UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SISTEMATIZACIÓN DE UN PLAN DE CONTINGENCIAS INFORMÁTICO PARA LA FACULTAD DE INGENIERÍA

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

ALMA ZOILA SANTOS MEDINA

FERNANDO ANDRÉS CALZADA SALAS

DIRECTOR DE TESIS:

ING. JOSÉ ARTURO ORIGEL COUTIÑO

2004

A mis padres y hermana:
Por el apoyo brindado en los
años difíciles y en los felices

A Andrés Calzada:
Por pertenecer a este proyecto y su
entrega en la realización del mismo

A Rafael Fernández:
Por enseñarme a no dejarme vencer
ante las adversidades y recordarme
que siempre hay esperanza

A Carmen y Maye:
Por sus palabras de aliento,
cuando más las necesitaba

A Felisa, Luz Elena, Azucena, Javier,
Gerardo, Héctor, Luis, Pedro y Noé:
Por ser amigos de la Facultad
con quienes tuve momentos
agradables y memorables

Alma Santos M.

Agradezco a DIOS y a mis Padres
por darme la vida y por sus dulces y valiosas lecciones;

a Claudia
por su gran amor y por la felicidad que tengo a su lado;

a mis hermanos: Ricardo y Armando
por su apoyo, sabiduría y cariño

y a mis familiares y amigos
por el gran significado que tienen en mi vida.

Andrés Calzada S.

Alma Santos y Andrés Calzada
queremos agradecer
al Ing. José Arturo Origel Coutiño
por creer en este proyecto y brindarnos
su apoyo incondicional.

ÍNDICE

3. ELABORACIÓN DEL PLAN DE CONTINGENCIAS

APÉNDICES

INTRODUCCIÓN

El desarrollo tecnológico ocurrido en las últimas décadas en el campo de la informática, ha permitido que el volumen de información manejado y almacenado dentro de muchas instituciones (incluyendo a la UNAM y todas sus dependencias), haya crecido de manera sustancial y se pueda acceder a dicha información de forma más rápida y eficiente, dándole a ésta una valor muy alto en función de los fines que persigan dichas instituciones en la explotación de dicha información.

Las computadoras y su capacidad de almacenamiento y procesamiento de datos, son una herramienta necesaria para proporcionar la información requerida por las instituciones, sin embargo no siempre se destina una prioridad alta a la responsabilidad en el manejo y protección de dichos procesos y almacenamiento de información [1].

Aunado a esto, las instituciones no están a salvo de posibles contratiempos que pueden imputarse a diferentes causas de índole natural, humano o tecnológico[2] , como siniestros (terremotos, inundaciones, incendios, etc.) , fallas prolongadas de energía eléctrica, daños intencionales (sabotajes) o accidentales, fallas en los equipos de comunicaciones o en los dispositivos de almacenamiento y proceso de información, o fenómenos sociales (huelgas, paros laborales, etc.) y que signifique la interrupción en los servicios informáticos o la perdida (o falta de acceso) a la información necesaria para la operación de la institución, teniendo en cuenta que la pérdida de dicha información pueda ser consecuencia de daños causados a sus dispositivos de almacenamiento, proceso y comunicación, o la perdida accidental o deliberada de la misma.

Considerando lo anterior, es importante establecer un curso de acción que permita a las instituciones continuar sus operaciones de procesamiento de la información mediante la utilización de los recursos de respaldo y operabilidad alternativa identificados en el desarrollo de un plan de contingencias o plan de recuperación en caso de imprevistos y que permita tener una guía de restauración rápida y organizada de las operaciones de cómputo después de una suspensión de los mismos.

[1] Fisher, Royal P. Seguridad en los sistemas informáticos. Ed. Diaz de Santos, 1988. p 1.
[2] http://www.ebcpartners.com/PDF/NIST_Plan.pdf p.7

1. PLANTEMIENTO Y DEFINICIÓN DEL PROBLEMA

1.1 Definiciones.

***Contingencia Informática*:** Se define como la interrupción no planificada de la disponibilidad de recursos informáticos (o de los medios y las facilidades necesarios para su correcta operación) de alguna organización o dependencia, ya sea temporal o definitiva, y que puede ser provocada por fenómenos naturales, por intervención directa del hombre o por fallas tecnológicas provocadas o incidentales.

Plan de Contingencias: Es un plan realizado por escrito en el que se detallan acciones, procedimientos, recursos y medidas de detección y de reacción que deben usarse durante un evento que provoque la destrucción parcial o total de los bienes y servicios de determinada institución. Esto se refiere básicamente a las medidas que deben tomarse con el fin de recuperar la información y restaurar los procesos y servicios durante y después de una emergencia o la interrupción de la operación en algún sistema. Su función principal radica en garantizar la continuidad de los procesos informáticos ante cualquier desastre que pudiese ocurrir.

El Plan de Contingencia deberá obedecer a un proceso formal de desarrollo y deberá ser la conclusión de un proyecto de realización del mismo que incluya la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución a posibles contingencias; además se deberá llevar a cabo una prueba –bajo condiciones controladas– del Plan desarrollado, una capacitación de las personas involucradas y una constante actualización; el Plan de Contingencias suele combinarse con planes de seguridad general.

El Plan de Contingencia se puede dividir en las siguientes fases:

a) Fase de emergencia: Es la fase inmediata a la aparición de la contingencia; su objetivo es minimizar el daño causado por el evento en cuestión, considerando primero la seguridad del personal y después el posible rescate de los recursos involucrados, su relevancia radica en la rapidez de su ejecución; en esta fase también se hace una valoración de los daños causados; es responsabilidad principalmente de la Organización en su conjunto.

   En esta etapa se considera la notificación del hecho al personal pertinente y la activación del resto de las fases del Plan de Contingencias dentro de la Organización.

b) Fase de restauración: Tiene por objetivo buscar alternativas que permitan continuar con la operación de los procesos críticos que realice la organización, los cuales deben restablecerse en un corto plazo para afectar lo menos posible el desempeño de la misma; en el caso de un plan de contingencias enfocado a recursos informáticos, la realización de esta fase es responsabilidad del área de informática, principalmente, en cooperación con los usuarios de dicha área.

c) Fase de recuperación: En esta fase, se pretende restablecer totalmente la operatividad de los procesos de la organización afectados durante el evento de contingencia; plantea estrategias a medio plazo para la recuperación de éstos (los procesos).

   Esta fase, al igual que la anterior deberán su éxito, en buena medida a la planeación previa y a las medidas preventivas adoptadas para la aparición de una contingencia.

El Plan de contingencia Vs. el Plan de continuidad: Dentro de la literatura referente a seguridad informática se pueden encontrar con frecuencia los términos "Plan de Contingencia" y "Plan de Continuidad", mismos que tienen entre ellos algunas diferencias las cuales es necesario precisar[3]:

El Plan de Continuidad está orientado a asegurar la productividad, satisfacción del usuario y continuidad operativa a pesar de la ocurrencia de eventos inesperados, operando bajo la premisa de *"no detenerse"* dentro del concepto de *"continuidad del servicio";* el Plan de Contingencia plantea como objetivo la minimización del impacto operativo que pueda acarrear un suceso inesperado dentro de la organización, dentro de éste tipo de plan se considera la existencia de tiempo fuera de línea, tiempo sobre el cual se declara la emergencia, y entran en operación una serie de procedimientos que permiten que el servicio se restablezca lo mas pronto posible.

El Plan de Continuidad está diseñado para sistemas y procesos que operan en tiempo real, se ejecuta permanentemente a través de la administración de riesgos tanto en la información como en la operación; el Plan de Contingencia está diseñado para sistemas y procesos que pueden tolerar intervalos de tiempo fuera de línea (72 horas inclusive), se concentra en la recuperación de eventos únicos que producen una interrupción del servicio.

A diferencia del Plan de Contingencia, el Plan de Continuidad se basa en tecnologías vanguardistas (como cableado estructurado alternativo para las redes de computadoras, servidores de replicación y cintas para copias de respaldo de altísima velocidad) y la excelencia operativa del centro de cómputo, razón por la

[3] http://delta.hypermart.net/prof/PRO189.html

cual resulta muy costoso y no está al alcance de todas las organizaciones, ni para todos los procesos de las mismas; se requiere un adecuado estudio de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no contar con él.

Resulta primordial determinar la criticidad de cada proceso dentro de las organizaciones. Para los de muy alta criticidad se deberá implementar un plan de continuidad, en los demás casos se implementa un plan de contingencia[4].

El Plan de contingencias Informáticas y el Plan de contingencias Físicas: Señalamos la diferencia entre estos dos tipos de plan de contingencia, haciendo énfasis en que ambos son complementarios entre ellos, en virtud de que en la mayoría de los casos una Contingencia Física cuya magnitud impida el acceso a los sitios en los cuales se encuentran los servicios y recursos informáticos, puede acarrear la ocurrencia de una contingencia de tipo informático o la incapacidad para poder utilizar oportunamente la información generada por dichos servicios y recursos.

El Plan de contingencias físicas se basa en la necesidad de solucionar problemas presentados en la infraestructura y en los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos; esto es todas aquellas contingencias que afecten directamente a las áreas de comunicaciones, ventilación, iluminación energía eléctrica, hardware, etc. Las principales causas de este tipo de contingencias pueden ser:

- Desastres naturales –incendios, tormentas, sismos, inundaciones, etc.
- Daños causados por la intervención humana, ya sea incidentales – operación inadecuada de los medios de infraestructura, falta de observancia en las medidas de seguridad, etc.– o provocados deliberadamente –sabotajes.
- Fenómenos sociales y atentados deliberados contra el equipo (sabotajes, robo, disturbios, huelgas, etc.)

El Plan de contingencias informático se refiere al manejo de los imprevistos provocados por errores tecnológicos y que puedan desembocar en la pérdida parcial ó total de los datos o de la operatividad informática de de la organización; dicha pérdida, también se refiere a la pérdida de la integridad o confiabilidad del conjunto de datos –o bases de datos– de la organización en sí, o en los medios a través de los cuales dichos datos son transportados, manipulados o presentados

[4] Siempre y cuando se cuente con los recursos necesarios para la implementación de un plan de Continuidad. En nuestro caso de estudio, la aplicación de un Plan de Continuidad resulta poco realizable.

para su uso[5], así como la corrupción de programas o redes que puedan interrumpir el desempeño normal de los procesos y reportes de información.

El Plan de contingencias informático involucra el concepto de seguridad Lógica, la cual consiste en la aplicación de barreras y procedimientos que resguarden la información y sólo se permita el acceso a la misma a las personas autorizadas para este fin. Los principales causales de contingencia que contempla este tipo de plan son:

- Infiltración de intrusos y agentes externos a los medios y servicios de información.
- Daños causados por virus informáticos.
- Perdida de información (Por daño a los medios de almacenamiento.)
- Integridad corrompida de la información.
- Fallas de conectividad en los servicios de red (LAN o WAN)
- Fallas en los servicios tecnológicos externos (teléfono, alimentación eléctrica, conectividad, Internet, etc.)
- Modificación errónea de programas y los archivos

Ya sea que la amenaza sea provocada por fenómenos naturales, errores u omisiones humanas, actos intencionales o fallas tecnológicas, ésta puede ser atacada:

- Minimizando la posibilidad de su ocurrencia de eventos dañinos (prevención).
- Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
- Diseñando métodos para una rápida recuperación de los daños experimentados.
- Corrigiendo las medidas de seguridad en función de la experiencia obtenida.

Plan Institucional de Desarrollo Informático (PIDI): Documento que permite establecer los objetivos, políticas y estrategias necesarias –tanto los actuales como los proyectadas a futuro– para llevar a cabo la correcta función y operación informática de una organización.

El Plan Institucional de Desarrollo Informático es aplicable en cualquier tipo de organización, ya sea de carácter publico o privado; los criterios a considerar para la elaboración del PIDI competen a todas las áreas de la organización que tengan relación con el área de informática y aquellas que en un futuro requerirán apoyo de dicha área.

[5] Toigo, Jon W. Disaster Recovery Planning. Prentice Hall 1989. p 4.

Un documento de este tipo debe contar con los siguientes atributos:

a) *Integral :* Debe estar dirigido a todas las áreas de la organización,

b) *flexible:* Se debe poder adaptar a los cambios derivados de los avances y progresos dentro de la organización,

c) *factible:* Deben poder desarrollarse todas sus etapas componentes, con base en una previsión de las actividades que lo conforman tomando en cuenta la disponibilidad de los recursos disponibles para su instrumentación,

d) *jerárquico:* Que dé respuesta a las prioridades determinadas por la alta dirección de la organización y

e) *normativo:* Debe constituir la base y marco de referencia que regule la operación de la función informática.

1.2 Marco de Referencia.

1.2.1 El PIDI de la Facultad de Ingeniería.

Al igual que algunas instituciones de carácter público y privado (p. e. INEGI), la Facultad de Ingeniería cuenta actualmente con un Plan Institucional de Desarrollo Informático (PIDI), sin embargo éste se encuentra en una fase complementaria, en la cual está planeado incluir tópicos referentes a seguridad informática (un apartado muy notable dentro del PIDI.)

Los objetivos que se pretenden cumplir con el PIDI (y su fase complementaria) son:

a) Establecer un esquema de desarrollo sistemático, armónico y racional de los servicios de informática con que cuenta la Facultad para apoyarla de forma eficiente en sus funciones para el logro de sus objetivos como institución educativa,

b) regular el desarrollo de la función informática bajo criterios únicos, desde su concepto hasta su implantación y

c) establecer las normas para el seguimiento y evaluación de aspectos referentes a la utilización de material, equipos, sistemas y servicios informáticos, tomando en cuenta los requerimientos técnicos y económicos de las adquisiciones, contrataciones y subrogación de servicios.

1.2.2 Lugar del Plan de Contingencia Informática dentro del PIDI de la Facultad de Ingeniería

El PIDI de la Facultad de Ingeniería (FI), considera un capítulo completo al tema de la Seguridad Informática, en el que se hace hincapié en las Políticas de Seguridad (PSC) en los tres rubros que lo conforman: Seguridad Física, Seguridad Lógica y Sanciones.

Tomando en cuenta la acciones preventivas consideradas para este capítulo del PIDI –que tienen como finalidad evitar la ocurrencia de sucesos que puedan afectar la operación de los sistemas y la integridad de la información de la FI–, se contempla también la necesidad de la existencia de un documento que proporcione las métricas y la metodología a seguir en caso de que las políticas de seguridad sean insuficientes y la ocurrencia de los mencionados sucesos se haga presente; es aquí donde se considera la existencia del Plan de Contingencia Informáticas –siendo éste un apartado en el capítulo de Seguridad Informática– como una metodología de acción en el caso de la ocurrencia de sucesos que afecten la operación –y por lo tanto que atenten contra la seguridad– de los procesos y los recursos informáticos de la FI; el citado Plan de Contingencia Informática es nuestro caso de estudio.

1.2.3 Necesidad de la existencia de un plan de contingencia Informática dentro de la Facultad de Ingeniería.

Considerando que los datos son el principal patrimonio de toda Institución que dependa de recursos informáticos para su operación, es necesario establecer un plan de acción que cuente con las disposiciones para proteger dichos datos –así como a sus medios de almacenamiento, transmisión y proceso– de eventos inesperados que puedan representar una amenaza para la integridad de los mismos.

Generalmente, la necesidad de contar con un plan de contingencia, es evidente para los encargados del área de informática de la mayoría de las organizaciones, quienes regularmente manifiestan una actitud protectora hacia los sistemas a su cargo, especialmente los sistemas desarrollados dentro de la organización. Los buenos directivos deberán tener interés especial en la seguridad y el buen desempeño de los sistemas a su cargo.

Así mismo, los profesionales en el área de informática tienen, como una de sus encomiendas principales, proteger la integridad de los sistemas y asegurar su supervivencia. Los acuerdos de servicios entre el área de sistemas y sus usuarios dentro de la organización –e incluso fuera de la misma– son una manifestación del compromiso de calidad y excelencia de sus procesos informáticos.

Deberá entonces existir un plan de contingencia si los mencionados acuerdos han de tener credibilidad. El personal encargado de los sistemas informáticos, deberán prestar atención al desarrollo de un plan de contingencias como uno de los esfuerzos dentro de la dependencia para garantizar la seguridad y la integridad de sus datos[6].

Puesto que el tiempo es crucial para la operación de los sistemas, es necesario contar con planes de respaldo para posibilitar una rápida reacción ante las fallas de las operaciones o los cambios en el entorno social o físico. Pongamos el ejemplo de un PC, suponiendo que ésta fue robada o está descompuesta: en primera instancia, esta situación representa un problema, pero si dicha PC no puede ser reparada o sustituida en un tiempo razonable, esta situación puede acarrear consecuencias catastróficas para quien la utiliza. Cualquiera que sea la causa, la suspensión de los servicios de cómputo dentro de una organización por un tiempo prolongado puede ser devastadora.

Además, el hecho de que una Organización cuente con seguros necesarios para solventar los daños a las instalaciones, hardware y a los medios de almacenamiento de la información después de una catástrofe, puede no servir de mucho en virtud de que se puede sustituir o reponer el equipo de cómputo, pero no la información que aloja.

La Facultad de Ingeniería, siendo una organización de carácter público dedicada a la formación de profesionales en el área de ingeniería y que maneja la información correspondiente a su alumnado –que asciende a una matricula de mas de diez mil Alumnos, a los cuales brinda atención en rubros como proceso y entrega de calificaciones e historias académicas, asignación de grupos, tanto a alumnos como profesores, servicios estudiantiles, entre otras tareas– y de numerosos proyectos de investigación, no puede correr el riego de prescindir de dicha información, o perderla en algún evento, no importando la naturaleza de éste.

Contar con un plan de contingencia informática, proporcionará a la Facultad una guía de recuperación rápida y organizada de las operaciones de cómputo después de una suspensión; minimiza la pérdida potencial de activos y mantener a la institución en un nivel de operación normal, al tomar acciones decisivas basadas en la planeación anticipada. El Plan de contingencia mitigará los efectos de dichos desastres y permitirá una respuesta rápida, una transferencia del procesamiento critico a otras instalaciones y una eventual recuperación.

Por las razones expuestas en los párrafos anteriores, dentro del capitulo de seguridad Informática del Plan Institucional de Desarrollo Informático de la FI, se plantea la necesidad de la existencia de un Plan de Contingencia Informática el cual sirva como auxiliar en la recuperación de información, sistemas, procesos y servicios en caso de la ocurrencia de algún evento extraordinario que altere la correcta operación de los anteriores.

[6] Toigo, Jon W. Disaster Recovery Planning. Prentice Hall 1989. p 7

1.3 El Plan de Contingencias como parte de los Estándares Internacionales de Seguridad Informática.

Durante el desarrollo del presente trabajo, consideramos prudente consultar algún estándar de seguridad informática. Debido al prestigio de la Organización Internacional para la Estandarización (ISO por sus siglas en inglés: *International Organization for Standarization*), optamos por basarnos en los documentos generados por esta organización con respecto a seguridad informática[7].

Basados en el capítulo 11 del documento ISO / IEC 17799 2000 se obtuvieron los enunciados descritos en los párrafos siguientes, los cuales servirán de referencia para la elaboración del Plan de Contingencia Informática para la FI:

Cada organización deberá contar con un plan de contingencia que permita contrarrestar las interrupciones en las actividades de dicha organización y proteger los procesos informáticos críticos de los efectos de fallas mayores o desastres; es decir, se deberá contar con un proceso de administración de la continuidad de la operación para reducir el lapso de interrupción de los servicios provocado por siniestros y fallas de seguridad –las cuales pueden ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas en los servicios informáticos o acciones deliberadas en contra de los mismos– para un nivel aceptable entre la combinación de controles de prevención y recuperación.

El plan de contingencia deberá desarrollarse e implementarse para asegurar que los procesos informáticos de la organización puedan ser restituidos dentro de un periodo de tiempo pertinente.

El citado plan deberá contemplar una fases de prueba y mantenimiento para que se vuelva una parte integral de todos los demás procesos de la organización. La administración de la continuidad de la operación deberá incluir controles para identificar y reducir riesgos, limitar las consecuencias de los incidentes perjudiciales y asegurar la recuperación oportuna de los procesos operativos esenciales.

Los elementos propuestos por la norma ISO/IEC 17799 con los que deberá contar el Plan de contingencia se describen a continuación:

a) Deberá existir un proceso bien administrado que favorezca el desarrollo y mantenimiento de la continuidad de operación de los procesos informáticos dentro de la organización.

[7] El documento generado por ISO que normaliza aspectos de seguridad informática es: *INTERNATIONAL STANDARD* ***ISO/IEC 17799*** *2000: Information Tecnology, code of Practice for Information Security management.* Dicho documento fue creado por el Instituto Británico de Estándares (BSI por sus siglas en inglés: *British Standards Institution*) bajo el nombre BS 7799.

b) La continuidad de operación los procesos informáticos deberá comenzar con la identificación de eventos que puedan desembocar en la interrupción de los procesos operativos, por ejemplo: fallas en el equipo de cómputo, inundaciones, incendios, etc.

   Estas acciones deberán acompañarse de una calificación de riesgo para determinar el impacto de dichas interrupciones –tanto en términos de nivel de afectación y periodo de recuperación–. Ambas actividades deben llevarse a cabo con la total atención de los propietarios de los procesos informáticos y los recursos de la organización.

c) Los planes de contingencia deberán desarrollarse para mantener o restaurar la operación de la organización en el lapso de tiempo requerido ya sea a causa de la interrupción o de la falla de los procesos críticos de dicha operación.

d) Nuestro plan de contingencia deberá mantener una estructura simple para asegurar que todos sus componentes sean consistentes y para identificar prioridades para prueba y mantenimiento.

e) El plan de contingencia deberá ser sometido a pruebas programadas de forma regular para asegurar su vigencia y nivel de efectividad. Dichas pruebas deben asegurar que todos los elementos del equipo de recuperación[8] y otros grupos de trabajo involucrados están concientes de la aplicación del plan.

f) El plan de contingencia deberá de someterse a constantes revisiones, actualizaciones y acciones de mantenimiento para asegurar su efectividad. El programa de administración de la organización deberá incluir información sobre los procesos informáticos críticos para asegurar que las cuestiones de continuidad están correctamente dirigidas.

[8] El Plan de Contingencia contempla la creación de grupos de trabajo y delegación de responsabilidades, las cuales se explicarán a detalle en capítulos posteriores.

1.4 Objetivo General de la Tesis

Elaborar el esquema de un Plan de Contingencia Informática para la Facultad de Ingeniería que considere el restablecimiento oportuno de los proceso informáticos y la información de carácter primordial, basado en el análisis de las necesidades y recursos generales de la Facultad a este respecto y apoyados por la consulta de un estándar de seguridad informática, con el fin de que el documento generado pueda incorporarse al Plan Institucional de Desarrollo Informático (PIDI) de la Facultad –como un apartado de la normatividad de seguridad adoptada dentro de la misma– y pueda difundirse a través de medios electrónicos a las dependencias que lo requieran para que, con base en la métricas sugeridas puedan implementar un Plan de Contingencias Informático adecuado al dependencia en cuestión.

2. ANÁLISIS

2.1 Introducción

El análisis de impacto es una parte fundamental en el proceso de elaboración del Plan de Contingencia, el cual permite al coordinador del plan, catalogar en su totalidad a los requerimientos, procesos e interdependencias de los sistemas y utilizar dicha información para determinar las necesidades y prioridades de recuperación del Plan de Contingencia.

Las fases del análisis de Impacto se describen a continuación:

a) Identificación de recursos esenciales: Los sistemas de información pueden ser muy complejos, con un gran número de componentes, interfaces y procesos. Un sistema cumple, en la mayoría de los casos, con varios objetivos –por ejemplo proporcionar información o servir como interfase de otros sistemas de cómputo–, lo que desemboca en diferentes perspectivas acerca de la importancia de los servicios o capacidades del sistema en cuestión.

   El primer paso en el Análisis de Impacto (AI) consiste en evaluar el sistema de información para determinar las funciones esenciales llevadas a cabo por dicho sistema e identificar los recursos específicos requeridos para ejecutarlas.

b) Impacto de la Interrupción de los servicios de cómputo y tiempo fuera de línea permitido: En esta fase, se deberán analizar a detalle los recursos críticos identificados con anterioridad para determinar las posibles consecuencias de que alguno de los citados recursos sea dañado o desconectado.

   En el análisis de impacto, se deberán evaluar dos factores principales: los efectos de estar fuera de línea y su relación con diferentes lapsos de permanencia en dicho estado. Esto nos permitirá determinar el tiempo máximo permitido que un recurso puede estar deshabilitado antes de que esta situación altere o inhiba la ejecución de una función esencial; los efectos de estar fuera de línea deben de tratarse con base en los recursos relacionados y sistemas de información dependientes, identificando cualquier efecto "en cascada" que pueda ocurrir como consecuencia de la interrupción de la operación de algún sistema y que pueda afectar otros procesos o sistemas relacionados con él.

c) Prioridades de recuperación: El tiempo permitido para tener nuestros servicios fuera de línea –y el impacto consecuente–, nos permiten desarrollar y dar prioridad a las estrategias de recuperación que serán

implementadas durante la activación del plan de contingencia. Por ejemplo, si se determina que el sistema debe de ser recuperado en un lapso no mayor a seis horas, se deben ajustar el plan de contingencia para recuperar los sistemas críticos en dicho lapso.

De la misma forma, si otros componentes del sistema pueden tolerar estar deshabilitados, digamos, 24 horas, pero se requiere que otros componentes no permanezcan en este estado mas de cuatro horas, el Coordinador del Plan de Contingencia deberá dar prioridad a la puesta en marcha de los componentes críticos. Asignando prioridades a las Estrategias de recuperación, se podrán crear documentos y fuentes de consulta más robustos y adecuados que consideren el tema de contingencias, ahorrando tiempo, esfuerzo y costos.

Se considera que el análisis propuesto sea responsabilidad de cada una de las áreas de la FI, sin embargo la colaboración del presente trabajo consiste en la identificación general de las situaciones alguna vez acaecidas dentro de la FI y que de han afectado el buen desempeño de los procesos informáticos dentro de la misma.

Para realizar el análisis antes mencionado, el primer paso fue hacer una serie de entrevistas a las personas encargadas del área de cómputo de cada División y Secretaría (que llamaremos expertos), que al mismo tiempo son parte del Comité Asesor de Cómputo de la Facultad de Ingeniería y por tanto conocen el funcionamiento, así como las limitaciones del área en cuestión.
Es importante mencionar que antes de iniciar las entrevistas, se obtuvo el número de Secretarías y Divisiones que conforman la Facultad, además, se solicito una relación del personal a cargo del área de cómputo de cada Secretaría y División.

Las entrevistas se llevaron a cabo de la siguiente manera:

- Se formularon una serie de preguntas[1] en las que se permitía al experto la oportunidad de contestar abiertamente e incluso comentar sucesos ocurridos del por qué, cuándo y cómo ocurrieron interrupciones de los sistemas a su cargo. Esto permito profundizar en algunos temas e incluso formular otras preguntas que no teniamos registradas en ese momento.

- En cada entrevista se realizaban anotaciones que permitía recordar con facilidad partes importantes y sustanciales de la conversación al momento de transcribir el reporte de la entrevista.

- Se aplicaron un total de 12 entrevistas, una por cada Secretaría, División y Coordinación.

[1] Las preguntas formuladas a los expertos se pueden consultar en el primer cuestionario del apéndice D

Finalmente, los resultados de las entrevistas nos permiten desarrollar los siguientes subtemas que se presentan a continuación.

2.2 Inventario de Recursos Críticos dentro de las Divisiones de la Facultad de Ingeniería

2.2.1 Inventario de recursos tecnológicos

La necesidad de contar con un inventario de recursos tecnológicos radica en las siguientes razones:

Evaluación de daños: Al hacer uso del inventario de recursos tecnológicos a manera de lista de verificación, se puede evaluar rápidamente el estatus del sitio y los elementos que lo componen. De esta manera podrá determinarse si el sitio cuenta con algún tipo de capacidad operativa después de ocurrida la contingencia.

Restauración de instalaciones: para poder corregir los daños acaecidos dentro del centro de cómputo por el impacto de un desastre, se utilizará el resultado de la evaluación del daño; permitirá identificar claramente los dispositivos destruidos y las instalaciones existentes se podrán habilitar mas rápidamente una vez ocurrida la contingencia.

Como parte de los resultados de la entrevista realizada a los expertos en las Divisiones y Secretarías que conforman la FI, fue posible registrar las siguientes clases de recursos tecnológicos:

- *Software:* Diez de las secretarías y divisiones de la FI cuentan con sus propias licencias y software de instalación de paquetería en discos compactos (CD's), en caso de que fuera necesaria la reinstalación de software en el equipo de cómputo correspondiente.

- *Datos*: Considerados como la parte medular de la operación dentro de las dependencias de la FI; la información critica se encuentra respaldada en once de las áreas entrevistadas.

- *Medios de almacenamiento y respaldo:* Once de las Divisiones y Secretarías, realiza los respaldos en CD's, sin embargo, existen dos lugares que utilizan cintas magnéticas.

- *Hardware:* Cada Secretaria y división dentro de la FI, cuenta con un inventario de hardware detallado, por tanto, se puede recurrir a él en caso de contingencia.

- *Equipo de comunicaciones y redes:* Igual que en el punto anterior, también se tiene registrado en este inventario, el equipo de redes y telecomunicaciones, en todas las Secretarías y Divisiones.

- *Documentación:* Son considerados en este rubro, los manuales técnicos y de usuario, así como registro de las direcciones de IP, mapas de las redes de cómputo, inventario de equipo de cómputo, documentos sobre los seguros, convenios, garantías sobre el equipo, entre otros. A continuación se presenta (Tabla1) un resumen del número de Secretarías y Divisiones que cuentan con los puntos mencionados anteriormente y nos permite explicar a detalle este punto.

Documento	Número de Secretarías y Divisiones que cuentan con este documento
Manuales Técnicos	4
Manuales de Usuario	6
Registro de direcciones IP	12
Mapas de Red	5
Inventario de equipo de cómputo	12

Tabla1. Número de Secretarías y Divisiones que cuentan con alguno de los documentos mencionados

Se registró que solo cuatro de las áreas entrevistadas, cuentan con los cinco puntos mencionados en la Tabla1, cuatro de las Divisiones solo cuenta con dos de los puntos, tres de las Divisiones cuenta con solo tres de los puntos mencionados y una División tiene cuatro de los puntos mencionados en la Tabla1. Un aspecto importante es que dos de las áreas entrevistadas no cuentan con los manuales actualizados.

Los seguros, convenios y garantías no se incluyeron dentro de esta descripción, ya que todas las Divisiones y Secretarías desconoce sobre los seguros, qué garantías se tiene y solo una división confirmo que no tiene convenios, sin embargo, existe un área dentro de la FI donde se cuenta con dicha información.

- *Equipo auxiliar:* En todas las Secretarías y Divisiones, cuentan con elementos complementarios al equipo de cómputo, tal como el aire acondicionado, equipo contra incendios, dispositivos de seguridad, etc.

- *Otros:* papel, formas previamente impresas, etc.

2.2.2 Requerimientos operativos mínimos

La mayoría de las dependencias entrevistadas, coincidieron con la siguiente lista de recursos operativos mínimos:

a) Usuarios: Enumeración y descripción de los usuarios del equipo de cómputo a su cargo.

b) Personal: quiénes son responsables de los servicios de cómputo en caso de una contingencia. Como se observo en el punto de documentación, las Secretarías y Divisiones no cuentan con manuales que puedan ayudar en caso de que el personal no se encuentre en el área o bien no están actualizados; esto trae como consecuencia que la solución al problema tarde mas de lo previsto.

c) Requerimientos de ejecución: Se refiere al tiempo de ejecución, fechas criticas, características del CPU, espacio en disco que requieren las aplicaciones, memoria principal, comunicaciones y redes.

d) Datos: archivos con información de la dependencia, espacio en disco necesario para almacenar estos archivos.

e) Software: Sistemas operativos y en general cualquier software de aplicación que sea necesario en la operación normal de la dependencia.

f) Equipo de respaldo: Diez de las áreas en la Facultad tienen solo el equipo necesario para descargar el trabajo cotidiano, por lo tanto no cuentan con la capacidad de tener hardware de respaldo que pueda servirles como apoyo en caso de ocurrir alguna emergencia. Las dos Secretarías que cuentan con equipos de respaldo, solo pueden disponer de él durante un periodo corto de tiempo.

g) Otros: se refiere a hardware complementario –p. e. impresoras–, insumos, requerimientos de comunicación de datos, etc.

2.3 Identificación de posibles causales de Contingencias dentro de la Facultad de Ingeniería

La identificación de posibles contingencias que pudiesen ocurrir dentro de la Facultad de Ingeniería, se basa principalmente en las experiencias de las personas que laboran en ella, en virtud de que dichas personas son las que han visto de cerca las situaciones que han puesto en riesgo la correcta operatividad de la Facultad, e incluso han colaborado en la restauración de las condiciones normales y han adoptado medidas de seguridad para evitar la recurrencia de dichas situaciones no previstas.

Por esta razón, se llevó a cabo un análisis a priori de las situaciones expuestas en el párrafo anterior; dicho análisis se basó en la aplicación y evaluación de una entrevista dirigida a los representantes de área ante el Comité de Computo de la FI y en la cual se les formuló una serie de preguntas sobre temas relacionados con seguridad informática y recursos con lo que cuenta cada División o Secretaría dentro de la FI; además se les preguntó a los participantes de la entrevista sobre las situaciones que han afrontado para permitir la correcta operación y función de los recursos informáticos dentro de su correspondiente área.

Un resumen de los resultados de la citada entrevista se plasman en el cuadro 2.A, donde se muestra el número de lugares donde se presentaron los problemas comunes detectados dentro de las 12 Secretarías y Divisiones entrevistadas.

Nótese la alta incidencia de hechos como robo de equipo, vulnerabilidades físicas, ataques causados por virus e intromisiones a través de la red.

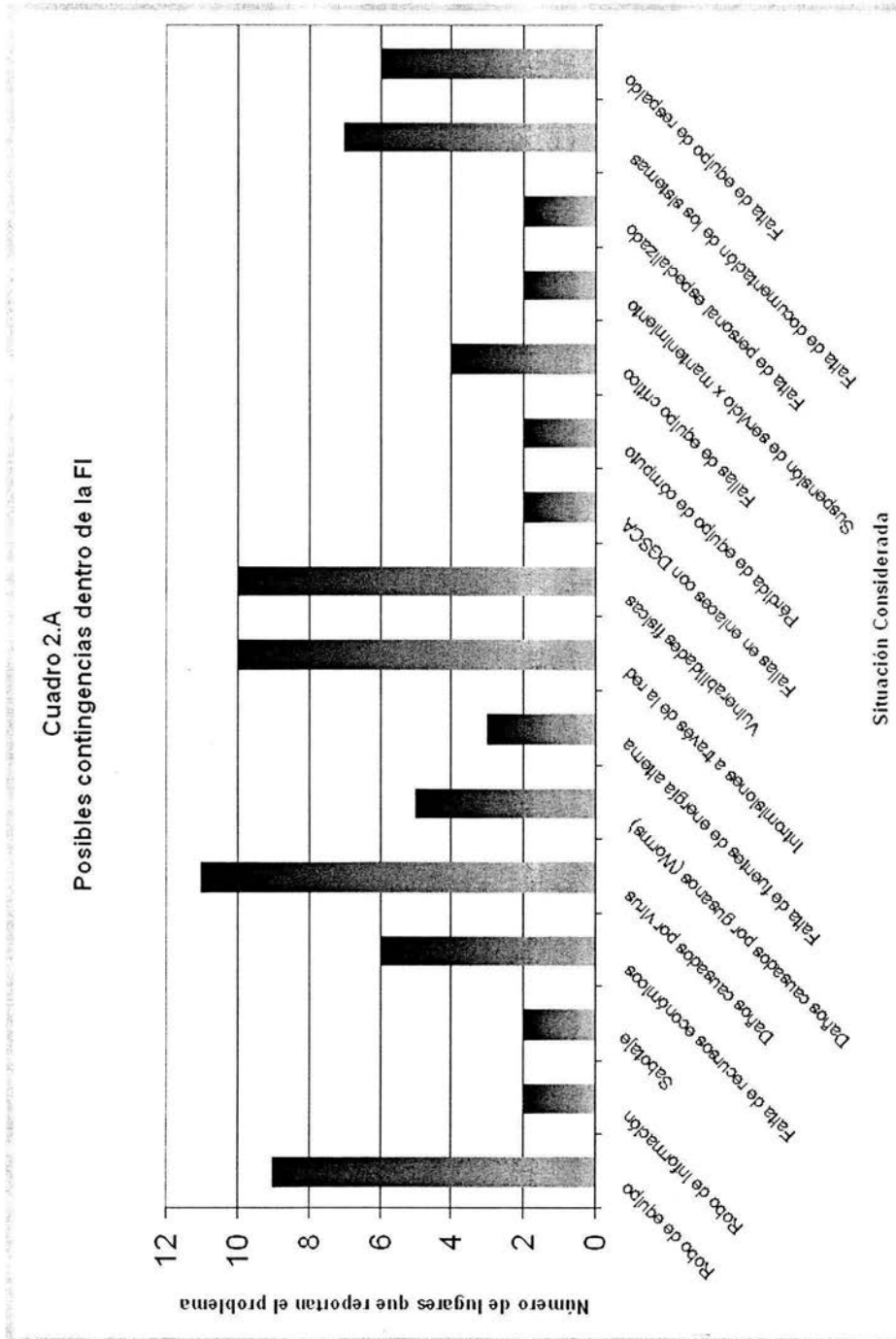
Las situaciones consideradas dentro de la entrevista, se describen en los siguientes apartados, agrupados como contingencias físicas y contingencias informáticas con un breve resumen de las observaciones mas notables hechas por los expertos. En el caso de contingencias físicas no se observó ningún hecho producido por desastres naturales, tales como terremotos o inundaciones, no obstante nuestro estudio deberá considerar estos aspectos como medida de prevención.

2.3.1 Contingencias Físicas: Las contingencias físicas que según nuestra encuesta ha enfrentado el personal de las diferentes áreas de la FI se resumen a continuación:

- Robo de equipo: En nueve de las áreas, esta situación ocurre por vulnerabilidades físicas, como son el no contar con protecciones antirrobo (cerraduras, alarmas, etc.) adecuadas o la mala utilización de éstas (omisión en el uso); además los entrevistados plantearon la posibilidad de que terceras personas cuenten con accesos al lugar donde se encuentra el equipo.

- Robo de información: Existe cierto tipo de información que produce y custodia la FI, la cual no es solamente útil para la institución si no para terceras personas, y en algunas ocasiones dicha información ha sido retirada por personal con acceso a la misma ya sea por beneficio propio o simplemente por causar daños a la Facultad. En este caso se involucra nuevamente el concepto de vulnerabilidad física.

Cuadro 2.A
Posibles contingencias dentro de la FI



- Vulnerabilidad Física: Siendo la FI una institución de carácter educativo y debido a la gran extensión de sus instalaciones resulta difícil restringir el acceso a las áreas que la conforman, incluso en las que se efectúan procesos importantes para la operación de la misma, tal es el caso de los sitios donde se encuentra el equipo de cómputo, donde muchas veces no se cuenta con las medidas de seguridad necesarias y se vuelven sitios vulnerables.

- Pérdidas o daños en el equipo de cómputo: Estos comentarios del personal entrevistado, se refieren al equipo dañado en forma incidental, el daño no solo se refiere a la pérdida física de los dispositivos en si, esta descripción se extiende incluso a la información contenida en el equipo dañado; según los resultados de la encuesta, en la mayoría de los casos no se cuenta con seguros que protejan contra este tipo de pérdida.

- Sabotaje: Este tipo de acciones generalmente obedecen a represalias tomadas por personas resentidas contra la FI –y que incluso forman parte de su plantilla laboral–, y que se reflejan en daños contra el equipo de cómputo o la información contenida en éste. Aunque no es una acción común, dos de las áreas encuestadas reportaron acciones de sabotaje en contra de ellas.

Consideramos prudente englobar en esta lista, algunas situaciones –la mayoría de índole económico– que si bien no se pueden considerar como una contingencia, pueden provocar percances en la operación informática de la FI, y que fueron reportados con frecuencia por el personal encuestado:

- Retrasos en la planeación general: La carencia de un recurso a causa del retraso de su adquisición, la cual haya sido programada anteriormente, presenta problemas constantes dentro de todas las áreas de la FI y los obliga a sustituir la operación del equipo esperado con los recursos que posean en ese momento.

- Suspensión de los servicios de cómputo por mantenimiento: El mantenimiento preventivo del equipo de cómputo es una acción necesaria para el buen funcionamiento de éste y para evitar posteriores fallas de mayor magnitud; sin embargo, la aplicación regular de estos mantenimientos puede llegar a retrasar la operación de algunos sistemas a cargo de la FI.

- Falta de recursos humanos para respaldar las actividades del personal especializado: Se refiere a la falta de personal que conozca y pueda desempeñar las funciones de los elementos capacitados para una tarea

específica y solo encomendada a dichas personas, este punto cobra relevancia durante la ausencia de la persona en cuestión, otorgándole a este un grado de "indispensable".

- Falta de documentación de los sistemas: Se enfoca a los documentos relacionados con el mantenimiento y operación de los sistemas del área y que puedan ser de utilidad en ausencia del personal a cargo de los mismos o para la capacitación del personal que sean designado para la operación y mantenimiento de dichos sistemas.

- Equipo de respaldo y operación alternativa: El personal entrevistado está conciente de la necesidad de contar con equipo de cómputo donde se pueda operar de forma alterna, sin embargo, implementar este tipo de medidas es muy difícil debido a la falta de recursos dentro de la FI.

- Fuente de energía alterna: La FI no se cuenta con una fuente alterna de energía eléctrica que permita la continuidad de la operación de los sistemas informáticos en caso que el suministro de energía sea suspendido; la mayoría de la divisiones y secretarias tienen como alternativa los acumuladores de energía (*No-breaks*), que proporcionan suministro de energía por tiempo limitado, suficiente solamente para respaldar información e interrumpir la operación adecuadamente.

2.3.2 Contingencias Informáticas: Las contingencias informáticas reportadas dentro de nuestra entrevista por el personal de las diferentes áreas de la FI se resumen a continuación:

- Ataques causados por Virus y Gusanos (Worms): Esta fue una de las contingencias reportadas comúnmente dentro de la entrevista, con una incidencia del 92%. Cabe señalar que este tipo de ataque suelen ser cada vez mas agresivos y dañinos y pueden provocar una pérdida total del equipo y / o de la información que custodian.

- Intromisiones a través de la red: También un evento reportado como de alta incidencia; dentro de la Facultad es una situación generalizada, a pesar de que solo se han reportado estos actos como medio para acceder a otros sitios, esto no exenta la posibilidad de un ataque dirigido a la FI.

- Falla en los servicios de comunicación externa (Servicios de DGSCA): Se refiere a los servicios de telecomunicaciones que presta la Dirección General de Servicios de Cómputo Académico a otras dependencias de la UNAM y de la cual la FI es usuario. Este tipo de incidentes fue reportado como de muy baja frecuencia, solo dos Divisiones la reportaron.

- Falla de proceso: En este tipo de incidentes, los periodos de interrupción durante la restauración de la operatividad pueden ser prolongados, los daños causados sobre el equipo suelen no ser permanentes pero pueden desembocar en perdida o corrupción de información.

- Perdida total de Equipo e información: Este punto se refiere a equipo que fue dañado accidental o con un propósito de daño, al igual que la información contenida en él y que por diversas razones no puedo ser recuperado.

2.3.3 Medidas de seguridad informática Implementadas actualmente dentro de la FI

Según la información aportada por los resultados de nuestra entrevista, existe actualmente un documento donde están plasmadas las políticas de seguridad informática aprobadas por el Comité Asesor de Cómputo de la Facultad de Ingeniería.

Se pretende que la mayoría de las políticas mencionadas se encuentren implementadas en las Secretarías y Divisiones de la Facultad a través de reglamentos internos, sin embargo, debido a que el Comité de Cómputo no había contemplado anteriormente la existencia de un Plan de Contingencias Informática, ninguna de las Secretarías y Divisiones cuenta con dicho plan o algún documento similar a éste.

Algunas de las medidas de seguridad informática ya implementadas en las Secretarías y Divisiones, se mencionan a continuación[2]:

- *Seguridad física:* En todos los casos se limita al resguardo convencional del equipo de cómputo (candados, chapas y ventanas de seguridad) y –en tres casos– alarmas, cámaras de video y vigilancia en los accesos, entre otros. La responsabilidad que tiene asignado el personal con respecto al equipo de cómputo asignado sirve de aliciente para acatar las medidas de seguridad física sobre el mismo.

- *Gestión de cuentas de acceso y contraseñas:* Solo el personal autorizado podrá otorgar permisos sobre las cuentas y contraseñas de acceso a los equipos de cómputo enlazados de la FI, esta tarea generalmente es asignado al administrador de red. Las contraseñas constituyen la primordial –y tal vez única– forma de autenticación y la única línea de defensa contra ataques externos. La asignación de contraseñas y las recomendaciones

[2] Para ampliar la información relacionada con las medidas de seguridad informática implantadas dentro de la Facultad, se recomienda revisar el apartado de políticas de seguridad informática, que encuentra en el PIDI de la FI.

sobre su conformación son también responsabilidad del administrador de la red.

- *Respaldos de Información en medios magnéticos:* En todos los casos, el administrador del sistema es responsable de realizar los respaldos de la información critica, la frecuencia de respaldo varía según los criterios de la división que la realiza y la criticidad de la información.

- *Normatividad Interna:* Se refiere a las métricas y lineamientos bajo los cuales se permite el uso del equipo de cómputo a los usuarios; Involucra tópicos como el uso adecuado del equipo de cómputo, cuentas y contraseñas asignadas, servicios de correo electrónico e Internet, etc., así como las sanciones correspondientes a los incumplimientos de dichas normas.

- *Administración de direcciones "Internet Protocol" (IP) :* Cada administrador de red cuenta con un registro de direcciones IP que ninguna otra División o Secretaría puede utilizar, es decir, no se permiten las direcciones homologas.

2.4 Evaluación de Resultados

Los resultados de la entrevista, nos permitieron obtener las siguientes evaluaciones, las cuales servirán como un antecedente para la siguiente parte de nuestro trabajo:

1) Las situaciones de contingencia catalogadas como desastrosas no fueron reportadas en ningún caso por el personal entrevistado y no se tiene documentada ninguna eventualidad por fenómenos naturales tales como terremotos, inundaciones, etc.

2) La mayor incidencia con respecto a situaciones de contingencia informática fueron provocadas por virus informáticos, ataques deliberados y sabotajes contra las dependencias de la FI, situación que puede preverse debido a la gran apertura que hay dentro de la FI, y en general en toda la UNAM en su carácter de Institución Educativa.

3) Al contrario de nuestras suposiciones iniciales, el mayor número de vicisitudes giró en torno de contingencias físicas, muchas de ellas causadas por vulnerabilidad de los sitios de operación.

4) Con las entrevistas realizadas a los expertos, el inventario de recursos tecnológicos y requerimientos operativos mínimos, nos permitieron determinar los efectos de estar fuera de línea y su relación con diferentes lapsos de permanencia en dicho estado. Para ello se considero lo siguiente:

- No existe equipo de respaldo en todas las dependencias
- Todas las Secretarías y Divisiones trabajan con lo mínimo
- No existe posibilidad de tener un lugar alterno en caso de ocurrir alguna contingencia física grave que obligue a cambiar de lugar el equipo de cómputo o la información.
- No existe fuente de energía alterna
- La documentación del centro de cómputo no esta completa o actualizada o simplemente no existe
- Faltan recursos económicos
- Todas las Secretarías y Divisiones reportaron como grave la suspensión de cualquiera de los sistemas

Con base en lo anterior y lo reportado sobre contingencias en las entrevistas, se plantearon escenarios:

- Si existe suspensión del servicio de energía eléctrica, con ayuda de los No-Breaks solo pueden respaldar la información o interrumpir adecuadamente la operación, sin embargo, después de una hora la Facultad se paraliza, ya que es el tiempo máximo de energía que proporciona el No-breaks.
- Si existe sabotaje en un área determinada y es necesario la suspensión de los sistemas, solo afectara a esa área determinada de la Facultad.
- Si existe robo de equipo con la Información o simplemente la información, dependerá de la importancia de esta, puede afectar desde terceras personas hasta un área especifica.
- En cuanto a la suspensión por mantenimiento, puede estar desactivado por 12 horas, considerando un aviso previo y realizando el mantenimiento en fin de semana.

5) Con el punto anterior y con los resultados de las entrevistas donde nos proporcionaron el tiempo de suspensión de los sistemas, a continuación se presenta:

Causa de la suspensión	Tiempo (h)
Mantenimiento	12
Robo de información / sabotaje	9
Falta de suministro eléctrico	4
Impedimento de acceso al área de trabajo	12 *
Otros	3

Es importante mencionar que una huelga pueden ser días e incluso meses.

6) El anterior punto nos permitió determinar el tiempo máximo permitido que un recurso puede estar deshabilitado antes de que esta situación altere o

inhiba la ejecución de una función esencial, donde, el tiempo máximo es 2 horas.

7) El no restablecer el sistema pronto, puede afectar notablemente no solo las actividades de los usuarios, implica también perdida de información.

8) El no tener personal capacitado en el área correspondiente, puede causar daños a la información y al equipo, teniendo perdida total, además, puede ser equipo irrecuperable.

9) A partir de la entrevistas realizadas se formularon dos cuestionarios más, los cuales se aplicaron a los expertos en informática de cada una de las áreas de la FI, estos cuestionarios se pueden consultar en el apéndice D y fueron de gran utilidad en la elaboración del Plan de contingencias. Los resultados de ellos se presentan en el siguiente capitulo.

3. ELABORACIÓN DEL PLAN DE CONTINGENCIAS

3.1 Introducción

La elaboración de un plan de contingencias es la fase definitiva en el proceso de establecer un programa de planeación de contingencias coherente. El plan deberá contener roles detallados, responsabilidades, grupos de trabajo y procedimientos asociados con la restauración de los sistemas de información después de una interrupción.

El Plan de Contingencias deberá elaborarse con base en las necesidades de la organización en cuestión –en este caso la Facultad de Ingeniería y las unidades que la conforman– y sus requerimientos, y mas aún, es importante que cada una de las unidades adapte el esquema planteado a sus necesidades específicas. Es necesario que nuestro plan de contingencias combine la flexibilidad en su aplicación y el detalle en su elaboración; en común que los planes excesivamente detallados permitan un nivel de escalabilidad y versatilidad menor.

El objetivo primordial de este capítulo, es el esquematizar un plan de contingencias que contenga tópicos de seguridad útiles a la mayoría de las áreas que conforman la FI; para ello nos basaremos en un análisis previo de los requerimientos necesarios para un lograr plan adecuado a las necesidades de la FI. Este análisis incluye la utilización de un método cualitativo de predicción el cual se describe más adelante.

3.2 Ponderación de contingencias y posibles recursos

Con base en los resultados del análisis de impacto descrito en el capítulo anterior, se logró definir el universo de recursos y necesidades de las áreas de cómputo de la FI, los cuales son datos esenciales en la elaboración del Plan de Contingencias de la institución, en virtud de que éstos están basados en experiencias del personal que compone las áreas de cómputo de la FI.

El análisis de la citada información, junto con la utilización de una herramienta que nos permita conocer la opinión de los expertos en informática dentro de las áreas que componen a la FI, son un factor que nos permitirá realizar un Plan de Contingencias robusto y totalmente enfocado a las necesidades de la Institución. Para esto se consideró la utilización de un método de predicción, en virtud de que estas metodología permiten, con base en un análisis a priori de hechos, pronosticar los que podrían resultar importantes o relevantes en un lapso determinado.

3.2.1 Elección de Método de Predicción

La elección de un método de predicción, surge de la necesidad de contar con un instrumento que nos permita conocer los elementos que se deberán considerar como indispensables dentro de nuestro Plan de Contingencias; considerando que este plan deberá ser funcional para las áreas de la FI no obstante la flexibilidad que tenga éste para adaptarse a las necesidades de otras organizaciones.

3.2.1.1 Métodos de Predicción Cualitativos: Con base en la aseveración anterior, se consideró el uso de un método de predicción cualitativo, en virtud de que, a pesar de que son menos precisos que los métodos cuantitativos y su uso en general requiere de una considerable flexibilidad para satisfacer las necesidades de la situación, éstos se pueden utilizar cuando no existe un conjunto de datos históricos útiles en los cuales pueda basarse un análisis[1] –que es el caso del presente estudio.

Esta facilidad les ha permitido a los métodos cualitativos ser cada vez mas importantes y comenzar a formar parte de los esfuerzos de planeación de muchas organizaciones, a causa del esfuerzo de éstas de poder preactuar en respuesta a cambios futuros previsibles.

[1] Gallagher, Charles A. Métodos Cuantitativos para la Toma de Decisiones en Administración. Mc Graw Hill 1988. p 140, 141.

Los métodos cualitativos confían plenamente en el juicio de los expertos del tema en cuestión –en este caso, el criterio del personal encargado de procesos informáticos y que están más familiarizados con las contingencias mas comúnmente acaecidas en la FI.

Uno de los factores que puede hacer costosa la aplicación de este tipo de métodos es la consulta frecuente a dichos expertos; sin embargo, cabe señalar que desde un inicio se contó con el apoyo del personal encargado de procesos informáticos de la FI para el desarrollo de este proyecto por lo que el análisis de costos de aplicación[2] no fue considerado.

Se estudiaron las características de cuatro métodos de predicción cualitativos con el fin de elegir uno de ellos[3] y aplicarlo en nuestra investigación de campo; los métodos evaluados fueron:

a) Método de Consenso de Panel,
b) Método Delphi,
c) Método de Analogía Histórica y
d) Método de Investigación de Mercado,

siendo el *Método Delphi* el más adecuado para nuestros fines[4].

3.2.1.2 El Método Delphi: El método Delphi se vale de la aplicación de una serie de encuestas a un grupo de expertos aislados uno de otro con objeto de minimizar el efecto de presión social y otros efectos del comportamiento de pequeños grupos (en nuestro caso, los expertos son miembros del Comité de Computo de la FI.)

Igual que en todos los métodos de predicción cualitativos, no se basa en análisis de datos históricos sino, en este método en particular, en el criterio del panel de expertos.

No existe una estructura rígida para aplicar el Método Delphi, pero se propone la siguiente secuencia:

---

[2] James L. Riggs (1968) plantea la utilización del Análisis de Valor (*Value analysis*) que defiende la selección de técnicas conocidas para la reducción de costos en la aplicación de un proceso. Plantea al *Costo de Aplicación* como un tipo de valor económico y lo define como la suma del factores como el trabajo, materiales, gastos generales y otros costos requeridos para la obtención de un recurso.

[3] James L. Riggs (1968) propone que la selección del método a utilizar deberá basarse sólo en la comparación con otros métodos factibles.

[4] Los métodos de Consenso de Panel, Analogía Histórica y de investigación de mercado se describen en el apéndice C del presente trabajo.

1. Se contacta a los expertos conocedores del tema y se les pide que participen en el panel.

2. Se entrega un cuestionario a los miembros del panel y se les pide que den su opinión acerca del tema.

3. Se analizan las respuestas y se identifican las áreas en las que están de acuerdo y en las que difieren.

4. Se entrega el análisis resumido de todas las respuestas a los miembros del panel, se les pide que llenen de nueva cuenta los tópicos del cuestionario donde el nivel de acuerdo no fue satisfactorio y den sus razones respecto a las opiniones en las que difieren.

5. Se repite el proceso hasta que se estabilizan las respuestas.

El Método Delphi no necesariamente requiere llegar a un consenso. Mas bien el objetivo es obtener un número de opiniones que se haya reducido por la aplicación del Método y que la información obtenida sirva después para formular planes.

A pesar de sus limitaciones[5], el uso que le dan muchas organizaciones al Método Delphi sugiere que con frecuencia su potencial excede sus limitaciones.

Para una evaluación más objetiva y pronta de los resultados obtenidos en las encuestas a realizar, se sugirió una variante del Método Delphi llamada *Delphi Numérico,* en la cual se efectúa una agregación estadística de los resultados, los cuales son expresados como una calificación de aceptación del enunciado propuesto; la calificación otorgada al enunciado por el panel de expertos se identifica mediante el promedio o la media de las calificaciones y se mide el consenso a través de la dispersión (desviación estándar.)[6]

3.2.1.3 El Panel de Expertos: Para nuestra investigación de campo fue considerada la participación de un panel del doce expertos, miembros del Comité de Cómputo de la FI, a quienes se aplicó un cuestionario (y que se espera que las respuesta obtenidas estén basadas en la experiencia de dicho personal) dividido en 2 partes:

[5] El Método Delphi ha sido criticado por su poca seguridad, demasiada sensibilidad de los resultados a la ambigüedad de las preguntas, dificultad para establecer el grado de experiencia de los miembros del panel y por los retrasos generados entre las repeticiones del proceso de entrevista.

[6] Rowe G, Wright G & Bolger F (1991). "Delphi: A reevaluation of Research and Theory" en "Technological Forecasting and Social Change" Vol. 39, pp 235-251

a) en la primera parte se pide calificar, en grado de nocividad, una serie de eventos que podrían suscitarse en situaciones de contingencia;

b) en la segunda parte se pide calificar, en orden de Necesidad y de Factibilidad, ciertas acciones que podrían considerarse como tópicos dentro del Plan de Contingencias para la FI.

En las próximas secciones se plasman los resultados obtenidos.

3.2.2 Ponderación de Contingencias en Orden de Nocividad

La calificación de los eventos analizados en este punto, se realizó con base en los resultados obtenidos después que fuera aplicado nuestro cuestionario Delphi[7]; cabe mencionar que el nivel de acuerdo entre los expertos del panel obtenido en la primera aplicación del cuestionario fue muy bajo, por lo que fue considerada una segunda aplicación del mismo, en el cual nos enfocamos a los temas en los que no existió un nivel de acuerdo aceptable dentro del panel de expertos[8].

En el cuadro 3.A se presenta la evaluación de la primera aplicación[9]; se puede apreciar que en la mayoría de los casos existe un bajo nivel de acuerdo, basando esta aseveración en el nivel de dispersión (desviación estándar).

Siguiendo las métricas propuestas por el método Delphi, consideramos necesaria una segunda fase de aplicación de la encuesta, tomando en cuanta al mismo panel de expertos que intervino en la primera encuesta. Dicha información se plasma en el cuadro 3.B.

Según la información aportada por el cuadro 3.B, algunos rubros alcanzaron un nivel de acuerdo más razonable, por lo que pudieron ser calificados con mayor facilidad; no obstante se consideró necesario la utilización de otros parámetros de evaluación para resolver los rubros donde existían ambigüedades.

---

[7] En el apéndice D del presente trabajo se presenta una plantilla de cada uno de los cuestionarios aplicados al panel de expertos en esta fase.

[8] Cabe enfatizar la cualidad de Método Delphi que permite adaptar los cuestionarios subsecuentemente aplicados con el fin de poder enfocarlos a los hitos en los que el panel de expertos no pudo llegar al nivel de consenso deseado, haciendo hincapié en que el método Delphi no obliga al panel a llegar al consenso.

[9] Se pidió a los expertos del panel que evaluaran los resultados con números enteros del uno al cinco, con el fin de evitar una analogía con la notación académica de diez (o cien) puntos que pueda prestarse a confusión.

Cuadro 3.A: SITUACIONES DE CONTINGENCIA

Grado de nocividad **(siendo el número 1 el de menor peso y el 5 el de mayor peso)** de los eventos enumerados, los cuales podrían suscitarse como situaciones de contingencia:

SITUACION	Media (μ)	Desviación Estándar (σ)	Moda	Frecuencia Moda	Nivel de Acuerdo	Aceptada
a) Falta de suministro de energía eléctrica	3.67	1.56	5	6/12	Regular	?
b) Daños causados por virus	3.75	1.22	5	4/12	Regular	?
c) Pérdida Incidental de Información	3.73	1.14	3	6/12	Regular	?
d) Impedimento de acceso al área de trabajo	4.08	1.08	5	6/12	Alto	SI
e) Fallas de conectividad	3.08	1.38	3	3/12	Bajo	?
f)Pérdida de Servicios Externos (Teléfono, Internet, etc.)	3.17	1.47	3	3/12	Bajo	?
g) Ataques deliberados causados por externos	4.83	0.58	5	11/12	Alto	SI
Daños incidentales causados a:						
h) equipo de cómputo (PC's)	3.50	1.31	3	5/12	Regular	?
i) redes locales (LAN)	3.42	1.68	5	5/12	Bajo	?
j) equipo del SITE	3.67	1.56	5	5/12	Bajo	?
k) servidores (archivos, información, aplicaciones, etc.)	4.08	1.51	5	7/12	Regular	?
l) Ausencia del personal apto para tareas específicas	3.83	1.34	5	5/12	Regular	?
m) Robo de equipo	4.92	0.29	5	11/12	Alto	SI
n) Siniestros (Sismo, Incendio, etc.)	4.42	0.79	5	7/12	Alto	SI

Nota: Los resultados presentados están basados en una muestra de doce (12) encuestas

Cuadro 3.B: SITUACIONES DE CONTINGENCIA

Grado de nocividad **(siendo el número 1 el de menor peso y el 5 el de mayor peso)** de los eventos enumerados, los cuales podrían suscitarse como situaciones de contingencia:

SITUACION	Media (μ)	Desviación Estándar (σ)	Moda	Frecuencia Moda	Coeficiente de Variación (V)*	Nivel de Acuerdo	Aceptada
a) Falta de suministro de energía eléctrica	3.83	1.40	5	6/12	37%	Regular	NO
b) Daños causados por virus	4.00	1.21	5	5/12	30%	Regular	SI
c) Pérdida Incidental de Información	3.83	1.03	5	4/12	27%	Regular	SI
d) Impedimento de acceso al área de trabajo	4.08	1.08	5	6/12	27%	Alto	SI
e) Fallas de conectividad	3.58	0.90	3	5/12	25%	Regular	SI
f)Pérdida de Servicios Externos (Teléfono, Internet, etc.)	3.92	1.00	3	6/12	25%	Regular	SI
g) Ataques deliberados causados por externos	4.83	0.58	5	11/12	12%	Alto	SI
Daños incidentales causados a:							
h) equipo de cómputo (PC's)	3.42	1.16	3	4/12	34%	Regular	NO
i) redes locales (LAN)	3.50	1.45	5	4/12	41%	Bajo	NO
j) equipo del SITE	4.08	1.24	5	6/12	30%	Regular	SI
k) servidores (archivos, información, aplicaciones, etc.)	4.25	1.14	5	6/12	27%	Alto	SI
l) Ausencia del personal apto para tareas específicas	3.92	1.16	5	5/12	30%	Regular	SI
m) Robo de equipo	4.92	0.29	5	11/12	6%	Alto	SI
n) Siniestros (Sismo, Incendio, etc.)	4.42	0.79	5	7/12	18%	Alto	SI

Notas: Los resultados presentados están basados en una muestra de doce (12) encuestas
Los resultados corresponden a una segunda aplicación del cuestionario.
* Se incorpora un nuevo parámetro de decisión llamado coeficiente de variación (V)

Considerando que la desviación estándar es una medida de variación absoluta, es decir, mide la cantidad real de variación presente de un conjunto de datos y depende de la escala de medición, optamos por valernos de una medida de variación relativa como el Coeficiente de Variación[10], el cual representa la desviación estándar como un porcentaje de la media y se define como:

Coeficiente de variación (V) = (σ / μ) 100 %

Considerando los rubros aun no calificados, nos basamos en su coeficiente de variación y aprobamos aquellos que lo tenían menor o igual al 30 % (considerando que los rubros que tenían el nivel de acuerdo más elevado, contaban con un coeficiente de variación del 6% y 18% respectivamente).

Otro parámetro utilizado en la calificación de los datos fue su moda (y frecuencia de la misma), dato que nos permitió asignar una calificación más objetiva a los tópicos de nuestra encuesta.

Los resultados de esta segunda vuelta se presentan en el cuadro 3. B, donde se puede ver que solamente los incisos a), h) e i) obtuvieron una calificación no aprobatoria; esto descarta a los mencionados incisos de ser considerados dentro del Plan de Contingencias de la FI[11].

[10] Miller, Irwin. Probabilidad y Estadística para Ingenieros. Prentice Hall 1986. pp 172.

[11] No obstante que algunas medidas recomendadas para evitar el robo de equipo pudieran aplicar en las mediadas para evitar el daño intencional al equipo de cómputo.

3.2.3 Ponderación de posibles recursos en orden de Necesidad y Factibilidad

Al igual que la ponderación de contingencias en orden de nocividad, basamos la calificación de estos rubros en los resultados obtenidos por medio del cuestionario Delphi, resultados que se representan en el cuadro 3.C.

En referencia a este caso, el panel de expertos estuvo de acuerdo en que la mayoría de los recursos planteados son necesarios, no así acordaron en su grado de factibilidad, en el que se presentaros notorias diferencias entre las respuestas de los encuestados.

Es por esta razón que se planteo la necesidad de una segunda fase de aplicación del cuestionario, pero evaluando solamente el rubro referente a la factibilidad. Estos resultados se presentan en el siguiente cuadro.

No obstante que el nivel de acuerdo alcanzado en esta segunda fase sí fue notoriamente mayor con respecto a la primera fase, fue necesario recurrir a criterios de evaluación como la moda y el coeficiente de variación con el fin de justificar nuestra calificaciones de manera más sólida.

La última columna de los cuadros **3.B** y **3.D** nos muestra específicamente la evaluación otorgada a cada uno de los rubros evaluados y nos indica si el citado rubro será contemplado o no dentro del esquema de contingencias, objeto de este estudio.

CUADRO 3.C MEDIDAS PREVENTIVAS

Necesidad y Factibilidad, (**siendo el número 1 el de menor peso y el 5 el de mayor peso**) de la existencia de las acciones descritas que podrían considerarse medidas de seguridad ante situaciones de contingencia.

MEDIDA	NECESIDAD					FACTIBILIDAD					Acep-tado
	Media (μ)	Desv. Est. (σ)	Moda	Frec. Moda	Nivel de Acuerdo	Media (μ)	Desv. Est. (σ)	Moda	Frec. Moda	Nivel de Acuerdo	
a) Contar con personal de respaldo que pueda desempeñar funciones específicas designadas a una sola persona.	4.42	0.67	5	6/12	Alto	3.58	1.38	5	4/12	Bajo	?
b) Emitir manuales de operación lo suficientemente específicos para poder reemplazar las funciones de la persona encargada en caso de ausencia.	4.50	1.17	5	9/12	Alto	3.75	1.29	3	5/12	Regular	?
c) Promover la existencia de un plan de contingencias cuya elaboración, prueba y mantenimiento sean añadidos a las actividades de algunos elementos del personal.	4.17	1.11	5	7/12	Alto	4.00	1.13	5	6/12	Regular	?
d) Contar con reglamentos internos que castiguen los daños (tanto accidentales como deliberados) al equipo de cómputo de la dependencia.	4.17	1.53	5	8/12	Alto	2.75	1.66	1	4/12	Bajo	?
e) Organizar campañas que promuevan medidas de seguridad informática en la dependencia (respaldo de información personal, discreción en claves de acceso, etc.)	4.92	0.29	5	11/12	Alto	4.08	1.00	5	5/12	Regular	SI
f) Negociar convenios con los proveedores de servicios externos	3.83	1.27	4	5/12	Regular	3.00	1.28	4	4/12	Bajo	?
g) Contar con respaldos (medio óptico o magnético) de información crítica.	5.00	0.00	5	12/12	Alto	4.58	0.79	5	9/12	Alto	SI
h) Contar con servidores de respaldo en caso de pérdida o no operabilidad de los originales.	4.75	0.45	5	9/12	Alto	3.25	1.60	5	4/12	Bajo	?
i) Contar con un SITE alternativo en caso de pérdida o inaccesibilidad al mismo.	4.75	0.62	5	10/12	Alto	3.67	1.30	5	4/12	Bajo	?
j) Contar con generador independiente para suministro eléctrico.	4.50	1.17	5	9/12	Alto	3.08	1.78	5	4/12	Bajo	?
k) Contratar seguros que cubran la pérdida o robo de equipo de cómputo	4.25	1.22	5	8/12	Alto	3.08	1.31	3	5/12	Regular	?

CUADRO 3.D MEDIDAS PREVENTIVAS

Necesidad y Factibilidad, (**siendo el número 1 el de menor peso y el 5 el de mayor peso**) de la existencia de las acciones descritas que podrían considerarse medidas de seguridad ante situaciones de contingencia.

MEDIDA	FACTIBILIDAD						Aceptado
	Media (μ)	Desv. estándar (σ)	Moda	Frecuencia Moda	Coeficiente. de Variación (V)*	Nivel de Acuerdo	
a) Contar con personal de respaldo que pueda desempeñar funciones especificas designadas a una sola persona.	3.92	1.44	5	6/12	37%	Regular	SI
b) Emitir manuales de operación lo suficientemente específicos para poder reemplazar las funciones de la persona encargada en caso de ausencia.	4.08	1.31	5	7/12	32%	Alto	SI
c) Promover la existencia de un plan de contingencias cuya elaboración, prueba y mantenimiento sean añadidos a las actividades de algunos elementos del personal.	4.33	0.89	5	7/12	20%	Alto	SI
d) Contar con reglamentos internos que castiguen los daños (tanto accidentales como deliberados) al equipo de cómputo de la dependencia.	3.92	1.38	5	6/12	35%	Regular	SI
e) Organizar campañas que promuevan medidas de seguridad informática en la dependencia (respaldo de información personal, discreción en claves de acceso, etc)	4.08	1.00	5	5/12	24%	Alto	SI
f) Negociar convenios con los proveedores de servicios externos	3.08	1.51	4	4/12	49%	Bajo	NO
g) Contar con respaldos (medio óptico o magnético) de información crítica.	4.58	0.79	5	9/12	17%	Alto	SI
h) Contar con servidores de respaldo en caso de pérdida o no operabilidad de los originales.	3.33	1.72	5	5/12	52%	Bajo	NO
i) Contar con un SITE alternativo en caso de pérdida o inaccesibilidad al mismo.	3.25	1.42	3	4/12	44%	Bajo	NO
j) Contar con generador independiente para suministro eléctrico.	2.75	1.76	1	5/12	64%	Bajo	NO
k) Contratar seguros que cubran la pérdida o robo de equipo de cómputo	3.42	1.38	3	4/12	40%	Regular	SI

3.2.4 Adaptación de objetivos al Estándar ISO 17799 de Seguridad Informática

Uno de los objetivos del presente trabajo reside en que el Plan de Contingencias generado para la FI se apegue lo mas posible al cumplimiento de estándares internacionales de seguridad informática con el fin de que, si la facultad decide someterse a un proceso de certificación en el mencionado rubro, la adaptación del Plan de Contingencias no implique una tarea demasiado laboriosa. Cabe señalar que el objetivo de este trabajo no radica en la obtención de mencionada certificación.

Basamos nuestro estudio en uno de los estándares de seguridad informática más reconocidos a nivel internacional, dicho documento es emitido por la Organización Internacional para la Estandarización (ISO), y lleva por título: *INTERNATIONAL STANDARD ISO/IEC 17799 2000: Information Tecnology, code of Practice for Information Security management.*

Los aspectos más destacables de la adaptación de nuestro estudio al Estándar ISO 17799 se enumeran a continuación:

a) La encuesta realizada al personal miembro del Comité de Cómputo de la FI, confirmada por el análisis del cuestionario realizado al mismo sector (y avalado por el método Delphi) nos permitió determinar las contingencias en potencia dentro de la FI a través del consenso del panel entrevistado.

b) El esquema del Plan de Contingencias Informático de la FI fue escrito con el fin de ser adoptado por las Divisiones y Oficinas de la Facultad para que puedan mantener y restaurar la operación de sus sistemas en los lapsos de tiempo prudentes en caso de alguna interrupción o falla de los procesos críticos de dichas dependencias.

c) El esquema del Plan de Contingencias Informático de la FI explica las condiciones para su activación, así como los individuos responsables de llevar a cabo cada uno de los componentes del plan.

d) Se incluye un apartado especial donde se plantean metodologías de pruebas y consideraciones para el mantenimiento del mismo.

3.3 Plan de Contingencias Informático para la Facultad de Ingeniería

Plan de Contingencias Informático para la Facultad de Ingeniería

1. Introducción

El nivel de dependencia que tiene la Facultad de Ingeniería (FI) de los procesos informáticos utilizados para soportar su operación y gestión, así como de sus medios electrónicos de almacenamiento y transferencia de datos –los cuales se vuelven mas sofisticados de acuerdo al desarrollo tecnológico de los dispositivos electrónicos–, ha crecido de forma notable en los últimos años. Esta creciente dependencia trae como consecuencia el riesgo de perder temporal o definitivamente los servicios informáticos de la institución, ya sea de forma parcial o total, en el caso de que dichos dispositivos se estropeen, hecho que puede afectar seriamente e incluso colapsar la funcionalidad de la institución.

Es por esta razón que el personal que labora en la FI debe estar preparado para afrontar situaciones que puedan poner en riesgo la operación de sus procesos informáticos, independientemente de las medidas de seguridad preventivas implementadas para evitar la ocurrencia de sucesos no deseados; una planeación que permita reducir el impacto de los mencionados hechos dentro de la FI puede resultar vital, no obstante la complejidad involucrada para el lograr el cumplimiento de esta meta.

El presente documento propone la realización de un Plan de Contingencias Informático adecuado a las necesidades y recursos de la FI: definir sus alcances, desarrollo, medidas de implementación, métricas, actividades recomendables, actualización y mantenimiento, así como sugestiones acerca del personal necesario para la aplicación y gestión del mismo.

La elaboración de un Plan de Contingencias, es una tarea que atañe directamente a todo el Comité de Informática de la FI, en virtud de que cualquier hecho fortuito que afecte la operación de sus sistemas de cómputo requerirá de esfuerzos conjuntos para tratar de atenuar las consecuencias del mismo.

Cabe mencionar que el presente documento intenta adecuarse a las recomendaciones de la norma de seguridad informática: STANDARD ISO/IEC 17799 / 2000: *Information Tecnology, code of Practice for Information Security management*, la cual recomienda la existencia de un Plan de Contingencias como parte de las medidas de seguridad informática dentro de una organización.

2. Aspectos Generales

OBJETIVO GENERAL

El Plan de Contingencias Informático de la FI (PCIFI) tiene como objetivo fundamental, reducir –en un nivel razonable– el riesgo de la interrupción en el funcionamiento de los recursos y procesos informáticos de la FI a través de la implementación de una estrategia que permita la continuidad operativa de los procesos críticos de la Facultad –o la restauración de estos en un lapso mínimo–, la incorporación de procedimientos de respaldo y recuperación de información, coordinación con áreas de soporte y servicio y una administración de recursos humanos que fomente la documentación adecuada y el respaldo de las funciones del personal asignado a tareas críticas, entre otras actividades.

ALCANCES

Los alcances proyectados para el presente Plan de Contingencias se enumeran a continuación:

1) Identificar los procesos críticos de la FI y los recursos necesarios para soportar su operación,

2) proponer alternativas de operación de dichos procesos críticos en caso de contingencia,

3) proporcionar las métricas necesarias para asegurar que el personal y los recursos requeridos para la operación de los procesos informáticos de la FI estén disponibles tanto en la previsión y respuesta –en caso de contingencia–, como en las acciones que permitan la oportuna restauración de los servicios,

4) determinar la responsabilidad del personal designado para gestionar e intervenir en el esquema de contingencia, ya que en caso de existir alguna, dicho personal fungirá como soporte de las áreas afectadas que les hayan sido asignadas,

5) ser difundido en todas las áreas de la FI que tengan que ver con procesos informáticos y

6) responder de su gestión ante el Comité de Cómputo de la FI.

CARACTERÍSTICAS

Personal a quien va dirigido

El presente documento va dirigido de manera particular a todo el personal miembro del Comité de Cómputo de la FI y en general a todo el personal de la FI que soporte su operación parcial o totalmente con procesos informáticos y que esté interesado en la implementación de un Plan de Contingencias dentro de su área de trabajo.

Modo de Uso

Favor de utilizar este documento para conocer los aspectos inherentes a la planeación de la recuperación y / o continuidad de la operación de los procesos informáticos críticos de la FI después de una contingencia, así como un verificador de realización de las tareas previas involucradas y entrenamiento del personal. Su contenido se abrevia a continuación:

1. Breve Introducción al Plan de Contingencias Informático de la FI,
2. aspectos generales del mismo,
3. roles y responsabilidades del personal involucrado en el Esquema de Contingencias del citado plan,
4. plan de acción y tareas de recuperación a ejecutar en caso de contingencia dentro de la FI y
5. esquema de pruebas y mantenimiento del Plan de Contingencias.

Cabe señalar que en caso de una contingencia o desastre, la única sección de referencia obligatoria es la sección 4.

Distribución

Será responsabilidad del Coordinador del Comité de Informática, la distribución del presente documento entre los miembros del citado comité, quienes a su vez lo harán llegar a quienes según su criterio deban tener conocimiento de este tema y / o los candidatos a conformar equipos de trabajo o brigadas en situaciones de contingencia.

Postulados

El presente plan de contingencias se basa en los siguientes postulados o suposiciones:

1. Una situación que provoque una contingencia, se refiere a la afectación de la operación normal de los procesos en la FI, así como problemas de conectividad y servicio de transferencia de datos, ausencia de servicios (energía eléctrica, teléfono, Internet, etc.) o inaccesibilidad a los lugares de operación y / o ausencia del personal operativo de los procesos críticos; no necesariamente se refiere a una situación de "desastre" general (p. e. terremotos de 1985 en la Ciudad de México.)

2. El plan depende principalmente de la disponibilidad de los sitios de operación, ya sea principales o alternativos y de las políticas y acciones de respaldo de información crítica.

3. El acceso a los Sitios Operativos de cada una de las áreas, es considerado un requerimiento crítico.

4. El presente documento se ajusta a las necesidades y recursos de la FI; no obstante puede ser utilizado como referencia para el desarrollo e implementación de Planes de Contingencias de otras dependencias de la UNAM u organizaciones externas.

3. Personal Involucrado

Una situación de contingencia que paralice la operación de los recursos informáticos críticos del área es un hecho que atañe a todo el personal adscrito a dicha área por lo que es recomendable que todos los miembros del citado personal desempeñen alguna función dentro del esquema de contingencias y que dichas funciones sean incluidas en su programa de actividades cotidianas y que no sean consideradas como actividades extra-laborales o complementarias.

La obligatoriedad de estas funciones será determinada por los jefes de cada división o jefatura de la FI, en la medida que el Plan de Contingencias sea implementado.

Designación de Cargos: Se recomienda que los cargos correspondientes al cumplimiento del Plan de Contingencias sean asignados al personal del área, en función de sus conocimientos y se su disposición para aceptar las nuevas funciones.

CARGOS Y FUNCIONES

Los cargos propuestos para cubrir el esquema de contingencias se describen en los siguientes párrafos. En algunos casos se plantea solamente la extensión de funciones para cargos ya existentes –como en el caso del Coordinador del Comité de Cómputo de la FI–.

Coordinador del Plan de Contingencias (CPC): Este es el cargo mas importante dentro del esquema de contingencias para cada una de las áreas de la FI.

Se pretende que la persona que desempeñe el cargo de CPC cumpla con el objetivo de minimizar los efectos nocivos de una situación inesperada a través del cumplimiento de las siguientes tareas:

- Representar al personal que desempeña alguna función dentro del Plan de Contingencias correspondiente ante los jefes de División y de Oficina y ante el Comité de Computo de la FI.

- Coordinar la implementación de medidas preventivas que permitan acelerar la respuesta del personal del área ante una situación de contingencia.

- Verificar la continua actualización de respaldos de información y de sistemas así como la continua actualización de la documentación de los mismos.

- Conformar los grupos de trabajo contemplados dentro del Plan de Contingencias y colaborar en la asignación del personal a dichos grupos.

- Seleccionar y convocar al personal adecuado y necesario dada una situación de contingencias.

- Verificar la correcta aplicación de las fases del Plan de Contingencias cuando se requiera la aplicación del mismo. Apoyar las acciones necesarias para el cumplimiento de esta tarea.

- Mantener en operación la fase de soporte del Plan de Contingencias todo el tiempo que ésta sea requerida.

- Intervenir, junto con los directivos correspondientes en la toma de decisiones para cumplir cabalmente los objetivos del Plan de Contingencias durante una situación adversa.

- Participar en la búsqueda de medidas de operación alternativas emergentes en caso de que las acciones planeadas no sean suficientes para afrontar una situación fortuita.

- Gestionar y ejecutar, con ayuda de los CPC's de otras áreas, las medidas pertinentes, en el caso de situaciones de contingencia del alcance institucional.

- Participar en las negociaciones y acuerdos con los proveedores de servicios informáticos y en la adquisición de seguros de cobertura para éstos.

- Ejecutar y evaluar las pruebas de efectividad hechas sobre el Plan de Contingencias; documentar las mejoras obtenidas como resultado de dichas pruebas.

- Estar al tanto de las medidas de seguridad informática adoptadas en el área, promover la aplicación de éstas.

Se establece que se puede designar a varias personas que desempeñen el cargo de CPC dentro de una sola área, cada uno de ellos comisionado a acciones compatibles y que sean complementarias con las funciones de los demás CPC's, sin embargo, en los siguientes párrafos de este documento solo se hará referencia a un solo CPC.

Coordinador del Comité de Cómputo de la FI (CCC): Se recomienda la incorporación de las siguientes funciones al rol de actividades del CCC:

- Gestionar las labores de los CPC's de la FI; fomentar la comunicación entre ellos para intercambio de ideas en la implementación de los respectivos Planes de Contingencias.

- Difundir el esquema del Plan de Contingencias de la FI para que pueda ser adoptado por las distintas áreas de la misma –se recomienda el uso de Internet para cumplir con este fin–.

- Coordinar las acciones conjuntas de las divisiones y oficinas de la FI en materia de seguridad para prever y afrontar contingencias de índole institucional.

- Participar en la búsqueda de medidas de operación alternativas emergentes en caso de que las acciones planeadas no sean suficientes para afrontar una situación de contingencia.

- Asesorar a las divisiones y oficinas de la FI que quieran implementar un Plan de Contingencias Informático en su área –para cumplir este fin se recomienda recurrir a los autores del presente documento–.

- Realizar campañas cuyo objetivo sea promover la adopción del Plan de Contingencias dentro de las distintas áreas de la FI.

- Promover la aplicación de medidas de seguridad dentro de las Divisiones y oficinas de la FI.

Representantes de área ante el Comité de Cómputo de la FI: Debido a la frecuencia de las reuniones del CCFI y de las responsabilidades de sus integrantes, se propone que los representantes de las áreas ante dicho comité desempeñen las siguientes funciones:

- Suplir, cuando la situación lo amerite, al CPC como representante del personal asignado al Esquema de Contingencias ante el CCFI.

- Apoyar al CCC en la promoción del Plan de Contingencias Informático dentro de la FI.

- Intercambiar información con las personas del CCFI, sobre las medidas de seguridad, políticas, normatividad y esquema de sanciones implementados en otras áreas de la Facultad.

Grupos de Soporte Técnico (GST): Se encuentran divididos en 4 áreas según la disciplina en la cual se especialicen: Redes Lan, Bases de Datos y aplicaciones, Telecomunicaciones y Servidores. Dependiendo las necesidades de cada una de las áreas, y de los conocimientos del personal adscrito a los GST's, los miembros de dicho personal podrán pertenecer a tantos GST's quieran, o se los demanden.

Las funciones comunes a todos los GST's :

- Atender oportunamente a los llamados del CPC en caso de contingencia.
- Elaborar con el CPC y los demás GST's, la estrategia de recuperación adecuada para poder soportar la operación del área en caso de algún contratiempo.
- Compartir con los GST's equivalentes de otras áreas, información sobre las medidas implementadas referentes al Plan de Contingencias.

GST Redes LAN: Sus funciones dentro del esquema de contingencias:

- Dar mantenimiento preventivo y verificar periódicamente la conectividad del sitio principal de operación –y del alternativo si existiere–.
- En caso de que existan, custodiar las herramientas y el material de sustitución correspondiente, proveerlo en situaciones de contingencia y llevar un inventario del mismo.
- Implementar, cuando sea posible, enlaces redundantes en el sitio de operación.
- Poder aislar eficazmente aquel equipo de cómputo dañado con virus informáticos y que potencialmente pueda dañar el resto de la red LAN.
- Proponer y establecer esquemas de monitoreo para la red LAN de su área.

GST Bases de Datos y Aplicaciones: Sus funciones dentro del esquema de contingencias:

- Verificar periódicamente la correcta actualización de los respaldos de información, sistemas y aplicaciones en los sitios destinados para su almacenamiento.
- Probar que dichos respaldos se pueden restaurar exitosamente.

- Verificar que los equipos donde se requiera restaurar la información y / o las aplicaciones cuenten con la infraestructura necesaria para este fin (sistema operativo adecuado, manejadores de bases de datos, librerías dinámicas, etc.)

- Desarrollar Técnicas para la rápida restauración de la información en caso de contingencia.

- Proveer los respaldos de información pertinentes en una situación de contingencia.

GST Comunicaciones: Sus funciones dentro del esquema de contingencias:

- Coadyuvar al GST Redes LAN para reestablecer y mantener la total conectividad del sitio utilizado para la operación, si esta se llegara a perder.

- En caso de contar con un sitio alternativo, asegurarse que los servicios de telecomunicaciones puedan ser implementados en este sitio y si es posible, mantenerlos en activo.

- Negociar acuerdos de apoyo con los proveedores de servicios de comunicaciones (Internet, microondas, telefonía, etc.) para contar con su apoyo en caso de interrupción de los servicios.

GST Servidores: Sus funciones dentro del esquema de contingencias:

- Identificar cuáles servidores soportan información y / o aplicaciones críticas.

- Identificar el equipo de cómputo capaz de respaldar la operación de los servidores asignados en caso de ser necesario.

- Contar con la infraestructura necesaria en los servidores que han de fungir como alternativas para poder restaurar la operación lo mas pronto posible.

- Colaborar en la búsqueda de equipos emergentes para soportar la operación en caso de que las medidas adoptadas no sea suficientes para responder a una situación de contingencia.

- Mantener convenios con los proveedores del equipo de cómputo para contar con su apoyo en situaciones meritorias

- Mantener estrechos vínculos de comunicación con los proveedores de software –sistemas operativos, antivirus, etc.– para contar con las versiones mas actualizadas de los mismos y evitar vulnerabilidades en la operación.

4. Plan de Acción

El Plan de Acción es la parte mas importante dentro del Plan de Contingencias Informático.

En éste se encuentran descritas todas las acciones, sugerencias y consideraciones, la cuales –aplicadas correctamente en cada una de las divisiones y oficinas de la FI– ayudaran a conformar un esquema que permita hacer frente a situaciones no pronosticadas y que amenacen con dañar la operación de las áreas informáticas de la Facultad.

El Plan de Acción está compuesto por cuatro fases, cuya aplicación dependerá del tipo y magnitud de las circunstancias que se estén enfrentando –salvo la fase preventiva, cuyas visión a priori le confiere una obligatoriedad casi inmediata–.

El encaminar esfuerzos al estudio e implementación de este Plan de Acción y dedicarle recursos, tanto humanos como tecnológicos, puede ayudarnos a prevenir situaciones lamentables.

FASE PREVENTIVA

Las acciones preventivas propuestas a continuación nos ayudarán a amortiguar los efectos de una situación de contingencia, siempre que sean implementadas adecuadamente.

Algunas de las medidas propuestas podrán parecer costosas e incluso inaccesibles, por lo que se hacen algunas recomendaciones para lograr un acercamiento con el esquema propuesto, recordando también que la inversión en recursos preventivos es mucho menos costosa que la no operatividad de nuestra área de trabajo.

Asignación de Prioridades

Cada una de las áreas de la FI deberá contar con un esquema ponderativo que les permita asignar una prioridad de recuperación –en grado de importancia– a los sistemas, aplicaciones e información que sea considerada primordial en la operación de su área y cuya falta pueda ser nociva para ésta y los objetivos que persigue.

Los sistemas, aplicaciones y datos que cumplan con las características anteriores serán designados como *críticos* y recibirán un tratamiento adicional especial que consiste en un análisis de los siguientes rubros.

- Análisis de Impacto: Un análisis a priori nos ayudará a determinar si un recurso se puede catalogar –o no– como crítico, bastará con preguntarnos qué impacto tiene la pérdida parcial o total de dicho recurso –o la incapacidad de acceso a éste– para el área y para la FI en general; este mismo análisis nos ayudará a determinar las medidas preventivas que se deberán tomar para proteger dicho recurso en caso de una contingencia.

- Tiempo permitido de interrupción: Este análisis nos permitirá conocer cuánto tiempo puede permanecer inoperante o inaccesible el recurso en cuestión sin que se vea reflejado un impacto negativo en nuestro operación. El poder determinar esta información junto con el esquema de pruebas del Plan de Contingencias Informático propuesto, nos permitirán poner en operación los recursos críticos, dentro de los lapsos de disrupción permitidos.

El análisis propuesto y su interacción con los demás puntos contemplados en este Plan de Contingencias Informático, nos servirán de guía para dar el tratamiento correcto a cada uno de los recursos considerados como críticos, con base en su correcta ponderación y prioridad de recuperación y con la premisa de no afectar –o afectar lo menos posible– la operatividad informática de la Facultad de Ingeniería.

Políticas de Respaldo

El Plan de Contingencias Informático de la Facultad de Ingeniería (PCIFI) considera la implementación políticas de respaldo de la información crítica para la institución; la implementación de políticas de respaldo nos permitirá llevar a cabo la recuperación de la información y será un factor que permita la recuperación operativa de nuestros sistemas de una forma mas rápida y efectiva.

Deben de tomarse en cuenta dentro de este esquema de respaldo, tanto los datos contenidos en servidores de información como en Computadoras Personales (PC's) del personal, en virtud de que un contingencia que puede no tener consecuencias graves para la institución en general, sí puede ser lamentable para una persona cuya PC fuere afectada.

No obstante que los recursos de la institución sean limitados, en la medida posible se deberá contar con respaldo de los equipo operativos, con los sistemas e información respectivos; mas adelante se citarán algunas recomendaciones para lograr este fin.

Políticas de Respaldo en Computadoras Personales: Las políticas y métricas propuestas para protección y respaldo de información contenida en Computadoras Personales son:

a) La seguridad de los equipos de cómputo personales es una responsabilidad compartida entre el equipo de trabajo asignado a cubrir este sector y de la persona que tenga asignado dicho equipo, en vista de que esta última puede ser la mas afectada por los daños provocados. El beneficiario deberá asegurarse de que las personas ajenas al área no pueda acceder fácilmente a su PC.

b) Se recomienda asignar a las personas perteneciente al área, una cantidad de espacio libre en un servidor de archivos con el fin de que puedan almacenar la información y los procesos que a su criterio considere crítica. La actualización de esta información se llevará a cabo frecuentemente y será responsabilidad de cada usuario del servidor de archivos.

c) Cada persona deberá respaldar su información critica en medios de almacenamiento magnético u óptico –discos flexibles o CD-ROM–. En caso de que el personal no cuente con unidad de escritura de CD-ROM, se recomienda habilitar una computadora que cuente con este servicio y establecer un calendario en donde se estipulen las fechas en las cuales el personal puede hacer uso de este servicio.

d) Los respaldos generados deberán de probarse intentando restaurar la información contenida en los mismos. De igual forma se pueden simular situaciones de contingencia donde se contemple la restauración de dichos respaldos.

e) Idealmente el personal deberá contar con 2 copias del material respaldado: una de ellas permanecerá en el área de operación normal y otro en el área de operación alternativa[1].

f) El Coordinador del Comité de Computo de la FI y los responsables del área de informática de cada dependencia deberá promover campañas en las que se aliente el respaldo periódico de la información y aplicaciones críticas; en las citadas campañas se denotarán los beneficios que acarrea el respaldo frecuente de las aplicaciones e información críticas y las facilidades para llevar a cabo esta acción.

g) Se recomienda el uso del servicio denominado *Disco Duro Virtual* que ofrecen algunos sitios de Internet, y en el que se puede almacenar

[1] Este tema será tratado mas adelante en esta misma sección

información personal en el servidor de archivos de dichos sitios; en muchos casos este servicio es gratuito –o muy accesible– y representa otra alternativa para el respaldo de información. Contacte a su proveedor de servicios Internet.

Políticas de Respaldo en Servidores de Datos y de Aplicaciones: Las métricas de protección y respaldo de Servidores de Datos y Servidores de aplicaciones se enumeran a continuación:

a) Se deberá analizar la criticidad de la información para determinar la periodicidad de respaldo de la misma; se recomienda que este análisis quede a cargo de los responsables de cada uno de los servidores y los usuarios de los datos y aplicaciones contenidos en ellos. Algunos ejemplos de periodicidad de respaldo pueden ser: respaldo de fin de día para la información crítica, y respaldos semanales o quincenales para la información que no es muy dinámica.

b) La información crítica deberá ser respaldada en medios ópticos (CD's) o magnéticos (cintas o discos), de los cuales se recomienda contar con dos copias, una de ellas será almacenada en un sitio de operación alternativo o en un lugar predeterminado para este fin.

c) Deberá verificarse la integridad de todos los respaldos generados restaurándolos en algún servidor de pruebas o un emulador del mismo. En caso de no contar con medios alternativos, se recomienda programar pruebas de restauración del servidor con base en los posibles periodos en que éste no sea utilizado.

d) En el caso de respaldo de aplicaciones se deberá verificar además el correcto funcionamiento de las mismas una vez restauradas y verificada su integridad; se recomienda respaldar conjuntamente la configuración de las mismas.

e) Se recomienda designar personal responsable de los respaldos resultantes con el fin de poder habilitar un almacén de respaldos y facilitar el control de los mismos.

f) Los medios de respaldo deberán contar con una etiqueta externa y un archivo de lectura (de preferencia un archivo de texto sin formato) donde se pueda consultar la siguiente información:

   - Oficina o dependencia propietaria de la información,
   - información contenida,
   - fecha de respaldo,

- archivos componentes,
- espacio ocupado en disco,
- persona responsable de realizar el respaldo,
- modo de restauración de información (en caso de que la información se encuentre compactada se deberá describir el método utilizado para compactar dicha información y, de ser posible, incluir el software de compactación)

g) Deberá existir un calendario que contenga las fechas en las que se llevaron a cabo los respaldos de información, con el fin de poder reciclar los medio de almacenamiento una vez que estos contengan datos obsoletos o redundantes.

Políticas de Respaldo de Funciones: Las políticas propuestas a continuación, cumplen con la finalidad de no interrumpir la operación de la dependencia por falta de recursos humanos específicos, o por funciones asignadas a un número limitado de personas y desconocidas para el resto de la dependencia:

a) El personal asignado a alguna función considerada como crítica dentro del área, deberá contar con otra persona que conozca –y pueda desempeñar– dichas funciones. Esta propuesta no solo es útil en caso de contingencia, si no en caso de ausencia, incapacidad e incluso asueto de la persona a cubrir.

b) Para lograr una mejor coordinación entre el personal asignado al respaldo de funciones, se propone un esquema semántico en el cual, el personal que forme parte de un grupo determinado, sirva de respaldo para las funciones del resto dicho grupo. La conformación de los grupos de trabajo se hará con base en las funciones desempeñadas, disponibilidad y conocimientos del personal del área.

c) Deberá existir un directorio actualizado en el cual aparezcan las personas asignadas a labores críticas; se recomienda que este directorio esté organizado según los grupos de trabajo existentes y que sea actualizado y distribuido de forma periódica dentro del área.

d) Las personas que operen y / o hayan colaborado en la realización de una aplicación considerada como crítica, deberán escribir y publicar un documento en el que se especifique lo siguiente:

- Descripción General de la aplicación,
- modo de operación de la aplicación,
- breve Nota Técnica y
- guía de solución de problemas comunes.

e) Deberán existir copias de los documentos elaborados, tanto en el Sitio de Operación Principal, como en el Sitio de Operación Alternativo; dichas copias deberán estar impresas y disponibles con el formato de algún procesador de texto estándar (p. e. Word para Windows)

El Sitio de Operación Alternativo

Se propone considerar las siguientes métricas en la implementación un Sitio de Operación Alternativo, el cual permitirá continuar con la operación de los sistemas críticos del área correspondiente, en el caso de algún percance en el sitio de operación principal:

El Stio de Operación Alternativo (Sitio Alternativo) deberá contar con la infraestructura mínima necesaria para mantener en operación los sistemas considerados como críticos, dado un escenario de contingencia; para esto, cada una de las áreas deberá llevar a cabo una evaluación que permita ponderar la importancia de los sistemas y módulos a su cargo, así como la factibilidad de alternativas de operación respondiéndose las siguientes preguntas:

- ¿Qué impacto tiene la interrupción de la operación del sistema para el área y para la FI?
- ¿Cuánto tiempo puede permanecer inoperante el sistema sin que se vea reflejado dicho impacto?
- ¿Los medios informáticos disponibles permiten la habilitación de recursos alternativos que permitan soportar la operación en caso de imprevistos? En caso contrario: ¿Es posible adquirir dichos medios y cuál es el costo de los mismos?
- ¿Cuáles dependencias de la FI, e incluso de la UNAM pueden brindarnos apoyo para habilitar un sitio alternativo y qué tan factible resultaría la interacción con las mismas?

Se considera la existencia de cuatro clases de sitios alternativos, cuyas características se describen a continuación[2]:

- Cold Site: Generalmente son sitios con espacio e infraestructura mínima – tal como energía eléctrica, comunicaciones básicas (teléfono, radios), etc.– adecuados para soportar la operación del área. Para poder habilitar la

[2] En la mayoría de las clases de Sitio Alternativo se conservaron los términos sajones proporcionados por el autor, al no encontrar una terminología adecuada para los mismos en el idioma español.

operación de este tipo de sitios se requiere el suministro de equipo de cómputo adecuado; estos sitios generalmente solo proporcionan un espacio alternativo donde trasladar el equipo de cómputo durante alguna eventualidad.

- Hot Site: Son espacios adecuados para soportar la operación del sistema en cualquier momento; cuentan con el hardware, infraestructura de comunicaciones, paquetería y respaldos de información necesarios para simular el ambiente de operación en poco tiempo.

- Warm Site: Es un punto intermedio entre un Cold Site y un Hot Site. Consiste en un espacio parcialmente adecuado para la operación de los sistemas del área, contando con algunos –e inclusive la mayoría– de los elementos de un Hot SIte; entre mayor similitud con éste último, se ocupará menos tiempo en adaptar el Warm Site para que sea funcional.

- Sitio Replicado: Es un sitio totalmente redundante y operativamente idéntico al Sitio Principal de Operación; cuenta con replicación de información en línea, infraestructura de telecomunicaciones completa y actualización de aplicaciones simultánea con el Sitio Principal. Esto sitios son la alternativa ideal para un esquema de contingencias ya que permiten el proceso y almacenamiento de información de manera idéntica al sitio principal.

La siguiente tabla resume las características de las clases de sitio alternativo descritas:

Sitio	Costo	Equipo y Hardware	Telecomunicaciones	Tiempo de Restauración
Cold Site	Bajo	Ninguno	Ninguno	Largo
Warm Site	Medio	Parciales	Parciales	Intermedio
Hot SIte	Medio / Alto	Completo	Completas	Corto
Replicado	Alto	Completo	Completas	Inmediato

Estando consientes de que los recursos destinados a situaciones de contingencia pudieran estar limitados a determinado presupuesto y que la puesta en marcha de un sitio alternativo resulta muy costosa, presentamos las siguientes acciones que podrían amortizar los costos de habilitación de un sitio alternativo.

a) Negociar y coordinar con otras dependencias de la FI y de la UNAM –que cuenten con una infraestructura similar– el mutuo alojamiento de sistemas críticos para ambas dependencias, argumentando los beneficios que se podrían obtener de dichos acuerdos. Algunas alternativas pueden ser la División de Educación Continua (Palacio de Minería) y el CEM Polanco.

b) En virtud de que la frecuencia de operación de algunos sistemas críticos es baja, e incluso esporádica –p. e. Inscripciones Semestrales–, se recomienda llevar cabo una programación de respaldos de los sistemas críticos en el sitio alternativo para aminorar la cantidad de recursos requeridos.

c) Es necesario mantenerse al tanto de las pólizas de seguro con que cuenta el equipo de cómputo del área, así como las condiciones de las mismas y el tiempo de respuesta estipulado por la compañía de seguros; en caso de no existir dichos servicios, se deberá promover la adquisición de éstos para el equipo de cómputo considerado como crítico.

d) Negociar con las empresas proveedoras de equipo de computo para que puedan proporcionar facilidades en caso de imposibilidad de acceso al equipo de cómputo crítico (préstamo o renta de equipos, etc.)

Los incisos c y d asumen la correcta aplicación de las políticas de respaldo y almacenamiento externo[3], considerando que una infraestructura con capacidad de operación no tiene ninguna utilidad si no se cuenta con la información y los sistemas que ésta soporta.

Plan de Acción dentro del Sitio Alternativo: Una vez que se cuente con un Sitio Alternativo, proponemos las siguientes acciones a seguir dentro del mismo:

a) El equipo de respaldo deberá contar con la misma configuración que los equipos principales, así como con una estructura de directorios similar donde se puedan instalar las aplicaciones y los datos necesarios; esta medida facilitará el mantenimiento y operación del Sitio Alternativo.

b) El acceso al Sitio Alternativo se coordinará a través de los responsables del área de computo y los representantes del área ante el comité de Informática. Se recomienda que cada persona involucrada en la coordinación del esquema de contingencias, cuente con llaves de acceso al Sitio Alternativo.

c) Una coordinación eficiente permitirá el registro del equipo existente dentro del Sitio Alternativo y las aplicaciones e información contenidos en él; dicho contenido dependerá de la capacidad de los equipos, recursos necesarios para las aplicaciones y el personal capacitado para la operación de los mismos, con el fin de hacer la operación del Sitio lo mas eficiente posible.

d) Se recomienda la utilización de un Servidor de Nombres (DNS) que se pueda dirigir al Sitio Alternativo con el fin de evitar configuraciones de tipo

[3] Este tema será tratado mas adelante en esta misma sección.

manual en las computadoras de respaldo. Se observa la necesidad de que una de las primeras tareas a realizar en caso de contingencia sea hacer los cambios necesarios en el DNS para que éste apunte al Sitio Alternativo.

e) Deberá existir un registro de versión de las aplicaciones instaladas en el Sitio Alternativo, con el fin de saber si éstas están debidamente actualizadas; de la misma manera se probará de forma periódica, la conectividad con el Sitio Alternativo y los equipos componentes. Los responsables del Sitio Alternativo promoverán la actualización periódica de las aplicaciones críticas –y las verificaciones de comunicación– y llevarán el control de las últimas versiones instaladas en dicho Sitio así como el estatus técnico del mismo.

Almacenamiento Externo: Un complemento necesario para las políticas de respaldo son las prácticas de almacenamiento de datos fuera del sitio de operación principal (Sitio Principal). Esto cumplen con la finalidad de proporcionar respaldos de datos y sistemas no obstante la inaccesibilidad o daño causado al Sitio Principal que impidan inclusive la recuperación de los medios de respaldo contenidos en él.

Las practicas sugeridas referentes al Almacenamiento Externo son:

a) Cada sitio alternativo deberá contar con respaldos actualizados de los datos y sistemas críticos, ya sea en las computadoras asignadas para sustitución y / o en medios ópticos o magnéticos

b) Los usuarios de PC's podrán decidir entre almacenar los respaldos de su información personal en los sitios alternativos y / o en los sitios que ellos consideren mas seguros, en virtud de que esta información está bajo su custodia.

c) Los encargados de los sistemas deberán programar la actualización de los respaldos en el Sitio Alternativo; dicha programación estará coordinada por los representantes de cada área ante el comité de informática, quienes además promoverán campañas para la continua actualización de respaldos.

d) La actualización de respaldos de los sistemas críticos en el Sitio Alternativo, deberá hacerse cada vez que se libere una nueva versión de los mismos.

e) En caso de que la información respaldada se encuentre compactada y / o codificada por algún tipo de software, los Sitios Alternativos deberán contar con la paquetería necesaria para restaurar la información al formato de operación original.

Consideraciones Preventivas para la Red de Área Local (red LAN)

Estas medidas preventivas, permitirán realizar reparaciones menores sobre la red LAN en caso de ser requeridas; a pesar de sus simplicidad, pueden ayudar a resolver eficazmente algunos problemas de conectividad de una red LAN sencilla:

a) Diagramas y Ubicación: Se recomienda contar con un diagrama general de la red LAN del área de trabajo en cuestión acompañado de un mapa de ubicación de elementos, con el fin de poder localizar y atender fallas de conectividad dentro de la misma red.

   El diagrama deberá contener la topología de red utilizada, los nodos con los que cuenta y los enlaces con otras redes LAN o WAN –y los puertos que permiten dichos enlaces–. El mapa de ubicación deberá permitirnos localizar con facilidad los elementos de la red LAN, tales como los dispositivos de conectividad, cableado estructurado, nodos, etc.

b) Materiales y Herramientas de Mantenimiento: Deseablemente, se contará con materiales y herramientas que permitan hacer restauraciones menores dentro de la red LAN, (p. e. un enlace punto-punto.) Las herramientas y materiales propuestos son:

   - Rollo de cable UTP nivel 5 (100 m aprox.)
   - Conectores RJ45
   - Pinzas especiales de ajuste
   - Herramienta de adaptación al "Patch Pannel "
   - Pinzas de corte

   También se recomienda la inclusión de un pequeño manual donde se explique la correcta conexión del cableado al "Patch Panel" y la adaptación de terminales RJ45. Este material podrá estar bajo custodia del encargado de operación de la red LAN.

c) Enlaces Redundantes: En el caso de los enlaces a través de fibra óptica (e incluso a través de UTP) se puede considerar la instalación de enlaces redundantes, los cuales puedan habilitarse en caso de perder la conexión punto a punto principal. La ruta del cableado de los enlaces redundantes, deberá ser distinta a la del enlace principal para disminuir la probabilidad de que ambos enlaces sean dañados.

d) Software de Monitoreo: Para reducir el tiempo en la detección de puntos de interrupción en la red LAN, podemos utilizar software de Monitoreo

(generalmente provisto por la empresa distribuidora de los dispositivos de red) el cual puede alertarnos acerca de fallas en la conectividad de la red LAN.

Sanciones

Contar con un esquema de sanciones sobre actos que atenten contra la correcta operación de nuestra área de informática, puede ayudar a prevenir daños sobre el equipo de cómputo. Las consideraciones planteadas a continuación no implican un objetivo de lucro, si no salvaguardar la integridad de nuestras áreas de trabajo y de la Facultad:

a) Se propone realizar campañas de difusión para que todo el personal que tenga acceso al sitio de cómputo sometido a políticas de esta índole, conozca puntualmente el esquema de sanciones.

b) Los daños causados sobre el equipo de cómputo pueden ser accidentales o deliberados; a pesar de que debe existir una sanción por daños accidentales, las sanciones por daños deliberados deberán ser notablemente mayores a las primeras.

c) Se debe considerar la reincidencia como un hecho grave dentro de las políticas restrictivas del área. Se recomienda llevar un registro del personal que incurra en actos dolosos, con el fin de detectar reincidencias.

d) Las sanciones a aplicar sobre hechos deliberados y reincidencias, deben ser tales que constituyan un verdadero escarmiento para la persona que cometió la falta; en especial en hechos que puedan desembocar en la interrupción de la operación o daño al equipo de cómputo.

Consideraciones Adicionales

Esta sección contempla los procedimientos de respaldo y de previsión de operación en sitio alternativo. La información aquí presentada, podrá ser de utilidad en la implementación de acciones de previsión de una contingencia informática y su utilidad puede no aplicar en todas las dependencias de la FI:

a) Estandarización de elementos en Computadoras Personales (PC's): El proceso de recuperación de este tipo de equipo será mucho mas fácil si existe una estandarización de Hardware, Software y Periféricos sobre todos los equipos del área, comenzando por la estandarización de sistema operativo y paquetería de uso general.

En caso de que las estandarización de configuración generalizada no sea posible, se propone la estandarización por grupos de trabajo o por modelo de PC. Así también, la estandarización de componentes de hardware, permitirá la rápida sustitución de dichos elementos en caso de que solamente un componente sea afectado.

b) Estandarización de elementos en Servidores: A pesar de que un esquema de estandarización de Hardware, Software y Periféricos resulta mas complicado en el caso de los servidores (a menos de que éstos sean del mismo tipo), se intentará la homogeneización de recursos informáticos, tales como protocolos de comunicación, software de compactación, servidor de nombres (DNS), e incluso la creación de una partición dentro de determinado equipo que emule la operación de otro servidor.

   Los elementos estandarizados en los servidores deberán estar descritos en la documentación de los mismos

c) Negociaciones y Convenios: Según las posibilidades del área, se deberán negociar convenios con los proveedores de servicios y / o equipo de cómputo, que estipulen qué apoyos pueden brindar los proveedores a la Facultad en caso de ocurrir alguna contingencia o algún desastre.

   En el caso de que ya existieran dichos convenios, el CPC investigará los alcances y características de dichos convenios, con el fin de poder hacerlos válidos en caso necesario.

d) Adquisición de Seguros: Se sugiere la adquisición de seguros que protejan la integridad equipo de cómputo considerado como crítico, el CPC o el personal designado, estudiarán la cobertura del seguro en cuestión y el procedimiento para hacerlo efectivo.

   Se recomienda también el estudio de las cláusulas estipuladas en el caso de que otras instancias ya hayan negociado la adquisición de dichos seguros.

e) Medidas de Seguridad: Cada uno de los sitios operativos deberá contar con extintores y botiquín debidamente habilitados para afrontar contingencias que puedan provocar daño físico, tanto al personal como al equipo de cómputo.

   Adicionalmente se deberán promover practicas preventivas dentro de los sitios operativos (p. e. evitar fumar dentro de los lugares de trabajo o evitar la sobrecarga de los contactos eléctricos)

FASE DE NOTIFICACIÓN / ACTIVACIÓN:

En esta fase se definen las primeras acciones a ser ejecutadas una vez que ha ocurrido la interrupción de la operación de un sistema o cuando una emergencia ha sido identificada y parece ser inminente.

El personal a cargo de la coordinación del plan de contingencias de cada área determinará el nivel al cual deberá ser escalada esta fase, en función de la magnitud del suceso ocurrido; una vez determinado el escalafón de la emergencia, esta fase debe ser puesta en marcha de forma casi sistemática para poder afrontar la situación lo mas pronto posible.

Procedimiento de Notificación: El proceso de notificación de una contingencia, cobra relevancia en función de la rapidez con la cual es ejecutado, en virtud de que esta fase es el detonador para la realización de las demás fases; mientras el personal de área no tenga conocimiento de la situación, nada podrá hacer para atenderla.

Consideraciones: Recomendamos considerar los siguientes aspectos en el proceso de notificación:

a) Una emergencia puede ser anunciada con cierto margen de anticipación. Por lo que entre mas tiempo nos podamos adelantar a ella y mas oportunamente sea activado el Plan, las consecuencias pueden ser menos graves (un ejemplo puede ser la alerta sísmica, la fecha probable de activación de un virus o un corte programando de energía eléctrica.)

b) Dependiendo de la magnitud y el tipo de contingencia, será el personal a ser notificado y requerido; preferentemente, esta labor será asignada al Coordinador del Plan de Contingencia (CPC) del área; también es recomendable designar diferentes grupos de trabajo adecuados para cada una de las contingencias previstas.

c) Cada uno de los sitios operativos deberá contar con un directorio periódicamente actualizado que permita la localización del personal requerido para cada una de las contingencias previstas. Dicho directorio deberá contemplar teléfonos de emergencia ya sea de dependencias de gobierno (bomberos, policía, luz y fuerza etc.) o de iniciativa privada (proveedores de servicios telefónicos, conectividad, antivirus, bases de datos, etc.) Se recomienda tener un contacto específico a quien se pueda plantear el problema de rápida.

d) El personal designado a tareas críticas deberá estar provisto de medios de comunicación inmediata sin caer en lo ostentoso; un pager para el personal

critico y un teléfono celular (alternativo a la línea telefónica) en el sitio de operación pueden ser mas que suficientes.

e) El personal operativo y de guardia deberán conocer perfectamente el esquema de notificación del Plan de Contingencias.

f) El personal miembro de los grupos de trabajo deberá conocer la ubicación de los sitios alternativos de operación.

Esquema de Notificación: A continuación se muestra un esquema del flujo de notificación al personal en caso de contingencias. Nótese que el CPC es una de las primeras personas que deberá ser notificada, de esta manera, él podrá determinar quiénes deberán ser puestos sobre aviso.

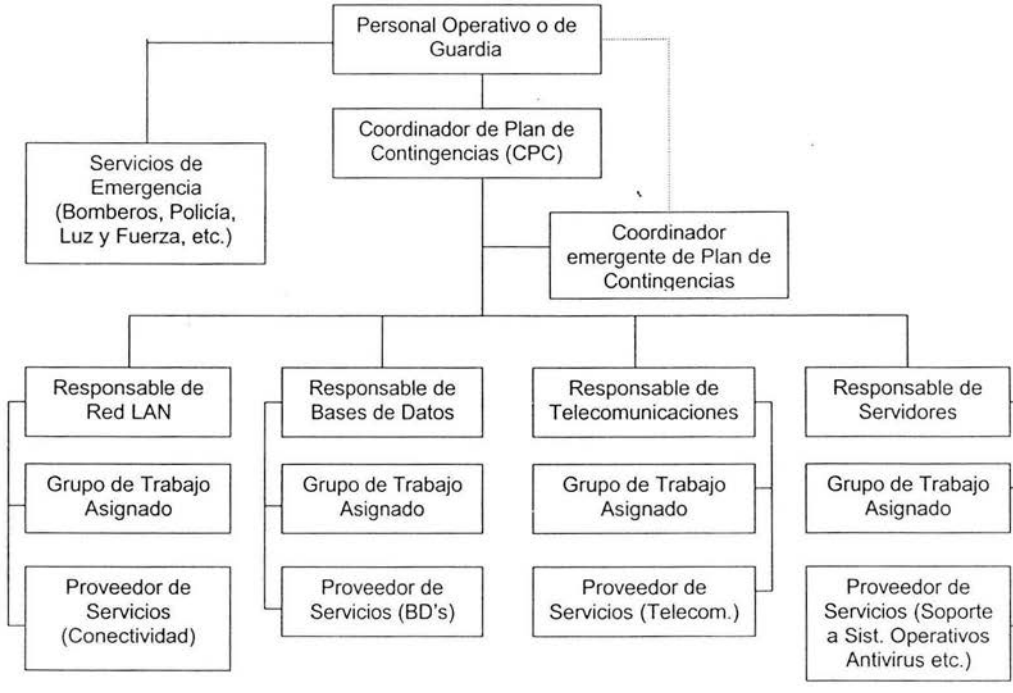


Diagrama IV.A: Esquema de Notificación de Contingencias

El diagrama IV.A muestra el esquema de notificación para una contingencia global, que involucre todos los aspectos operativos del área; dependiendo del tipo de problema que se esté enfrentando, el CPC podrá determinar cual sector del diagrama deberá ser convocado para poder afrontar la situación en cuestión.

Nótese que el responsable de cada uno de los servicios es quien deseablemente deberá contactar al proveedor de servicios correspondiente, sin embargo, en su ausencia, puede ser el Coordinador del Plan de Contingencia el encargado de esta tarea.

En vista de lo apremiante que resulta la ejecución de este procedimiento, recomendamos que el personal encargado de enterar al CPC, redacte una breve recapitulación del problema, la cual permita plantearlo de forma mas concisa al momento de ser requerida.

El recuento sugerido deberá incluir los siguientes puntos:

- Naturaleza del incidente ocurrido,
- fecha y hora aproximada de ocurrencia,
- personal lesionado o muerto (si fuera el caso),
- breve recuento de daños materiales (se debe dar prioridad a los bienes que resulten críticos para la continuidad de la operación, incluyendo la infraestructura),
- recuento de los sistemas dañados,
- medios de comunicación habilitados,
- de manera complementaria, el CPC determinará un sitio y horario tentativos de reunión.

Al momento de contactar al personal designado para hacer frente el problema, el CPC solamente deberá notificar de un status global del problema y del punto de reunión designado, éste último será, en orden de funcionalidad: el Sitio Principal, el Sitio Alternativo o algún otro sitio designado por el CPC (siempre y cuando los dos primeros sean totalmente inaccesibles.) Se toma esta medida para hacer la comunicación lo mas rápida posible.

Medios de Notificación: Una vez elegido el personal para afrontar la contingencia, el CPC se valdrá del cualquier medio de comunicación para contactar a éstos, siendo los mas recomendables (por cuestiones de rapidez) el teléfono, pager, celular o la notificación personal –se descarta el uso del correo electrónico por el tiempo estimado de respuesta por parte del contactado.

Procedimiento de Activación: Una vez reunido el personal necesario para afrontar la situación, el CPC deberá activar el Plan de Contingencias, tomando en cuenta los siguientes rubros:

Evaluación del sitio: El CPC, con colaboración del personal convocado, evaluará si el sitio de reunión cumple con los requisitos para hacer frente a la contingencia; se deberán contemplar aspectos tales como:

a) *Seguridad del personal*, la cual no deberá ponerse en riesgo a causa de la permanencia en el sitio designado.

b) *Accesibilidad al sitio,* la cual puede estar restringida por cuestiones de seguridad o en caso de que la contingencia sea de índole social (huelgas o paros), una contingencia de este tipo puede limitar las siguientes acciones del Plan de Contingencias sobre el sitio en cuestión si no se llega a algún acuerdo con los promotores de esta situación.

c) *Infraestructura de operación suficiente*, tal como servicios de electricidad, telefonía, conectividad, etc.

d) *Sistemas e Información requeridos*, considerando la correcta aplicación del esquema de respaldos.

Evaluación del estado actual: Los puntos a considerar en esta evaluación son:

- Cantidad y nivel de daño de los sistemas afectados: El nivel de daño de los sistemas y los recursos necesarios para su habilitación (respaldos de información, equipo de cómputo e infraestructura) puede ir desde niveles aceptables que permitan la operación de los mismos, hasta dejarlos totalmente inservibles.

- Nivel de criticidad de los mismos: De manera previa se deberá contar con un análisis de criticidad de los sistemas afectados; éste deberá ser realizado por un grupo conformado por el personal operador de los sistemas y coordinado por el CPC.

- Recursos Humanos Disponibles: El CPC decidirá si requiere apoyo adicional de otras áreas; el Coordinador del Comité de Cómputo de la FI puede servir como medio de comunicación para facilitar esta tarea.

- *Recursos Adicionales,* tales como liberación de nuevas versiones de antivirus o documentación técnica y operativa de los sistemas, en caso de ser requeridos.

Con base en las evaluaciones anteriores se podrá generar un cronograma de recuperación de la operación.

FASE DE RECUPERACIÓN:

Esta es la fase inmediatamente posterior a la notificación y activación del Plan de Contingencias. En este nivel, los daños ya deben haber sido evaluados, el personal involucrado deberá haber sido notificado de la situación (y en el mejor de las casos deberá estar en el punto de reunión) y los equipos deberán estar organizados según las tareas que desempeñarán.

Cabe señalar que dependiendo de la magnitud de la contingencia, puede requerirse el apoyo de servicios de emergencia e incluso su presencia puede ser indispensable[1]

Las actividades a desempeñar durante esta fase se enfocan en tomar medidas concretas para recuperar, aunque sea de manera temporal las capacidades de operación de los sistemas a cargo del área –en fases posteriores nos encargaremos de la rehabilitación total de la operación, incluyendo un análisis de las causas de la contingencia, y de ser posible la restauración total del sitio y de los recursos originales, de momento nos conformaremos con mantener latente la operación.

Al finalizar esta fase, los sistemas deberán ser operacionales y nos podremos valer de cualquier medio para conseguir este objetivo incluso las siguientes acciones:

a) Operación Manual Temporal de los sistemas y aplicaciones,

b) soporte y operación de los sistemas desde Sitios Alternativos e incluso

c) sustitución de la operación en sistemas y aplicaciones alternativos;

por lo expuesto anteriormente se asume que el equipo asignado a la atención de las contingencias deberá estar totalmente familiarizado con el desarrollo, soporte y operación de los sistemas y aplicaciones involucradas, así también el personal encargado de la infraestructura (telecomunicaciones, conectividad, telefonía, etc.)

Nuestra estrategia de recuperación involucra dos procedimientos básicos: el Procedimiento de Emergencia y el Procedimiento de Soporte, detallados a continuación.

[1] Se detalla mas adelante en los procedimientos de emergencia.

El personal designado a realizar tareas correspondientes a esta fase, deberá ser capaz de ejecutar las acciones de recuperación asignadas en el menor tiempo posible, este objetivo podrá cumplirse llevando a cabo las pruebas y mejoras pertinentes dentro del Plan de Contingencias (mismas que se plantean en apartados posteriores.)

Cabe aclarar que en caso de contar con el personal suficiente y si la situación lo amerita, estos procedimientos podrán ser ejecutados simultáneamente, es decir: un sector del personal disponible podrá dedicarse a salvaguardar la seguridad de los recursos (tanto humanos como materiales) en el sitio afectado, mientras el resto, destacado en el Sitio Alternativo, se dedicará a llevar a cabo el procedimiento de soporte con el objetivo de restaurar temporalmente la operación del área.

Procedimiento de Emergencia: Dependiendo de la magnitud de la situación que se esté enfrentado, el procedimiento de emergencia podrá tener el estatus de innecesario hasta indispensable (en un caso extremo será el único procedimiento que podrá ser ejecutado.)

El procedimiento de emergencia es el conjunto de acciones prioritarias a ser llevadas a cabo en caso de alguna eventualidad. En orden de prioridad, esta fase pretende el cumplimiento de los siguientes objetivos:

1) Rescate de vidas humanas: En caso de tratarse de alguna contingencia provocada por un desastre, no estaremos exentos de enfrentar una situación de rescate de personas; para esto (y en caso de que el personal del área no este capacitado para prestar este tipo de servicios) el personal del área se adecuará a las indicaciones y servicios de los cuerpos de rescate asignados para su apoyo.

2) Acceso al área de operación: Si la situación afecta directamente el sitio principal o el sitio designado para la operación (o alguno de los recursos considerados como críticos, ya sea equipo de cómputo o respaldos de información o aplicaciones) y el acceso al sitio está prohibido, el CPC o el personal que él designe, darán seguimiento al estatus del sitio hasta que el acceso a éste sea reestablecido.

   En caso necesario y en la medida de sus posibilidades, el personal del área se pondrá al servicio de los cuerpos de emergencia y de rescate.

   En el caso de que el impedimento de acceso al sitio sea por causa de una contingencia social (paros, huelgas, etc.) se deberá contactar a los directivos de la división (e incluso de la Facultad) para que designen al

personal adecuado para negociar el acceso al sitio con los activistas o que dichas negociaciones ayuden a mantener la integridad de las instalaciones y del equipo alojado.

3) Levantamiento de Recursos disponibles: Una vez reestablecido el acceso al área de operación afectada, el CPC, con ayuda del personal especializado, procederá a hacer un levantamiento para determinar el estado de los siguientes puntos:

   - El grado de daño del equipo operativo
   - El nivel de daño de la infraestructura necesaria para la operación.
   - El grado en que fue dañada o suspendida la operación de sistemas críticos.
   - La integridad de la información procesada o almacenada en dichos sistemas.
   - La capacidad de continuar operando en ese sitio o trasladar la operación a un sitio alternativo.
   - En caso de tratarse de un ataque producido por virus, evaluación del equipo afectado y probabilidad de transmisión hacia otros equipos.

4) Acciones Especiales: Se refieren a las acciones propias a la contingencia enfrentada, algunos ejemplos se plantean a continuación:

   - En caso de un ataque causado por virus, deberán aislarse los equipos que se encuentren infectados con el fin de evitar la propagación del mismo.
   - Si la contingencia consiste en intromisiones a la red interna del área, será primordial determinar cual equipo sirve como medio de acceso al intruso para evitar daños posteriores.
   - Solicitar la intervención de las autoridades competentes en caso de robo o impedimento de acceso a las instalaciones por razones de carácter social; en caso de ser necesario, se deberá presentar la denuncia correspondiente ante el ministerio público.

5) Determinación del tiempo de recuperación: Con base en los resultados del levantamiento del nivel de daño, el CPC podrá determinar el tiempo necesario para recuperar la operatividad de los sistemas críticos; esto dependerá de factores tales como:

   - Si la operación podrá ser restaurada en el sitio evaluado.
   - Si los procedimientos de soporte fueron habilitados simultáneamente en un Sitio Alternativo.
   - Si los servicios externos para continuar con la operación están habilitados de forma normal (electricidad, telecomunicaciones, conectividad, telefonía, etc.)
   - Si en el sitio se encuentra el personal necesario para habilitar nuevamente la operación.
   - Si se puede contar con apoyo de proveedores de recursos o servicios (p. e. provisión temporal de equipo, respuesta de las empresas aseguradoras o liberación de nuevas versiones en caso de proveedores de antivirus.)

   Cabe mencionar que este análisis se hará en el momento de la evaluación de los daños; debido a su importancia como punto de partida de las siguientes acciones del Plan, el CPC deberá supervisar personalmente este punto, para asegurar su rapidez y eficacia.

Consideraciones: Las siguientes consideraciones nos permitirán llevar a cabo los procedimientos de emergencia propuestos de forma eficaz:

a) Una vez determinado el tiempo de recuperación tentativo de los sistemas críticos, el CPC discernirá si es necesario el uso de un Sitio Alternativo para apoyar parcial o totalmente la operación de sistemas críticos. Los umbrales de tiempo para la toma de esta clase de decisiones deberán ser proporcionados por el personal operativo del área e inclusive por los directivos de las divisiones de la FI.

b) Las acciones planteadas dentro de este procedimiento, podrán variar dependiendo de la magnitud y tipo de contingencia, por ejemplo:

   En caso de daños en la operación causados por virus informáticos o por bloqueos provocados por activistas, es muy probable que la aplicación de los primeros tres pasos de este procedimiento no sea necesaria, y que la

recuperación de la operación pueda llevarse a cabo en el sitio principal sin mayor problema y que solo sea necesario determinar el tiempo de recuperación.

Sin embargo si los daños a la operación son provocados por una catástrofe (p. e. un incendio), la aplicación de los primeros tres pasos son de observancia casi obligatoria y el nivel de los daños puede ser tal que dependamos totalmente del Sitio Alternativo para intentar recuperar la operación de nuestros sistemas.

c) Se deberán verificar constantemente las causales de la situación de contingencia, para asegurar que éstas no sean recurrentes y puedan provocar otra situación similar en el mismo sitio, en un lapso corto de tiempo.

   En caso de ser necesario –y de ser posible–, se deberá contactar a las empresas proveedoras o a las empresas aseguradoras de la infraestructura y / o del equipo de cómputo dañado para hacer cumplir los convenios pactados con éstas. Esta consideración se extiende a los proveedores de software antivirus en espera de la liberación de versiones nuevas que ayuden a contrarrestar una situación de ataque provocado por nuevos virus informáticos.

   Se recomienda que una persona del área siga de cerca estas negociaciones para mantener al tanto al CPC y de esta forma incluirlas en la organización y el desempeño de las fases posteriores del Plan.

d) La recomendación del seguimiento de las negociaciones hecha en el inciso anterior, se extiende a los casos de paros laborales o huelgas, donde sea necesario negociar con los activistas el acceso a las instalaciones o la integridad de los recursos del sitio.

Procedimiento de Soporte: La importancia de la aplicación de este procedimiento, radica en la necesidad de mantener los sistemas críticos de la operación del área mientras es activada la fase de recuperación definitiva.

El principal objetivo de los procedimientos de soporte radica en recuperar la operación de los procesos informáticos críticos del área. Dicha recuperación se realizará en el Sitio Principal y /o en el Sitio Alternativo de Operación, dependiendo de la magnitud de los daños provocados por la contingencia y de los resultados de la evaluación hecha por el CPC en los procedimientos de emergencia.

A continuación se muestran las consideraciones generales sugeridas en la ejecución de estos procedimientos; posteriores a éstas, se muestran las consideraciones que atañen a cada uno de los sitios destinados a soportar la operación.

Consideraciones Generales: Aplican en cualquiera de los sitios de operación a utilizar.

a) En el caso de la recuperación de un sistema complejo en el que interactúen varios componentes independientes, los procesos de soporte deberán ser ejecutados en una secuencia que obedezca a las prioridades planteadas en las fases previas del Plan de Contingencias y al los tiempos que los sistemas puedan permanecer inoperantes.

b) Las tareas del Procedimiento de Soporte deberán escribirse a manera de lista de verificación de forma secuencial en orden de prioridad de restauración

c) Cuando el inciso anterior sea cumplido, se deberá obedecer a la lógica para la restauración de los sistemas críticos. Por ejemplo, en el caso de la recuperación de una red de área local (LAN) se comenzará con la restauración de servidores, equipo activo y cableado estructurado, y se dejará hasta el último la restauración de terminales de corta funcionalidad e impresoras.

d) Es muy probable que los GST's del área tengan un papel crucial en este procedimiento, el CPC se basará en el criterio de éstos para la toma de decisiones importantes a nivel técnico.

Soporte en el Sitio Principal: Con base en el estudio realizado dentro de la FI, las áreas que la integran difícilmente podrán contar con un sitio alternativo donde puedan soportar sin contratiempo la operación de los sistemas críticos que les corresponden, por lo que las consideraciones planteadas a continuación adquieren una importancia muy especial:

a) Una vez llevada a cabo la evaluación de los daños, tanto en el equipo de cómputo como en los sistemas y aplicaciones, el CPC con ayuda de los GST's "*Servidores*", "*Redes LAN*" y "*Comunicaciones*" deberán decidir si es necesaria la redirección de algunos sistemas o aplicaciones basándose en los posibles daños que pudiera sufrir el equipo que los alojare o la infraestructura que soporte la conectividad de dicho equipo.

Una vez detectada la necesidad de la redirección, la tarea primordial del GST "*Servidores*", será llevar a cabo los cambios necesarios en el DNS para operar sobre los nuevos equipos de soporte.

b) Para llevar a cabo la redirección del inciso anterior, también es necesario contar con los respaldos de la información y los sistemas realizados con anterioridad.

   En caso de que los respaldos alojados en el sitio principal hayan sufrido daños, se deberá contar con los respaldos alojados en el sitio alternativo o en el lugar designado para su almacenamiento, se considera tarea del GST "*Bases de Datos*" .

   La rapidez en la transportación de dichos respaldos, afectará directamente el tiempo de recuperación del sistema y la información, siendo el transporte físico solo una alternativa para hacer llegar esta información al sitio principal, se puede recurrir a la comunicación vía Internet o algún protocolo de transporte como el FTP.

   Los respaldos de información y de sistemas, también cobran una relevancia especial cuando la contingencia es provocada por inaccesibilidad al área de trabajo. La búsqueda de infraestructura y equipo de cómputo alternativo para soportar la operación, sería inútil sin la disponibilidad de los citados respaldos.

c) En el caso de ataque por virus sobre equipo considerado como crítico, una vez aislado el citado equipo, se deberá buscar el software antivirus correspondiente, y a la vez evaluar la posibilidad de sustituir dicho equipo de manera temporal para mantener la operación o esperar por el software antivirus, el tiempo de espera lo determinará la empresa proveedora de dicho software.

d) Dependiendo del tamaño y disposición de la red LAN, existen posibilidades reales de poder brindarle mantenimiento con el material adecuado (a cargo del GST's "*Redes LAN*"); estas posibilidades no se extienden tan fácilmente a las comunicaciones externas, (para las cuales en algunos casos hay que esperar por el apoyo de terceros). No obstante, podemos basarnos en los siguientes enunciados –que plantean ideas con una probabilidad de éxito aceptable– para defender el postulado expuesto al final del inciso:

   - Existe la posibilidad de que los servidores requeridos para soportar un proceso informático se encuentren dentro de la misma subred.

- Es común que la infraestructura basada en telecomunicaciones solamente provea un medio de salida de información, y que su ausencia provoque problemas en el proceso de dicha información.

En este caso, existe la posibilidad de brindar soporte para la comunicación a nivel local y procesar la información requerida, mientras se espera por la restauración de las telecomunicaciones para la difusión de dicha información.

e) En caso de que la infraestructura de telecomunicaciones no pueda ser restaurada de forma rápida, se deberá pensar en alternativas para la transferencia de información, que pueden ir desde el soporte de las comunicaciones y la operación en una institución externa hasta la transferencia de archivos vía Internet.

Soporte en Sitios Alternativos: No deberá entenderse, forzosamente, por sitio alternativo el lugar previamente preparado para poder soportar de forma oportuna la operación llevada a cabo en el Sitio Principal.

Un sitio alternativo, puede obedecer o distar por mucho de la definición anterior, pudiendo ser incluso solo un espacio físico donde, con recursos limitados y obtenidos extemporáneamente, se intente soportar la operación original –de hecho, la bibliografía correspondiente al tema "*Disaster Recovery*", maneja el concepto "*Cold Site*" (Sitio Frío) cuya descripción es muy similar a nuestra segunda definición de Sitio Alternativo–. Por esta razón considérense las siguientes acciones para la operación en Sitios Alternativos:

a) Es muy probable que la operación en sitio alternativo implique el traslado de los recursos informáticos originalmente alojados en el sitio principal. No obstante que el traslado de dichos recursos debe ser rápido, también debe ser realizado de forma ordenada y documentada, de preferencia utilizando ordenes de entrada y de salida para todo el equipo trasladado. El llevar a cabo este inventario previene de posteriores pérdidas de equipo de cómputo.

b) En caso de que la contingencia sea causada por fenómenos sociales como huelgas o muestras de inconformidad por parte de activistas, la operación en el sitio alternativo (en caso de existir) deberá llevarse a cabo de forma discreta, solamente enterando de ésta al personal directamente involucrado.

c) Las negociaciones de apoyo mutuo con otras organizaciones pueden brindar una excelente alternativa de operación en Sitios Alternativos.

d) El CPC procurará que las decisiones tomadas bajo estas circunstancias involucren directamente a los directivos de la Facultad con el fin de saber si ellos pueden autorizar un aporte extra de recursos que permitan habilitar la operación de forma mas rápida.

e) La recomendación de habilitar primero la infraestructura de Red LAN antes que la infraestructura de telecomunicaciones se extiende a este grupo de consideraciones.

FASE DE RECONSTITUCIÓN:

La fase de reconstitución pretende restaurar la operación de la dependencia a una forma igual a la realizada antes de la situación de contingencia. Esta fase comienza inmediatamente después de la fase de activación, de forma paralela con la fase de recuperación.

Si los elementos iniciales (sitio de operación, recursos humanos y tecnológicos, etc.,) se han perdido definitivamente, las actividades realizadas en esta fase deberán estar encaminadas a la aportación de nuevas facilidades para restaurar la operación normal de los sistemas.

El tiempo requerido para la reconstitución total del área y la puesta en marcha de los recursos informáticos y los sistemas e información alojados, puede variar desde algunos días hasta meses enteros y dependerá de los siguientes factores:

- El daño causado por la situación de contingencia.
- La recurrencia de dicha situación de contingencia.
- La cantidad de recursos asignados para llevar a cabo la restitución del área.
- La eficiencia del personal asignado a esta tarea.

Cabe señalar que, según la magnitud del problema, es posible que la estimación de tiempo de restauración ya no sean responsabilidad directa del CPC si no de los directivos de la Facultad, e incluso de la UNAM.

Consideraciones: No obstante que, en esta fase, las cuestiones logísticas pudieran quedar fuera del alcance del personal del área, se plantean las siguientes recomendaciones:

a) No importando que la fase de recuperación y la fase de reconstitución inician de manera simultánea, es prioritario finalizar con la fase de

recuperación, en virtud de la importancia de mantener latente la operación del área.

b) Hasta el momento en que un sistema o aplicación es reconstituido y sometido a pruebas operativas, seguirá funcionando la versión habilitada en la fase de recuperación.

c) Una vez que el sitio original –o un sitio nuevo– quede habilitado al nivel en que nuevamente pueda soportar la operación de los sistemas a cargo del área, se deberán reinstalar los sistemas al modo de operación original, para lo cual, los respaldos de los sistemas, hechos antes de que ocurriera la contingencia, nuevamente serán de mucha utilidad.

d) El resto de las actividades técnicas a realizar en esta fase se enumeran a continuación:

- Asegurar el correcto suministro de servicios, tales como energía eléctrica, telefonía, telecomunicaciones, etc.
- Restablecer la conectividad y las interfaces de las redes de área local (LAN) y de área amplia (WAN)
- Probar la correcta operación de los sistemas para asegurar su total funcionalidad
- Respaldar el sistema y los datos utilizados en la fase de recuperación y restaurar el sistema original.
- Apagar los sistemas utilizados durante la contingencia.

e) El CPC deberá elaborar, con ayuda del personal operativo y los GST's, un inventario de las pérdidas totales, con el fin de poder solicitar la restitución de dichos recursos.

f) Se deberá dar seguimiento puntual a las indemnizaciones otorgadas por las compañías aseguradoras y ver si se lleva a cabo el total cumplimiento del contrato inicial.

5. Pruebas y Mantenimiento

Una vez que se tiene un Plan de Contingencias adecuado a las necesidades del área, es fundamental dedicarle los recursos necesarios para que éste nunca se vuelva obsoleto por falta de actualización y mantenimiento, y para descubrir las posibles fallas o conceptos no contemplados, con el fin de que, si algún día llega a ser requerido, el Plan de Contingencias sea lo mas eficaz posible.

ESQUEMA DE PRUEBAS

Llevar a cabo un esquema de pruebas sobre el Plan de Contingencias del área, es un elemento esencial en la depuración y desarrollo del mismo. Este tipo de acciones deja al descubierto las deficiencias que el Plan pudiese tener, las identifica y las ubica.

Probar el Plan de Contingencias también ayuda a evaluar la capacidad de respuesta –tanto en rapidez como en eficiencia– del equipo de trabajo asignado a desempeñar funciones en el esquema de contingencias, además de que les ayuda a familiarizarse con las tareas que deberán desempeñar dentro del citado esquema y a integrar un verdadero grupo de trabajo con el resto del personal asignado a esta tarea.

Metodología de Pruebas

En vista de lo variados y complejos que pueden ser los Planes de Contingencias de las Divisiones de la FI (con respecto a los tópicos y tipos de sistemas que manejan), se describe una metodología general para llevar a cabo las pruebas del los respectivos Planes de Contingencias. Cada área de la FI adaptará esta metodología a sus necesidades:

1) Establecer los objetivos de la Prueba: En vista de la gran cantidad de clases de contingencias que pueden existir, se recomienda realizar pruebas variadas, cada una con sus propios objetivos específicos y con su propia visión de cuales aspectos se estarán evaluado en dicha prueba.

2) Establecer un escenario de prueba: Con base en los objetivos de la prueba, se deberá adaptar un escenario adecuado para el tipo de contingencia que se desea emular, se deberá poner especial atención en los hechos que propician la ejecución de los puntos a evaluar.

3) Identificar a los participantes: Este es un punto importante, en virtud de que en una contingencia real, cada uno de los participantes podría desempeñar una tarea fundamental en la restauración de la operación y la observación minuciosa del personal puede pulir muchos detalles que en una situación real pueden desembocar en ineficacia.

4) Documentar los resultados de la prueba: Con base en los objetivos específicos de la prueba, se deberán plasmar en un documento todas los comentarios que de ella resulten: evaluaciones, contratiempos, vivencias de los participantes, etc. Todo esto con el fin de depurar cada vez mas el Plan de Contingencias.

Consideraciones: Además de la metodología planteada, se propone tomar en cuenta las siguientes consideraciones:

a) Antes de llevar a cabo una prueba generalizada del Plan de Contingencias, se deberá probar individualmente cada uno de los sistemas involucrados en éste, con el fin de confirmar la exactitud de los procedimientos individuales de recuperación

b) Las pruebas deberán llevarse a cabo bajo condiciones controladas para evitar incidentes. Una prueba de los elementos del Plan de Contingencias no deberá de poner en riesgo el sano desempeño del área.

c) Una prueba robusta de la eficacia del Plan de Contingencia en conjunto, podría considerar los siguientes tópicos:

   - Recuperación de un sistema a través de los respaldos generados.
   - Coordinación entre los participantes de la prueba.
   - Conectividad interna y hacia el exterior.
   - Desempeño de los sistemas en equipo alternativo.
   - Restauración normal de la operación.

d) En caso de no contar con equipo para realizar las pruebas, estas se pueden programar en un horario en que no se afecte a la producción.

e) Se recomienda realizar pruebas sobre el Plan de Contingencias cada cuatro o seis meses.

ESQUEMA DE MANTENIMIENTO

La incorporación de nuevos sistemas al la operación informática del área, el establecimiento de una nueva tecnología a la infraestructura del sitio operativo o

la adaptación de nuevos roles de actividades dentro del área –aunados al rápido desarrollo tecnológico que vivimos actualmente y que obliga a una filosofía de constante renovación–, pueden llevar al Plan de Contingencias de nuestra área a un nivel de no-actualización tal que se puede volver un documento obsoleto en un lapso corto de tiempo.

Para ser un documento efectivo, el Plan de Contingencias deberá ser sometido a procesos periódicos de mantenimiento y actualización, con el fin de que refleje exactamente los requerimientos, componentes y políticas de los sistemas.

La actualización y el mantenimiento del Plan de Contingencias, idealmente deberá enfocarse en los siguientes puntos:

- Requerimientos operacionales de área
- Requerimientos de seguridad
- Procedimientos técnicos
- Hardware, software e infraestructura en general
- Información general del personal
- Información general de los proveedores de equipo de computo y seguros

Consideraciones: Además de la actualización de los puntos planteados, es prudente considerar los siguientes aspectos:

a) De forma ideal, el Plan de Contingencias debe ser actualizado al menos una vez al año, o cuando ocurra un cambio que repercuta de forma importante en la operación informática del área (existe información que deberá ser actualizada con mayor frecuencia como los directorios del personal.)

b) Después de cada modificación, deberán entregarse copias del Plan de Contingencias actualizado a todo el personal involucrado en el esquema de contingencias (se recomienda entregar el ejemplar actualizado contra la entrega del ejemplar anterior.)

c) Deberá existir una copia del Plan de Contingencias actualizado en el sitio de operación principal y en el alternativo (si existiese.)

d) La actualización del Plan de Contingencias estará a cargo del CPC, en colaboración con el personal operativo o técnico que tenga que reportar algún cambio importante dentro de la operación de los módulos o elementos a su cargo.

3.4 Difusión

3.4.1 Inclusión del Plan de Contingencias dentro del PIDI de la FI

Actualmente existe –dentro del PIDI de la Facultad de Ingeniería– un apartado dentro del capítulo 6 (Seguridad Informática) destinado al Plan de Contingencias Informático de la Institución; se pretende que una parte del presente trabajo ocupe el mencionado apartado con el fin de que su consulta sirva de apoyo en la implementación de los planes de contingencias respectivos a cada una de las áreas de la Facultad.

Cabe mencionar la propiedad modular con la que cuenta el apartado 3.3 del presente trabajo, ya que su extracción e incorporación dentro del PIDI, cumplirá con el objetivo de dotar a éste último –una vez aprobado por el Comité de Computo de la FI– de un Plan de Contingencias Informático.

3.4.2 Manual de Contingencias en Internet : Elaboración de Páginas HTML, URL y espacio reservado en el W. W. W.

La página web del Plan de Contingencias Informático de la FI fue desarrollada como parte del presente trabajo de tesis y contiene toda la información plasmada en el apartado 3.3 del mismo, la información fue dividida en páginas que pueden ser referenciadas desde un índice principal –ubicado en la página principal– para una fácil navegación y búsqueda de tópicos específicos.

Una vez que el Plan de Contingencias Informático sea aprobado por el Comité de Cómputo de la FI, se espera que este documento se encuentre a disposición de la comunidad universitaria –y del público en general– con fines de consulta a través de una página HTML con accesibilidad desde el portal de Internet de la Facultad de Ingeniería.

EL URL temporal[1] de la página web del Plan de Contingencias Informático de la FI se escribe a continuación:

http://www.geocities.com/pci_fi.

[1] No obstante que se tiene planeado mantener y dar continuidad al presente proyecto, se pretende que esta página forme parte del dominio de la Facultad de Ingeniería en Internet y que se pueda acceder a ella a través del URL http://www.fi-a.unam.mx.

En caso de que la solicitud de incorporación al dominio de la FI sea aceptada, se llevará a cabo la migración de la información referida y se incorporará a la información del URL temporal una liga con la nueva dirección de la página HTML.

y la página principal tendrá una presentación similar a la imagen **V. A.**

Los pasos contemplados para la creación y difusión de esta página se describen a continuación:

a) Diseño y elaboración de marcos (*frames*), que puedan ser utilizados en todas las páginas HTML del PCIFI para que éstas sean homogéneas.

b) Incorporación de la información el apartado 3.3 de este trabajo de tesis, el cual contiene el PCIFI

c) Pruebas técnicas de las páginas HTML.

d) Difusión de la página del PCIFI en un dominio gratuito (se eligió geocities.com)

e) Revisión y aprobación por parte del representante del Comité de Cómputo de la FI

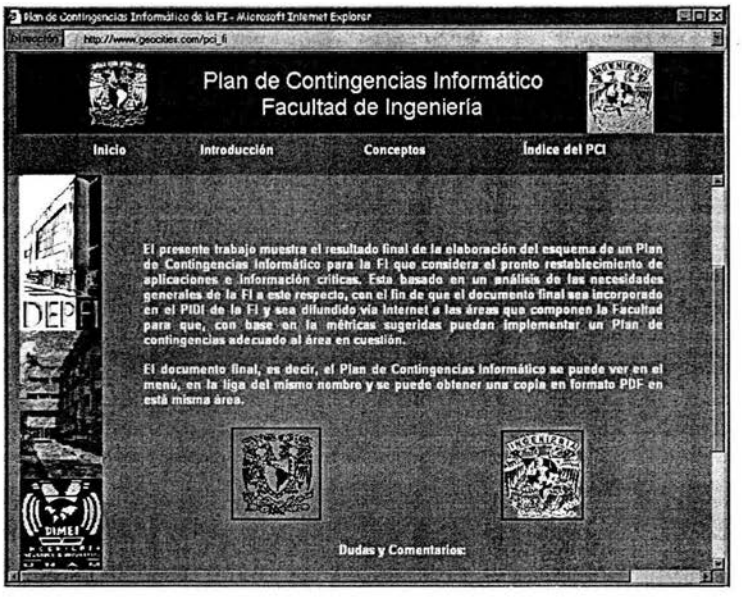


Imagen V. A: página HTML principal del Plan de Contingencias Informático de la Facultad de Ingeniería

CONCLUSIONES Y RECOMENDACIONES

El trayecto recorrido durante la realización del presente trabajo, nos transmitió varias experiencias que consideramos prudente sean plasmadas a manera de conclusiones y recomendaciones para las personas que tengan a bien revisarlo:

- Para la investigación realizada dentro de la FI y evaluación de los resultados correspondientes, nos valimos de un método de predicción cualitativo que se basa en las posturas de expertos en el tema, en vista de que no se contaba con un historial que respaldara la utilización de algún otro método; sin embargo es recomendable que las investigaciones similares en instituciones que cuenten con dichos historiales, se basen en la aplicación de métodos de predicción cuantitativos, los cuales son mas exactos y mas confiables si se cuenta con el escenario adecuado.

- La adquisición de la Norma ISO/IEC 17799, puede hacerse a través de las sucursal en México del Instituto Británico de Estándares (BSI) ; no obstante, si los interesados requieren de esta norma solo con fines de consulta, ésta se encuentra disponible en la biblioteca de la Dirección General de Normatividad de la Secretaría de Economía. Las ligas de Internet de ambos sitios, se encuentran disponibles en la bibliografía del presente trabajo.

- En los inicios del presente trabajo, se consideró que la mayoría de las contingencias con las que podríamos enfrentarnos, serían de índole informático, sin embargo concluimos que la relevancia de las contingencias de orden físico es equiparable –y en algunos casos superior– a las informáticas; recomendamos considerar el enunciado anterior para que los trabajos posteriores cuenten con un marco de referencia mas amplio.

- El Plan de Contingencias es una herramienta propia y única para la institución que la implementa, es decir, no obstante que se recomienda la revisión y consulta de los planes de contingencia de otras instituciones para el diseño e implementación de un Plan propio, el análisis de necesidades y recursos dentro de la organización es fundamental, en virtud de que todas las instituciones son diferentes entre ellas y difícilmente un plan de contingencias de determinada institución pueda adaptarse transparentemente a las necesidades de otra.

- Un aspecto común mencionado por el personal encuestado para la elaboración de este trabajo, fue la falta de recursos económicos dentro de la institución –que desemboca en la carencia de recursos tecnológicos–, así como la tramitología necesaria para solicitar nuevo equipo de cómputo. Estamos conscientes de que esta situación no es exclusiva de la FI y

sugerimos revisar las consideraciones referidas en Plan de Contingencias concernientes a este punto.

- Un recurso que puede ser de mucha utilidad en una situación de contingencia –y que no requiere de una inversión cuantiosa respecto a recursos económicos–, es la documentación correspondiente a las aplicaciones manejadas por el área, así como las especificaciones técnicas del equipo de cómputo, infraestructura, comunicaciones y suministro eléctrico; no obstante, en muchos casos esta documentación es escasa e incluso inexistente en virtud de que su utilidad está subestimada; recomendamos la destinación de recursos con la finalidad de recabar la documentación mencionada. Así también, otro recurso valioso dentro de los esquemas de contingencia y que no se le da la importancia debida, es el almacenamiento externo de los respaldos de nuestra información; cabe la observación de que los respaldos almacenados dentro del área de trabajo convencional, pueden resultar inútiles si la contingencia a enfrentar es de carácter físico y daña de forma cuantiosa la citada área.

Al inicio del presente trabajo, intentamos desasociar el concepto de seguridad informática del Plan de contingencias informática –en vista de que partimos de la categórica hipótesis de que la seguridad informática se refería a aspectos preventivos y un Plan de Contingencias solo tenía que ver con la inminente ocurrencia de un evento no deseado–, sin embargo, observamos la existencia de una fuerte relación entre la seguridad informática y el plan de contingencias informático y que este último no puede ser eficaz, si no se tiene una sólida estructura de seguridad informática en vista de que para desarrollar un Plan de Contingencia se deben conocer las medidas de seguridad implantadas en la institución.

A pesar de que actualmente existe mucha bibliografía acerca del diseño e implementación de Planes de Contingencia –así como una gran cantidad de metodologías para conseguir este fin–, los autores de dichos libros, presuponen cuantiosas asignaciones de recursos para la realización de sus propuestas; es posible que por esta razón sean pocas las empresas y corporaciones que tienen una metodología bien definida de respuesta para contrarrestar alguna situación de Contingencia.

No obstante, y a pesar de la limitación de recursos que vivimos actualmente, se debe hacer lo posible – si bien es cierto que no existe un modo infalible que proteja de los efectos de circunstancias fortuitas –para adaptar alguna metodología acorde a nuestras necesidades y recursos y que nos brinde protección contra las mencionadas situaciones de Contingencia, en especial en un país como el nuestro donde las circunstancias adversas están a la orden del día.

Así también, debemos adquirir conciencia de que la elaboración, mantenimiento y prueba de un Plan de Contingencias no es una tarea independiente o ajena a las funciones de nuestra área y de nuestro personal y que una vez adoptado se convierte en una parte importante de nuestras funciones, no hay que perder de vista que éste tipo de acciones nos ayudan a prevenir la posible pérdida del bien mas valioso con el que podemos contar dentro del ámbito computacional: la información.

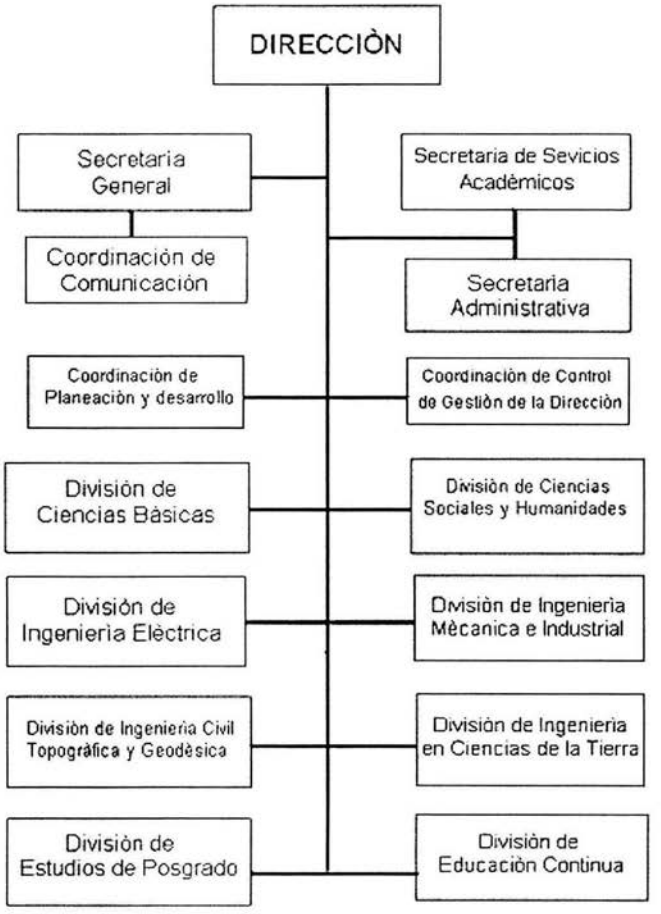
APÉNDICES

APÉNDICE A

GENERALIDADES

Organización interna de la Facultad de Ingeniería.

La facultad de Ingeniería esta formada por tres Secretarías y ocho Divisiones; a continuación presentaremos un organigrama y se mencionaran las actividades que llevan a cabo cada una de estás Secretarías como las Divisiones.



- Secretaría General. Tiene como objeto planificar, implantar, evaluar y coordinar la ejecución de los asuntos con carácter académico de la Facultad.

- Secretaría de Servicios Académicos. Tiene como objetivo coordinar la ejecución de las actividades de administración escolar, del programa editorial de la Facultad, de apoyo a maestros y alumnos y, en general, proporcionar los servicios que se requieran en la Facultad para el mejor desempeño de las actividades académicas.

- Secretaría Administrativa. Tiene como objetivo principal velar, de acuerdo con las políticas fijadas por el director, por el mejor aprovechamiento de los recursos financieros de la Facultad, de tal forma que se dé cumplimiento a programas institucionales.

- División de Educación Continua La educación continua es un proceso de mejoramiento permanente y de actualización de los profesionales de la ingeniería. Diseña e imparte cursos en distintas modalidades: abiertos, institucionales, a distancia. Organiza seminarios, conferencias, mesas redondas y otras actividades educativas, especialmente diseñadas para actualizar y transmitir nuevos conocimientos.

- División de Estudios de Posgrado. A través de los programas de especialización, maestría y doctorado, la División prepara candidatos para el trabajo profesional especializado, forma profesores para la enseñanza de la ingeniería e investigadores que desarrollan innovaciones científicas y tecnológicas en ingeniería para contribuir a la resolución de problemas nacionales y en las tareas de difusión y extensión académica.

- División de Ingeniería Civil, Topográfica y Geodésica. Imparte y coordina académica y administrativamente las carreras de Ingeniero Civil e Ingeniero Topógrafo y Geodesta.

- División de Ciencias de la Tierra. Imparte y coordina académica y administrativamente las carreras de Ingeniero Geólogo, Ingeniero de Minas y Metalurgista, Ingeniero Geofísico y Ingeniero Petrolero.

- División de Ingeniería Eléctrica. Imparte y coordina académica y administrativamente las carreras de Ingeniero en Computación, Ingeniero Eléctrico Electrónico e Ingeniero en Telecomunicaciones.

- División de Ingeniería Mecánica e Industrial. Imparte y coordina académica y administrativamente las carreras de Ingeniero Mecánico e Ingeniero Industrial.

- División de Ciencias Básicas. Imparte las asignaturas de las ciencias básicas: matemáticas, física y química, contenidas en los planes de estudio de todas las carreras.

- División de Ciencias Sociales y Humanidades. Imparte las asignaturas humanísticas y sociales que forman parte de los planes de estudio de las carreras de la Facultad y organiza las actividades socioculturales.

Componentes Actuales del PIDI.

El PIDI esta compuesto actualmente por siete capítulos:

- Objetivos y Funciones. Este capítulo describe los objetivos y funciones, que en el ámbito de cómputo tienen cada una de las Divisiones y Secretarías que conforman a la Facultad de Ingeniería y que anteriormente se mencionaron.

- Infraestructura informática. Describe los elementos que componen a cada área dentro de la Facultad de ingeniería, es decir, dentro de este capitulo se encuentran cuatro capítulos mas que describen Hardware, Recursos Humanos, Requerimientos y el ultimo apartado menciona la Investigación, Desarrollo, Docencia y Administración, especificado por área.

- Políticas. Es uno de los capítulos más extenso del PIDI, ya que, trata los temas relacionados con Requisiciones y Adquisiciones, es decir, normas y políticas especificas para la compra de equipo tanto nacional, como extranjero, formatos e instructivos para la compra de equipo, sin olvidar formatos e instructivos para los almacenes y suministros. Además, en este capitulo se cuenta con las políticas que se deben considerar para el uso de equipo de cómputo, mantenimiento del mismo y desarrollo de Sistemas.

- Esquema de Desarrollo Informático. Plantea de una forma sencilla el objetivo de actualizar y complementar el PIDI, considerando las perspectivas de la Facultad de Ingeniería para el presente siglo. Para llegar a alcanzar el objetivo planteado por el Comité de cómputo se plantea una estrategia, planeación, acciones preliminares, acciones informáticas estratégicas, y reflexiones que permitirán alcanzar las metras propuestas.

- Estrategia de Desarrollo Informático. Se presentan las estrategias que seguirá cada División y Secretaría dentro de la Facultad de Ingeniería que les permita mantener actualizados el equipo de cómputo, así como el personal, y por tanto la eficiencia del mismo.

- Seguridad. El capítulo de Seguridad esta dividido en tres partes fundamentales, que son: Seguridad Física, Seguridad Lógica y Sanciones. Básicamente se muestra un panorama general acerca de lo que son las PSC, porqué son importantes, qué ventajas tienen, cuáles son los problemas más comunes a los que se enfrentan las personas encargadas de elaborarlas al momento de querer implantarlas, además de sugerir algunas consideraciones que deben tenerse en cuenta al momento de escribirlas, con el propósito de crear políticas adecuadas para la organización en cuestión. Además es un capitulo de suma importancia, ya que debe contener un apartado para el Plan de Contingencias Informático, y que finalmente es la meta del presente trabajo.

- El Comité Asesor de Cómputo de la Facultad de Ingeniería. Finalmente es este último capítulo se presentan las Bases para su funcionamiento las cuales son: Consideraciones Generales, Disposiciones Generales, Integración de la Comisión, Funciones de la Comisión, Funciones de los Integrantes de la Comisión, Sesiones de la Comisión y Modificaciones a las Bases.

APÉNDICE B

NORMA ISO/IEC 17799 (CAPÍTULO 11)

Manejo de la continuidad de la Operación

11.1 Aspectos del Manejo de la continuidad de la Operación

Objetivo: Contrarrestar los efectos de la interrupción de la operación y las actividades y proteger los procesos críticos de los efectos de fallas mayores o desastres.

Se debe de contar con un plan de contingencias que permita contrarrestar interrupciones en las actividades de la dependencia y proteger los procesos críticos de los efectos de fallas mayores o desastres.

El proceso de administración de la continuidad de la operación debe ser implementado para reducir la interrupción causada por siniestros y fallas de seguridad (las cuales pueden ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas en el equipo o acciones deliberadas) para un nivel aceptable entre la combinación de controles de prevención y recuperación.

Las consecuencias de desastres, fallas de seguridad y pérdidas de servicios, deben ser analizadas. Los planes de contingencia deben ser desarrollados e implementados para asegurar que los procesos de la dependencia pueden ser restaurados dentro de los lapsos de tiempo pertinentes. Tales planes deben ser mantenidos y practicados para convertirse en una parte integral de todos los otros procesos.

La administración de la continuidad de operación debe incluir controles para identificar y reducir riesgos, limitar las consecuencias de los incidentes dañinos y asegurar la recuperación oportuna de operaciones esenciales.

11.1.1 Proceso de la administración de la continuidad de la operación

Debe existir un proceso bien administrado que favorezca el desarrollo y mantenimiento de la continuidad de la operación dentro de la dependencia. Éste debe proporcionar los siguientes elementos clave de la administración de la continuidad de la operación:

a) Entender los riesgos que la dependencia enfrenta en términos de su viabilidad e impacto, incluyendo una identificación y ponderación de los procesos críticos;

b) entender el impacto de las interrupciones que pueden ocurrir en la operación (es importante que las soluciones sean dadas para manejar pequeños incidentes, así como incidentes serios que puedan poner en riesgo la operación de la dependencia) y establecer los objetivos de las facilidades del proceso de información:

c) considerar la adquisición de seguros que puedan formar parte de los procesos de la continuidad de la operación;

d) formular y documentar una estrategia de continuidad consistente de los objetivos y prioridades acorados;

e) formular y documentar un plan de continuidad de acuerdo a la estrategia acordada;

f) probar y actualizar los planes de continuidad de forma regular;

g) asegurarse que la administración de la continuidad de la operación sea incorporada dentro de la estructura y los procesos de la dependencia. La responsabilidad de la coordinación del proceso de administración de la continuidad debe ser asignada a un nivel adecuado dentro de la organización, por ejemplo un comité de seguridad informática.

11.1.2 Continuidad y Análisis de Impacto

La continuidad de operación debe comenzar con la identificación de eventos que puedan causar la interrupción de los procesos operativo, por ejemplo fallas en el equipo, inundaciones o incendios. Esto debe de acompañarse de una asignación de riesgo para determinar el impacto de dichas interrupciones (tanto en términos de nivel de afectación y periodo de recuperación.) Ambas actividades deben llevarse a cabo con la total atención de los propietarios de los procesos y los recursos de la organización. Esta asignación considera a todos los procesos.

Dependiendo de los resultados de la asignación de riesgo, debe ser desarrollado un plan estratégico para determinar una aproximación generalizada de la continuidad de la operación. Una vez que este plan ha sido creado, debe ser endosado a administración.

11.1.3 Escribiendo e implementado planes de continuidad.

Los planes deben ser desarrollados para mantener o restaurar la operación de la organización en los lapsos de tiempo requeridos ya sea por interrupción o falla de los procesos críticos de dicha operación. El proceso de planeación de la continuidad debe considerar los siguientes tópicos:

a) Identificación y acuerdo de todas las responsabilidades y procedimientos de emergencia;

b) implementación de procedimientos de emergencia que permitan el recobro y restauración en los lapsos de tempo pertinentes. Se debe prestar especial atención a la evaluación de dependencias externas y los contratos en curso;

c) documentación de los procedimientos y procesos acordados;

d) educación apropiada del grupo de trabajo en los procedimientos y procesos de emergencia acordados incluyendo manejo de crisis;

e) prueba y actualización de los planes.

El proceso de planeación debe enfocarse a los objetivos requeridos por la organización, por ejemplo, la restauración de servicios específicos en lapsos de tiempo mesurables. Deben ser considerados os servicios y recursos que harán posible lo anterior, incluyendo coordinación de grupos de trabajo, recursos no informáticos, así como los acuerdos para facilidades en el proceso de información.

11.1.4 Estructura del Plan de Continuidad

Debe de mantenerse una estructura simple en nuestro plan de continuidad para asegurar que todos sus componentes sean consistentes y para identificar prioridades para prueba y mantenimiento. Cada plan de continuidad debe especificar claramente las condiciones para su activación, así como los individuos responsables de llevar a cabo cada uno de los componentes del plan.

La estructura de un plan de continuidad debe considerar lo siguiente:

a) Las condiciones para activarlos planes que describen el proceso a seguirse (como evaluar la situación, quienes están involucrados, etc.) antes de la activación de cada plan;

b) procedimientos de emergencia, los cuales describen las acciones a ser ejecutadas después de un accidente que ponga en peligro la operación de la organización y / o la seguridad de los recursos humanos. Estos deben

incluir acuerdos con cuerpos públicos de seguridad, p.e. Cuerpo de Bomberos, Policía o Gobierno Local;

c) procedimientos de retorno los cuales describen las acciones a ser tomadas para trasladar actividades y procesos esenciales o servicios de soporte hacia localidades alternativas temporales, y reactivar dichos procesos en los lapsos de tiempo requeridos;

d) procesos de reanudación que describen las acciones a ser tomadas para regresar al estatus normal de operación;

e) un calendario de mantenimiento que especifique como y cuando debe ser probado el plan, y el proceso de mantenimiento del mismo;

f) actividades de concientización y educación, diseñadas para que el personal comprenda el proceso de continuidad y asegurar que los procesos continúen de forma efectiva;

g) las responsabilidades de cada uno de los individuos, describiendo quien es responsable de la ejecución de cada elemento del plan.

Cada plan debe tener un propietario. Los procedimientos de emergencia, los procedimientos de retorno y los procedimientos de reanudación deben ser consideradas como una responsabilidad inherente de los propietarios de los procesos o recursos correspondientes. Los convenios de servicio técnico alternativo, tales como servicios de comunicación o procesos de información, deberán ser responsabilidad de los proveedores de los mismos.

11.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

11.1.5.1 Prueba de los planes: Los planes de continuidad suelen fallar al momento de ser probados, la mayoría de las veces por suposiciones incorrectas, descuidos o cambios en el equipo o en el personal. Por lo tanto éstos deben ser probados con regularidad para asegurar para asegura que están actualizados y son efectivos. Dichas pruebas deben asegurar que todos los miembros del equipo de recobro y otros grupos involucrados están concientes de la aplicación del plan.

El calendario de pruebas para el plan de continuidad deben indicar cómo y cuando cada uno de los elementos del plan deben ser probados. Es recomendable que se prueben con frecuencia cada uno de los componentes del plan de forma individual. Deben ser utilizadas varias técnicas para proporcionar la seguridad de que el plan funcionará en caso de una contingencia real. Estas pruebas incluyen:

a) Prueba de varios escenarios;

b) simulación (particularmente para la gente en entrenamiento);

c) pruebas de las técnicas de recuperación (asegurarse que los sistemas de información pueden ser restaurados de forma efectiva);

d) pruebas de recuperación en un Site alternativo (ejecutando procesos en paralelo con la información recuperada fuera del Site principal);

e) pruebas de los servicios de los proveedores (asegurarse que los servicios y productos proporcionados de forma externa cumplirán con los compromisos pactados)

f) simulacros completos (probar que la organización, el personal, el equipo, los servicios externos y los procesos pueden afrontar un escenario adverso)

Las técnicas utilizadas deben reflejar la naturaleza del plan de recuperación especifico.

11.1.5.2 Mantenimiento y reevaluación del plan: Un plan de continuidad debe ser mantenido, revisado y actualizado regularmente para asegurar su efectividad. Los procesos deben ser incluidos en el programa de administración de la organización para asegurar que las cuestiones de continuidad están correctamente dirigidas.

La responsabilidad debe asignarse por revisiones regulares al plan de continuidad; la identificación de cambios en los acuerdos tomados y aun no reflejados en el plan de continuidad deben contar con el seguimiento adecuado dentro de las actualizaciones del plan. Este proceso formalizado de control de cambios deberá asegurar que las secciones actualizadas sean reforzadas por revisiones regulares y se incorporen al plan completo.

Algunos ejemplos de situaciones que conllevan a la actualización del plan pueden ser la adquisición de nuevo equipo, modificaciones a los sistemas operacionales o cambios en:

a) el personal

b) direcciones y números telefónicos

c) estrategias de operación

d) localizaciones, facilidades y recursos

e) legislación

f) contratistas y proveedores

g) riesgo (financiero y operacional)

APÉNDICE C

MÉTODOS DE PREDICCIÓN CUALITATIVOS

Los métodos de predicción cualitativos son utilizados principalmente cuando se desea realizar predicciones de eventos para los cuales no se cuenta con datos históricos que permita fundamentar la predicción de una forma mas sólida – tal es el caso de la introducción de un nuevo producto en el mercado de consumo, o nuestro caso de estudio que contempla un análisis de los puntos de atención a ser contemplados dentro de un Plan de Contingencias para la FI–. En estos casos, se deberá depositar la confianza en otra evidencia, generalmente en un tipo de información subjetiva o crítica, como la base para el pronóstico deseado.

Los Métodos de predicción que no contemplan la utilización de una base de datos histórica, se llaman *Métodos de Predicción Cualitativos* y son el objeto del presente apéndice. A continuación describiremos brevemente cuatro de los modelos cualitativos mas comúnmente utilizados:

a) ***Método de Consenso de Panel***: El Método de Consenso de Panel asume que la institución o la empresa, cuenta en su matrícula con expertos que poseen el conocimiento esencial o la experiencia que les permita evaluar eficientemente los efectos inciertos del futuro; incluso asume que dichos panel de expertos reconocerán diferentes áreas técnicas importantemente involucradas y, por el complemento del conocimiento de terceros, llegarán a un consenso apropiado respecto a la predicción del tópico analizado.

   La primera dificultad esperada con el Método de Consenso de Panel consiste en que ciertos factores sociales pueden provocar que nunca se llegue a un consenso entre los integrantes del panel; quizás ciertos miembros de éste, simplemente no estén dispuestos a declinar su postura. Puede existir también, en el grupo, una tendencia de índole jerárquico que provoque que los expertos permitan que su opinión sea influenciada por expertos de mayor jerarquía, lo que provocaría un resultado tendencioso.

b) ***Método Delphi:*** El método Delphi intenta eliminar los efectos de una tendencia jerarquizada –que podría ser provocada por el *método de Consenso de Panel*– haciendo uso de una serie de cuestionarios, los cuales son diseñados para eliminar los factores de tendencia que pueden perturbar la predicción.

   El *método Delphi* emplea los servicios de un panel de expertos (tanto internos como externos a la situación) y asesores quienes dan su opinión acerca de la situación que se desea pronosticar.

Las respuesta dadas por los expertos en un primera aplicación del cuestionario –si es que no se llego a un consenso general– son utilizadas para generar un segundo cuestionario; un nuevo panel de expertos (o el mismo) son invitados a responder este segundo cuestionario. Sus respuestas son utilizadas para generar un tercer cuestionario, sucesivamente hasta que los expertos tengan la información necesaria para emitir un veredicto sobre el problema planteado.

Utilizando el método Delphi, a información y los resultados obtenidos es compartida por un grupo de expertos, los cuales pueden modificar los juicios del resto de los expertos, pero como las opiniones y revisiones de las mismas se realizan de forma individual e independiente del resto del panel, los efectos de acarreo y la influencia jerárquica tienden a ser eliminados. Otra ventaja del Método Delphi sobre el de Consenso de Panel consiste en el ahorro de tiempo propiciado por la eliminación de debates y la organización necesaria para hacer coincidir a todos los elementos del panel.

c) ***Analogía Histórica:*** La Analogía Histórica es un modelo cualitativo que permite pronosticar sucesos con base en el estudio y equiparación con modelos similares ocurridos en el pasado y de los cuales se pueden evaluar sus resultados. Una suposición fundamental de este tipo de acercamiento, consiste en que el suceso utilizado como referencia, debe desarrollarse –durante su etapa de introducción– en un escenario similar al ambiente o las circunstancias del evento a pronosticar. Si la suposición anterior es inválida, no tendremos –por lo tanto– ninguna justificación para nuestra analogía.

d) ***Acercamiento de Juster:*** Este método de predicción se ajusta principalmente a estudios de mercado. Una muestra de opiniones tomada a través de una encuesta, es capaz de determinar el escenario de ventas potencial para un producto –compradores en potencia– los cuales pueden ser el acercamiento mas adecuado para obtener un pronóstico de las ventas de determinado producto. Los métodos de estudio típicos sobre mercados identifican a la población de compradores potenciales sobre el producto, selecciona una muestra representativa de tamaño n de dicha población, después encuentran la proporción p de la muestra, la cual indica que la persona compraría el producto si se le presentara la oportunidad; el pronóstico de ventas es entonces Np, donde N es el número de de compradores potenciales en la población.

Realizando una encuesta con una respuesta sencilla –si o no– entre los consumidores con intenciones de compra, Juster (1966) ideó una forma donde las respuestas a una encuesta sobre un estudio de mercado,

permiten recopilar la información probabilística de consumo del producto. El acercamiento de Juster requiere que los encuestados seleccionen una palabra descriptiva –p. e. seguro, muy probablemente, poco probable, etc.– la cual describa su intención respecto a la adquisición del nuevo producto. Juster asocia cada palabra descriptiva con una "probabilidad de intento de compra" determinada a partir de repetir la encuesta numerosas veces. El promedio de las probabilidades de intento de compra se utiliza entonces como la estimación de p, la proporción de aquellos que en la población de consumidores adquirirán el producto.

La estimación de la proporción p en la población se la encuesta aplicada en la investigación de mercados, es una aplicación del muestreo. En el *acercamiento de Juster* se debe seleccionar un diseño apropiado de la encuesta según las características de la población que será muestreada.

APÉNDICE D

CUESTIONARIO APLICADO EN LAS ENTREVISTAS

1.- Actividades que desempeña el entrevistado, y en general el área a su cargo

2.- Número de equipos a su cargo, personal total y diario promedio que dependen de él.

3.- Terceras personas que dependen de su servicio (es decir no usuarios directos pero si beneficiarios de sus servicios)

4.- Consecuencias de la suspensión de sus servicios y tiempo (ya sea total, parcial, temporal o indefinida)

5.- ¿Han enfrentado alguna vez una contingencia que los haya enfrentado con el planteamiento anterior? (Describir con detalle incluyendo tiempo de restauración, consecuencias, medidas previas y posteriores, etc.)

6.- ¿Se realiza algún tipo de respaldo de archivos?

7.- ¿Cada cuando se realiza el respaldo de archivos?

8.- ¿Se cuenta con equipo de respaldo en caso de algún problema? (ejemplo: Impresoras, servidores, computadoras, etc.)

10.- ¿Alguna vez ha existido robo de equipo de cómputo con información importante para el usuario?

11.- Para evitar lo anterior, ¿qué tipo de restricción al acceso físico se tiene?

12.- ¿Cuenta con probables fuentes de energía alterna, en caso de falla del suministro eléctrico?

13.- Los Virus, gusanos, troyanos, entre otros a los que se ha enfrentado, ¿han producido algún daño?

14.- ¿Se cuenta con manuales de usuario y técnicos a la mano?

15.- ¿Transmite y recibe información?, de ser así, cómo saber si la recepción de la información es falsa ?

16.- ¿Alguna vez ha tenido problemas con la intromisión no autorizada, por medio de la red? De ser así, ¿qué clase de daños ocasiono?

17.- ¿Ha sufrido algún tipo de sabotaje? De ser así, ¿cuáles han sido los daños ocasionados?

18.- ¿Todos los usuarios, cuentan con un password? Medidas para asignarlos.

19.- ¿Se realiza algún tipo de encriptación de archivos?

20.- ¿Cuentan con algún guión que puedan aplicar para actuar en caso de contingencias?

21.- En caso contrario: ¿Cuál seria su interés por contar con un Guión como el descrito?

CUESTIONARIO INFORMATIVO DE MÉTODOS Y PROCESOS DE PREVENCIÓN ANTE CONTINGENCIAS INFORMÁTICAS

1.- SITUACIONES DE CONTINGENCIA

Sírvase a calificar en grado de nocividad (siendo el número 1 el de menor peso y el 5 el de mayor peso), los siguientes eventos que podrían suscitarse en situaciones de contingencia:

Falta de suministro de energía eléctrica	1	2	3	4	5
Daños causados por virus	1	2	3	4	5
Pérdida Incidental de Información	1	2	3	4	5
Impedimento de acceso al área de trabajo	1	2	3	4	5
Fallas de conectividad	1	2	3	4	5
Pérdida de Servicios Externos (Teléfono, Internet, etc.)	1	2	3	4	5
Ataques deliberados causados por externos	1	2	3	4	5
Daños incidentales causados a:					
• equipo de cómputo (PC's)	1	2	3	4	5
• redes locales (LAN)	1	2	3	4	5
• equipo del SITE	1	2	3	4	5
• servidores (archivos, información, aplicaciones, etc)	1	2	3	4	5
Ausencia del personal apto para tareas específicas	1	2	3	4	5
Robo de equipo	1	2	3	4	5
Siniestros (Sismo, Incendio, etc)	1	2	3	4	5

2.- MEDIDAS PREVENTIVAS

Sírvase a calificar en orden de Necesidad y de Factibilidad (siendo el número 1 el de menor peso y el 5 el de mayor peso), las siguientes acciones que podrían considerarse como medidas de seguridad; si la medida sugerida ya está implementada en su dependencia favor de tachar la opción correspondiente.

a) Contar con personal de respaldo que pueda desempeñar funciones especificas designadas a una sola persona.

Necesidad	1	2	3	4	5
Factibilidad	1	2	3	4	5

Implementada ☐

b) Emitir manuales de operación lo suficientemente específicos para poder reemplazar las funciones de la persona encargada en caso de ausencia.

Necesidad	1	2	3	4	5
Factibilidad	1	2	3	4	5

Implementada ☐

c) Promover la existencia de un plan de contingencias cuya elaboración, prueba y mantenimiento sean añadidos a las actividades de algunos elementos del personal.

Necesidad 1 2 3 4 5
Factibilidad 1 2 3 4 5
Implementada ☐

d) Contar con reglamentos internos que castiguen los daños (tanto accidentales como deliberados) al equipo de cómputo de la dependencia.

Necesidad 1 2 3 4 5
Factibilidad 1 2 3 4 5
Implementada ☐

e) Organizar campañas que promuevan medidas de seguridad informática dentro de la dependencia (respaldo de información personal en medio óptico o magnético, confidencialidad en claves de acceso personales, etc)

Necesidad 1 2 3 4 5
Factibilidad 1 2 3 4 5
Implementada ☐

f) Negociar convenios con los proveedores de servicios externos.

Necesidad 1 2 3 4 5
Factibilidad 1 2 3 4 5
Implementada ☐

g) Contar con respaldos (medio óptico o magnético) de información crítica.

Necesidad 1 2 3 4 5
Factibilidad 1 2 3 4 5
Implementada ☐

h) Contar con servidores de respaldo en caso de pérdida o in-operabilidad de los originales.

Necesidad 1 2 3 4 5
Factibilidad 1 2 3 4 5
Implementada ☐

i) Contar con un SITE alternativo en caso de pérdida o inaccesibilidad al mismo.

Necesidad	1	2	3	4	5
Factibilidad	1	2	3	4	5

Implementada ☐

j) Contar con generador independiente para suministro eléctrico.

Necesidad	1	2	3	4	5
Factibilidad	1	2	3	4	5

Implementada ☐

k) Contratar seguros que cubran la pérdida o robo de equipo de cómputo.

Necesidad	1	2	3	4	5
Factibilidad	1	2	3	4	5

Implementada ☐

3.- CONVENIOS

En caso de tener convenio con los proveedores de servicios o equipo de cómputo cuya finalidad sea brindar soporte en caso de contingencias, favor de describirlos.

_____

_____

_____

4.- COMENTARIOS

Agradeceremos sus comentarios y sugerencias sobre este tema.

_____

_____

_____

_____

_____

Gracias por su colaboración.

CUESTIONARIO INFORMATIVO DE MÉTODOS Y PROCESOS DE PREVENCIÓN ANTE CONTINGENCIAS INFORMÁTICAS
(Segunda Versión)

1.- SITUACIONES DE CONTINGENCIA

Sírvase a calificar en grado de nocividad (siendo el número 1 el de menor peso y el 5 el de mayor peso), los siguientes eventos que podrían suscitarse en situaciones de contingencia:

a) Falta de suministro de energía eléctrica	1	2	3	4	5
b) Daños causados por virus	1	2	3	4	5
c) Pérdida Incidental de Información	1	2	3	4	5
e) Fallas de conectividad	1	2	3	4	5
f) Pérdida de Servicios Externos (Teléfono, Internet, etc.)	1	2	3	4	5
Daños incidentales causados a:					
h) equipo de cómputo (PCs)	1	2	3	4	5
i) redes locales (LAN)	1	2	3	4	5
j) equipo del SITE	1	2	3	4	5
k) servidores (archivos, información, aplicaciones, etc)	1	2	3	4	5
l) Ausencia del personal apto para tareas específicas	1	2	3	4	5

2.- MEDIDAS PREVENTIVAS

Sírvase a calificar en orden de Factibilidad (siendo el número 1 el de menor peso y el 5 el de mayor peso), las siguientes acciones que podrían considerarse como medidas de seguridad, junto con un breve comentario referente a la razón de su calificación; si la medida sugerida ya está implementada en su dependencia favor de tachar la opción correspondiente y omitir el comentario.

a) Contar con personal de respaldo que pueda desempeñar funciones especificas designadas a una sola persona.

[1] [2] [3] [4] [5]

Implementada ☐

b) Emitir manuales de operación lo suficientemente específicos para poder reemplazar las funciones de la persona encargada en caso de ausencia.

1 2 3 4 5

Implementada ☐

c) Promover la existencia de un plan de contingencias cuya elaboración, prueba y mantenimiento sean añadidos a las actividades de algunos elementos del personal.

1 2 3 4 5

Implementada ☐

d) Contar con reglamentos internos que castiguen los daños (tanto accidentales como deliberados) al equipo de cómputo de la dependencia.

1 2 3 4 5

Implementada ☐

f) Negociar convenios con los proveedores de servicios externos.

1 2 3 4 5

Implementada ☐

h) Contar con servidores de respaldo en caso de pérdida o no operabilidad de los originales.

1 2 3 4 5

Implementada ☐

i) Contar con un SITE alternativo en caso de pérdida o inaccesibilidad al mismo.

1 2 3 4 5

Implementada ☐

j) Contar con generador independiente para suministro eléctrico.

1 2 3 4 5

Implementada ☐

k) Contratar seguros que cubran la pérdida o robo de equipo de cómputo.

1 2 3 4 5

Implementada ☐

4.- COMENTARIOS

Agradeceremos sus comentarios y sugerencias sobre este tema.

Gracias por su colaboración.

APÉNDICE E

GLOSARIO

CCC: Abreviatura de *Coordinador del Comité de Cómputo de la Facultad de Ingeniería*.

Conectividad: Palabra que hace referencia a la interconexión de dispositivos informáticos. P. e. al momento de construir una red informática se hace uso de la conectividad para que todas las computadoras puedan comunicarse en dicha red.

CPC: Abreviatura de *Coordinador del Plan de Contingencias*; persona encargada de la gestión y el control de las acciones dirigidas a activar un esquema de contingencias.

GST: Abreviatura de Grupo de Soporte Técnico; grupo de personas destacadas en alguna disciplina informática designadas a colaborar en el soporte técnico del área en caso de contingencia.

LAN: Abreviatura de *Local Area Network* (Red de Área Local); red de datos habilitada para dar servicio a un área geográfica que se encuentre dentro del orden de cientos de metros cuadrados.

Marco (*Frame*): Espacio definido dentro de una página HTML en el cual se puede desplegar el contenido de otra página referenciada.

Patch Pannel: Panel donde se concentran las terminales del cableado de red para que las computadoras que la componen puedan ser conectadas al equipo que permite la comunicación entre éstas.

PCIFI: Abreviatura de *Plan de Contingencias Informático de la Facultad de Ingeniería*.

Conector RJ45: Conector estándar utilizado como terminal de los cables UTP utilizados en algunas redes de computadoras.

UTP: Abreviatura de *Unshielded Twisted Pair* (Par Trenzado no Blindado); cable hecho de dos alambre de cobre aislado trenzados entre ellos; el UTP Nivel 5 consiste en 4 pares trenzados y es el tipo de cable de red mas utilizado actualmente.

WAN: Abreviatura de *Wide Area Network* (Red de Área Amplia)

BIBLIOGRAFÍA

- Toigo, Jon William. Disaster Recovery Planning. Yourdon Press,1989.
- Swanson, Marianne. Contingency Planning Guide for Information Tecnology Systems. Nacional Intitute of Standards and Tecnology (NIST), 2001.
- Isaacson, Jerry. MIT Business Continuity Plan. Massachussets Institute of Technology, 1995.
- Fisher, Royal P. Seguridad en los Sistemas Informáticos. Prentice Hall, 1988.
- International Organization for Standardization (ISO). INTERNATIONAL STANDARD ISO/IEC 17799. ISO, 2000.
- Miller, Irwin. Probabilidad y Estadística para Ingenieros. Prentice Hall, 1986.
- Riggs, James L. Economic Decision Models. MacGrawHill, 1968.
- William, James E. Statistics for Management and Economics. Duxbury Press.
- Makridakis, Spyros. Forecasting:Methods & Applications. Wiley, 1983.
- Gallagher, Charles A. Métodos Cuantitativos para la toma de decisiones en Administración. McGrawHill, 1980.
- Lemay, Laura. Aprendiendo HTML4 para Web. Prentice Hall, 1998.
- http://www.drj.com (Página web de *Disaster Recovery Journal*)
- http://delta.hypermart.net (Página web de *Informe Delta*)
- http://www.bsiamericas.com/Mexico/index.xalter (Página web de British Standard Institute, México)
- www.economia.gob.mx (Página web de la Secretaría de Economía)
- http://www.mundopc.net (Página del diccionario de términos informáticos)