pérdidas millonarias. Tales pérdidas pueden ser causadas por catástrofes que no pueden ser evitadas y cuya posibilidad de ocurrencia es baja, pero también pueden ser causadas por acontencimientos frecuentes, razón por la que todo centro de cómputo debe estar preparado para enfrentar estas emergencias".

Este documento presenta el resultado de la investigación de un grupo interinstitucional en torno al tema de planes de contingencia, y más específicamente, los relacionados con centros de procesamiento electrónico de datos.

El capítulo 2 presenta la normativa que debe considerarse a la hora de desarrollar un plan de contingencias.

El anexo A considera las medidas de seguridad necesarias para la operación normal de los centros PED, y un modelo o guía de como las instituciones pueden desarrollar su plan de contingencias para operar en situaciones anormales.

1.1. Justificación

Parte de la estabilidad social y económica de nuestro país depende del procesamiento y acceso oportuno a datos almacenados en medios electrónicos, los cuales están ubicados en su mayoría en los centros PED en el Valle Central.

Una investigación realizada en 1987, demostró que ninguno de los centros de cómputo de las instituciones y empresas más importantes del país, disponían de planes concretos a excepción de los esfuerzos que ya el Instituto Costarricense de Electricidad realizaba en ese campo, para enfrentar contingencias.

El hecho de que Costa Rica esté localizada en una zona de gran actividad sísmica y en una zona propensa a otro tipo de desastres de origen natural, obliga a cuestionar la seguridad de los recursos computacionales, y a dedicar esfuerzos para elaborar normas que promuevan el desarrollo de planes de contingencias.

Desastres como los terremotos ocurridos en Estados Unidos, México, El Salvador, Nicaragua y el incendio que destruyó en 1988 una central de commutación telefónica en Chicago, inutilizando los datos de varias compañías demuestran la necesidad de contar con planes eficaces para contingencias que garanticen la recuperación de la capacidad de procesamiento electrónico de datos.

Un estudio realizado en 1988 por la Secretaría Ejecutiva de la Comisión de Política Informática y cuyos resultados se resumen en el documento de "Propuesta de una Política Nacional en Informática para Costa Rica", revela los siguientes datos sobre los recursos computacionales existentes en el país:

SECTOR	MICROS	MINIS	MAINFRAMES
PUBLICO	15.000	25	28
PRIVADO	15.000	475	2
TOTAL	30.000	500	30

Cuadro No.1.
Unidades computacionales instalados por sector.

REGION	MICROS %	MINIS %	MINFRAMES %	VALOR (MILLONES $)
URBANA	80	93	93	116.9
NO URBANA	20	7	7	17.1
TOTAL	100	100	100	134 $

Cuadro No. 2
Unidades computacionales instalados por sector

Actualmente, el programa de la Fundación Omar Dengo amplió sustancialmente la cantidad de micros, con laboratorios instalados por todo el territorio nacional, según se explica en el gráfico No. 1 del anexo B.1.

Es importante destacar que del equipo descrito, casi el100% de los denominados "main frame" están en el Sector Público y ubicados en la Región Urbana, precisamente una de las más propensas a sismos, de acuerdo con los datos de la Comisión Nacional de Emergencia (ver gráfico No.2 del anexo B.1). Asimismo, puede apreciarse en los gráficos No.3, 4 y 5 de este anexo, la forma en que huracanes e inundaciones han afectado el país. Los cuadros No.1 al 3 del anexo B.2, resumen algunos datos sobre erupciones volcánicas y huracanes en Costa Rica, América Latina y el Caribe.

1.2. Antecedentes e Instituciones participantes.

El 30 de agosto de 1988, el Sector de Informática de la Comisión Nacional de Emergencia, acordó de su interés la ejecución del proyecto de **Normas para Enfrentar Desastres en Centros de Cómputo**, propuesto por la Secretaría Ejecutiva de la Comisión de Política Informática **(SE-COPOIN)**.

El 29 de noviembre de 1988, la Comisión de Política Informática en su primera sesión ordinaria acordó en el artículo quinto del acta respectiva:

Acuerdo 4

> Apoyar la ejecución del proyecto de Normas para enfrentar Desastres en Centros de Cómputo.

Acuerdo 5

> Proponer a la Comisión Nacional de Emergencia, que lleve a cabo la coordinación y la ejecución del proyecto de Normas para Enfrentar Desastres en Centros de Cómputo, con la participación de la Secretaría Ejecutiva de la Comisión de Política Informática."

La Comisión de Informática de la Comisión Nacional de Emergencias formó una subcomisión para detallar el proyecto. Producto del trabajo de la misma, se formalizó el documento actual de propuesta del proyecto (ver anexo C.1), en el cual se plantea como obejtivo general:

"Establecer un conjunto de normas para que en base a ellas, una organización pueda elaborar planes de contingencia, que le permitan enfrentar desastres de origen humano o natural, en sus centros de procesamiento de datos".

En mayo de 1989, la Comisión de Informática aprobó la realización del proyecto, formalizándose así el apoyo de la Comisión Nacional de Emergencias al proyecto.

Partiendo de la iniciativa de la Secretaría Ejecutiva de la Comisión de Política Informática y de la Comisión Nacional de Emergencias, varias instituciones del país manifestaron su complacencia en participar en el desarrollo del proyecto "NORMAS PARA LA ELABORACION DE PLANES DE CONTINGENCIA EN CENTROS DE PROCESAMIENTO ELECTRONICO DE DATOS".

En orden alfabético, las instituciones involucradas en la ejecución del proyecto son:

-Banco de Costa Rica
-Banco Nacional de Costa Rica
-Comisión Nacional de Emergencias
-Instituto Costarricense de Electricidad
-Instituto Nacional de Seguros
-Ministerio de Ciencia y Tecnología
-Radiográfica Costarricense S. A.
-RECOPE
-Secretaría Ejecutiva de la Comisión de Política Informática.
-Universidad de Costa Rica

1.3. Metodología.

Con el apoyo de todas las instituciones participantes se conformaron dos comisiones, una de nivel ejecutivo y otra de nivel técnico. A esta última se le encomendó la tarea de elaborar un documento con el cual la primera pudiera analizarla problemática y recomendar las acciones a seguir, desde el punto de vista interinstitucional (ver C.2).

Como parte de la organización y metodología del desarrollo del proyecto, el Grupo Técnico realizó sesiones de trabajo en donde se analizaron objetivos, alcances del proyecto, revisión de bibliografía, experiencias tanto de los mismos miembros del Grupo como de profesionales y empresas nacionales, problemática computacional del país, y en general, actividades que procuraban la adquisición de conocimientos sobre el tema y la problématica global que encierra éste.

El Grupo Técnico desde las primeras sesiones definió la organización y un cronograma de las principales actividades a desarrollar (ver C.2).

Parte importante del resultado final del proyecto lo han constituído dos talleres de trabajo, en los que el grupo ha logrado formalizar este documento.

Para los talleres las instituciones han facilitado tiempo completo de sus representantes en el Grupo Técnico y los recursos necesarios para su satisfactoria ejecución.

INTRODUCCION

Se presentan en los apartados siguientes un conjunto de normas de caracter general sobre la planificación, organización, composición, alcances y naturaleza de un plan de contingencias.

Buscando claridad en su presentación, se han clasificado las normas en:

1-.Generales (administrativas).

2-.Sobre seguridad general.

3-.De los componentes de un Plan.

Los enunciados de las normas se han ordenado y numerado para facilidad de referencia posterior. En adelante hablaremos del Plan de Contingencias o del Plan indistintamente.

2.1 NORMAS GENERALES (ADMINISTRATIVAS)

Son aquellas que se refieren al Plan como un todo. Abarcan los objetivos, naturaleza, metas, etc.

Las normas definidas como generales son:

100. Toda institución debe contar con un plan de contingencias.

101. El Plan debe tener como características:

- Responder a las necesidades particulares de la Institución (auténtico),
- Factible
- Escrito,
- Suscrito, legitimado, tener apoyo por escrito, autorizado por la administración superior de la institucion,
- Conocido, divulgado.

- Actualizado, debe revisarse permanentemente para garantizar su confiabilidad,

- Probado.

102. ETAPAS PARA EL DESARROLLO DE UN PLAN.

Todo plan de contingencias debe tener al menos tres etapas.

102.01 ETAPA I: PLANIFICACION.

El objetivo primordial es obtener el apoyo y aprobación de la administración superior para eldesarrollo del Plan.

Deberá incluir el alcance del Plan, la organización, los recursos, un cronograma de actividades, así como las políticas y estrategias que servirán para su elaboración.

102.02 ETAPA II: ELABORACION.

El objetivo primordial es elaborar el Plan. Deberá concluir con la presentación de un documento que contenga la descripción detallada del Plan.

102.03 ETAPA III: APROBACION Y EJECUCION.

El objetivo primordial es obtener la aprobación final de la administración superior para la ejecución del Plan.

200. COORDINACION DEL PLAN.

El desarrollo del un Plan debe estar bajo coordinación de una persona o comité responsable ante la autoridad superior de la Institución.

300. COORDINACION INSTITUCIONAL E INTERINSTITUCIONAL.

El plan debe ser congruente con las políticas y procedimientos de otras instituciones afines, así como las de auxilio y seguridad nacionales tales como bomberos, Cruz Roja, policía, etc.

2.2 NORMAS DE SEGURIDAD GENERAL.

Estas normas son las mínimas que todo centro PED debe practicar con la finalidad de asegurarse un funcionamiento adecuado bajo condiciones normales. El hecho de omitir la práctica de algunas de ellas puede llevar a una institución a situaciones de contingencia.

Las normas consideradas dentro de seguridad general según áreas de atención son:

100. Edificio.

101. Materiales de construcción.

El edificio donde se ubique el centro PED debe estar construido con materiales que cumplan los estándares mínimos; estos deben ser no combustibles y resistentes al fuego.

102. Tuberías para aguas.

Evitar el paso de tuberías de agua por encima o por debajo del centro PED con el fin de prevenir filtraciones.

103. Ventanas.

Construir el mínimo de ventanas exteriores con el fin de evitar interferencias provenientes del exterior, reducir la posibilidad de entradas no autorizadas y la condensación de agua en días fríos.

104. Servicios.

El edificio debe contar con:

- Espacios disponibles para instalación de equipos derespaldo y auxiliares.

- Acceso razonable para la introducción y extracción de los equipos sin que sufran daños.

- Servicios públicos adecuados: teléfono, electricidad, aguas, vías de comunicación.

- Las salidas de emergencia necesarias.

105. Instalaciones Eléctricas.

Todas las instalaciones deberán ser construidas de acuerdo con los códigos y normas vigentes sobre esta materia (tierras físicas, capacidad máxima de conductores, ductos, códigos de colores, pararrayos, señalamiento de dispositivos, etc.)

106. Localización Geográfica.

106.1 El centro PED no debe instalarse en áreas urbanas potencialmente conflictivas, cerca de compañías que ofrezcan algún peligro (por política o por la naturaleza de sus productos y actividades), cerca de sitios de radares, autopistas o vías muy transitadas, ferrocarriles y rutas de vuelo de aviones.

106.2 Se debe hacer un análisis de las condiciones sismológicas así como de las ambientales: contaminación, ruido y vibraciones.

200. Ambiente del centro PED.

201. Aire acondicionado.

El centro PED debe contar con un adecuado sistema de aire acondicionado que cumpla con las especificaciones recomendadas por el proveedor del equipo de computación.

202. Protección contra el fuego.

202.1 Almacenar sólo el mínimo indispensable de materiales combustibles (papel, cajas de cartón, etc.) dentro delcentro PED.

202.2 Evitar tener cables conductores de corriente eléctrica sueltos o con contactos en mal estado.

202.3 Las cortinas, muebles, pisos, techo, filtros de aire acondicionado, aislantes eléctricos y acústicos deben estar fabricados con materiales no combustibles.

202.4 Debe preveerse la instalación de detectores de humo y alarmas con el fin de descubrir el fuego en su etapa incipiente. Además, instalar aspersores o extintores demano, recomendados para equipo electrónico.

203. Control de ingreso.

203.1 El centro PED debe considerarse un área de acceso restringido, debe contar con: personal de vigilancia debidamente entrenado, una sola puerta de entrada debidamente controlada y el resto como salidas de emergencia.

203.2 Se debe llevar un control del ingreso de personas y vehículos a las instalaçiones, así mismo debe contar con un control de entrada y salida de suministros, dispositivos magnéticos, equipos e información procesada.

300. Personal.

301. Seguridad del Personal

Debe brindarse el máximo de seguridad física al personal que labora en los centros PED, para ello deben tomarse en cuenta las recomendaciones técnicas sobre la iluminación, reglas de seguridad, equipo de primeros auxilios, señalamiento y el equipo de protección que debe utilizar el personal.

302. Definición de funciones.

Para todas las funciones en el centro PED (planeación, producción y mantenimiento) deben especificarse claramente la responsabilidad, en el nivel de autoridad, y cumplirse con la separación de funciones.

400. Administración.

401. Análisis de Riesgos de los Sistemas.Identificación de Sistemas Críticos.

Se debe hacer un análisis regular de los riesgos a que puedan estar sometidos los sistemas, especialmente los considerados críticos y asignar las prioridades de atención y procesamiento.

402. Políticas de Seguridad.

402.01 Los fraudes y otros problemas con el personal deben ser comunicados a las autoridades con el fin de que se sienten las responsabilidades del caso.

402.02 Deben elaborarse políticas de seguridad de acceso a los sistemas de información. Estas deben establecer las prioridades de acceso hacia los programas, archivos, bases de datos, procesos, etc.

500. Datos y Programas.

501. Respaldos de aplicaciones.

Debe definirse un calendario y los métodos de registro necesarios para ejecutar los procesos de respaldo de la información, sistemas operativos, programas, etc.

502. Lugares de Almacenamiento de los Respaldos.

Estos sitios deben ser dedicados especialmente al almacenaje de medios magnéticos. Su construcción debe garantizar total protección contra accesos no autorizados y contra agentes destructivos tales como el agua y el fuego.

503. Documentación.

Los sistemas y programas deben tener respaldo de documentación actualizada y comprensible.

504. Protección de la información producida.

La información confidencial que no se emplea, debe ser destruida. De la misma manera la información importante debe ser almacenada en sitios seguros.

600. Equipo de Cómputo.

601. Mantenimiento.

Deberá contarse con servicio de mantenimiento preventivo y correctivo para los equipos de cómputo, siguiendo las recomendaciones del fabricante.

602. Inventario de equipo.

Debe existir un adecuado registro del equipo instalado. En él se debe especificar el modelo, la marca, serie, número de placa interno, características técnicas del equipo, nombre del proveedor, etc.

603. Operación del Equipo

Deben haber procedimientos claros del encendido y apagado de los equipos.

604. Equipo de ambiente

Deberá contarse con servicio de mantenimiento preventivo y correctivo para los equipos que controlen temperatura, humedad, limpieza de la sala de cómputo, aire acondicionado, limpieza de filtros, entrada de polvos, y humo, equipo de extinción de incendio.

700. Organización Interna.

701. Controles.

701.1 Debe existir un adecuado control sobre el envío o recepción de documentos importantes o formularios sensibles.

701.2 Debe mantenerse un registro de los incidentes de seguridad y de las fallas de los equipos.

702. No deben permitirse malos hábitos en el cuarto del computador (comer, fumar o almacenar material inflamable).

800. NORMAS DE AUDITORIA.

801. Deben existir procedimientos o programas propios de auditoría.

802. Todo sistema o aplicación debe dejar rastros adecuados para la auditoría.

803. Los sistemas deben tener suficientes controles internos.

2.3 NORMAS PARA LOS COMPONENTES DEL PLAN

100. Normas para la Etapa I: Planificación.

101. Aprobación.

La aprobación para realizar el Plan debe darse en los niveles superiores de la administración y en forma escrita.

102. Organización.

Existirá una organización formal.
El personal participante se definirá según el tamaño y las necesidades de la institución, con representantes de la administración superior, usuarios y personal especialista en PED, conformando el grupo planificador.

102.01 Responsabilidades.

El grupo tendrá claramente definidas sus responsabilidades y acciones; deben contar con la autoridad suficiente para establecer los lineamientos correspondientes.

102.02 Personal de la Administración superior.

Sus responsabilidades y acciones se deben orientar a brindar el apoyo necesario para que los recursos asignados se mantengan o mejoren, para lograr el desarrollo del Plan de acuerdo a los objetivos planteados. Además, define las prioridades de procesamiento de aplicación.

102.03 Usuarios.

Sus responsabilidades y acciones se deben orientar a identificar la criticidad de las acciones y definición de sistemas alternos.

102.04 Personal de PED.

Sus responsabilidades y acciones se deben orientar a definir los requerimientos, recursos y procedimientos de sus áreas específicas (redes, sistemas de información, operaciones, etc.)

104. Ambito.

El grupo planificador definirá el alcance del Plan, sus limitaciones, los supuestos, las condiciones de operación y a quién va dirigido.

105. Ubicación.

El grupo definirá los lugares apropiados para ubicar el Plan y las respectivas copias.

106. Características.

El grupo definirá el formato de presentación que se dará al Plan dentro de los siguientes lineamientos:

- Claro y consiso
- Esquemático
- Adaptable

103. Capacitación.

Existirá un programa de capacitación en la materia de planes de contingencia para los participantes en su elaboración.

200. NORMAS PARA LA ETAPA II: ELABORACION.

201. Definición de categorías de procesamiento.

Se establecerá una categorización de prioridades de procesamiento para las aplicaciones, que permita clasificarlas según su importancia para la supervivencia operativa de la organización.

202. Documentación para la contingencia.

Para las aplicaciones críticas, existirá una documentación propia para la contingencia, que indique la prioridad de procesamiento, el tiempo de caída permisible y los recursos necesarios para su funcionamiento.

203. Definición del Centro PED alterno.

Se escogerá el sitio alterno de procesamiento de acuerdo con los requerimientos de las aplicaciones críticas definidas.

204. Organización durante la contingencia.

Se organizará el personal en grupos de trabajo que actuarán en la fase de Atención y Recuperación, en la de Regreso a las Condiciones Normales y en la Revisión y Mantenimiento.

204.01 Funciones y responsabilidades

Se definirán las funciones y responsabilidades de cada grupo, las funciones y responsabilidades de cada miembro del grupo y las relaciones y jerarquía entre ellos.

204.02 Administración de los recursos.

Se identificarán, organizarán y mantendrán actualizados los recursos necesarios para que los grupos de trabajo actúen de acuerdo con las funciones y responsabilidades encomendadas.

300. NORMAS PARA LA ETAPA II: ELABORACION FASE DE ATENCION Y RECUPERACION.

301. La Atención.

Los procedimientos de atención indicarán claramente las acciones a tomar, desde el momento en que se da la contingencia hasta la activación de los procedimientos de recuperación.

Se tomarán en consideración los siguientes aspectos:

a. Lugares de reunión del grupo coordinador
b. Notificación
c. Evaluación
d. Funcionamiento de los grupos de trabajo en lo que respecta a la Atención.

302. La Recuperación

Los procedimientos de recuperación indicarán claramente las acciones a tomar desde la recuperación hasta la activación de la fase de Regreso a las Condiciones Normales.

Se tomarán en consideración los siguientes aspectos:

a. Uso de la documentación de las aplicaciones para la contingencia.

b. Funcionamiento de los grupos de trabajo en lo que respecta a la recuperación.

400. Normas para la Fase de Regreso a las Condiciones Normales.

Se definirán claramente los procedimientos para el regreso a las condiciones normales.

Se tomarán en consideración los siguientes aspectos:

a. Definición del sitio en que operará el Centro PED encondiciones normales.

b. Se ponen en funcionamiento los grupos de trabajo en lo que respecta a esta fase.

c. Adecuación del ambiente del Centro PED.

d. Reubicación de recursos den Notificación de la finalización de la emergencia.

401. Evaluación de la contingencia.

Se hará una evaluación de la forma en que se atendió la contingencia, como se recuperó y cómo se regresó a las condiciones normales. Este estudio debe documentarse en un informe que considere los siguientes aspectos:

- Impacto de la contingencia
- Efectividad de las acciones
- Descripción de los problemas que se presentaron y las soluciones planteadas.
- Modificaciones que deben hacerse al plan de contingencia.

500. FASE DE REVISION Y MANTENIMIENTO DEL PLAN.

En esta fase se revisa la efectividad del Plan a través de pruebas previamente definidas y se establecen los medios adecuados para mantenerlo actualizado, tanto por el resultado de las pruebas como por los cambios normales en las instituciones.

501. Las pruebas

Existirá un plan de pruebas documentado que indique, participantes, frecuencia, tipos de pruebas y forma de conducir la prueba.

501.01 Participantes.

En las pruebas participará el personal que está involucrado en el Plan, personal de la administración superior, personal del centro PED, usuarios y proveedores. Además es importante la participación de los auditores para que ayuden a detectar problemas y den recomendaciones.

501.02 Frecuencia.

Se establecerá una frecuencia adecuada para realizar las pruebas tomando en cuenta para ello, la cantidad de cambios que sufre el Plan y el período ideal para mantener al personal involucrado actualizado.

501.03 Tipos

Se establecerá, para el período que abarque el Plan de pruebas los tipos de pruebas que se realizarán, por ejemplo:

- Total
- Parcial por áreas de interés (capacitación del personal, reacción de los proveedores, condiciones del sistema alterno y de respaldo, disponibilidad de los suministros, etc).

501.04 Puesta en práctica de la prueba.

Para poner en práctica la prueba se tomará en cuenta losiguiente:

- Seleccionar el componente o componentes a probar.
- Establecer objetivos de la prueba, para determinar el éxito.
- Revisar los requerimientos de la prueba y obtener suaprobación y el respaldo.
- Anunciar la prueba y su duración (esta acción puede ser omitida).
- Recopilar los resultados de la prueba.
- Evaluar los resultados de la prueba.
- Analizar las implicaciones de la prueba.
- Documentar los resultados de la prueba y recomendaciones.
- Actualizar el plan de contingencia.

502. El mantenimiento

Existirá un procedimiento de mantenimiento del Plan que asegure que sea actualizado y conocido por los involucrados.

502.01 Actualización.

El Plan se actualizará siempre que se dé alguna de éstas situaciones:

- Conclusión de una prueba.
- Cambio de política de la institución.
- Cambios en los recursos tales como personal, software, hardware, proveedores, etc.

502.02 Comunicación de cambios

Comunicación de cambios se deben establecer los procedimientos y mecanismos apropiados que aseguren el conocimiento del personal sobre cambios que se realicen al Plan.

503. Se deben establecer los mecanismos y procedimientos apropiados que garantizan un conocimiento general del Plan,así como preparar capacitación necesaria para su uso apropiado.

600. Normas para la Etapa de Aprobación y Puesta en Ejecución del Plan.

601. La administración superior indicará las modificaciones necesarias para que sean desarrolladas por el grupo coordinador.

602. La administración superior dará el apoyo necesario para su ejecución.

603. La auditoría controlará la ejecución del Plan y presentará informes periódicos a la administración superior, acerca del curso que mantiene el Plan.

3. CONCLUSIONES Y RECOMENDACIONES

3.1. CONCLUSIONES

La necesidad de Planes de Contingencias está suficientemente demostrada. Conforme las organizaciones aumentan la automatización de sus operaciones, éstas son más dependientes de la tecnología que capta, almacena y procesa la información vital para su funcionamiento.

Es imperativo que en nuestro país se tome consciencia del problema y se dicten las medidas necesarias para salvaguardar la enorme inversión que se ha realizado en el campo de la computación, especialmente la del Sector Público.

Las conclusiones que se derivan del trabajo presentado pueden resumirse de la siguiente forma:

La planeación para la recuperación de una contingencia no es un problema técnico ni exclusivo del área de procesamiento de datos. Debe ser enfocado como parte integral de la planeación general de la organización.Esta consiste en planes y disposiciones que son necesarias para asegurar la continuidad de las operaciones. Los planes deberán cubrir todos los eventos que puedan producir el cese de operaciones o destrucción de datos o dispositivos. Por eso, debe poseer varias características como:

Factible
Vendible
Dinámico
Exclusivo
Fácil de implantar
Concreto
Previsor
Autoritario
Completo

- El Plan requiere de una planeación cuidadosa para garantizar que el mismo sea oportuno y realista, en términos de tiempo y características de la institución para la que fue creado.

- En este tipo de proyectos es necesaria una gran labor educativa, pues es un hecho que en la actualidad no es claro para la alta dirección de las instituciones, la necesidad de un plan de contingencias. Esta labor es muy importante pues la decisión de trabajar en un Plan implica la asignación de recursos.

Además, la existencia de un Plan escrito no garantiza de por sí la capacidad de recuperación en caso de contingencia.

Los aspectos concernientes a seguridad general son indispensables para evitar una contingencia.

- El Plan requiere de un fuerte apoyo de la administración superior.

3.2. RECOMENDACIONES

1. Solicitar a la Comisión Nacional de Energencias, divulgar los resultados de este trabajo.

2. Solicitar a la Secretaría Ejecutiva de la COPOIN promover políticas en torno a la necesidad de planes de contingencia en el sector público del país.

3. Solicitar a la Secretaría Ejecutiva de la COPOIN y la Comisión Nacional de Emergencias, realizar gestiones pertinentes para establecer en el país, una normativa en torno al desarrollo de planes de contingencia.

4. Dar segumiento a los resultados del desarrollo de planes de contingencia en las instituciones involucradas en este proyecto.

5. Promover entre las instituciones públicas del país la búsqueda de asesoría en el desarrollo de planes de contingencia.

6. Promover talleres periódicos de intercambio y actualización a nivel nacional.

7. Promover la capacitación del Grupo Técnico con talleres, asesoría con expertos internacionales, u otros mecanismos.

8. Las instituciones deben plantear estrategias de corto y largo plazo que les permitan crear consciencia sobre la necesidad de estos Planes.