UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM TEXCOCO

"PROPUESTA DE UN PLAN DE CONTINGENCIA DE RESPALDOS DE INFORMACIÓN DEL SOFTWARE Y LA INFORMACIÓN DE LAS ORGANIZACIONES"

TESIS

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

PRESENTAN:

Catalina Burgos Rodríguez
Rosa Edith Sánchez Ayala

DIRECTOR:

M. en C. José Sergio Ruíz Castilla

REVISORES:

M. en C. Yedid Erandini Niño Membrillo
Lic. Hipólito Gómez Ayala
Lic. Eduardo Daniel Escudero Santamaría

TEXCOCO MÉXICO, OCTUBRE 2009

Texcoco, México a 3 de Septiembre de 2009

DR. EN. E. JOSE HÉRNANDEZ RAMÍREZ
SUBDIRECTOR ACADÉMICO DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO
PRESENTE:

COPIA

AT'N M. en Fin. GUADALUPE LIZETH ARCE CHÁVEZ
RESPONSABLE DEL DEPARTAMENTO DE TITULACIÓN.

Con base en las revisiones efectuadas al trabajo escrito titulado "PROPUESTA DE UN PLAN DE CONTINGENCIA DE RESPALDOS DE INFORMACIÓN DEL SOFTWARE Y LA INFORMACIÓN DE LAS ORGANIZACIONES" que para obtener el título de Licenciado en Informática Administrativa presentan las sustentantes C. Catalina Burgos Rodríguez con número de cuenta 9714284 y C. Rosa Edith Sánchez Ayala con número de cuenta 0122721 respectivamente, se concluye que cumple con los requisitos teórico-metodológicos necesarios para su aprobación, pudiendo continuar con la etapa de impresión del trabajo escrito.

ATENTAMENTE

Lic. Eduardo Daniel Escudero Santamaría	**M.C.A. Yedid Erandini Niño Membrillo**	**Lic. Hipólito Gómez Ayala**
REVISOR	REVISOR	REVISOR

M. en C. José Sergio Ruíz Castilla
DIRECTOR

TITULACION
RECIBIDO
Por _____
Texcoco, Méx., a 15 de 09 de 09

c.c.p. C. Catalina Burgos Rodríguez y C. Rosa Edith Sánchez Ayala
c.c.p. M. en C. José Sergio Ruíz Castilla
c.c.p. M. en Fin. Guadalupe Lizeth Arce Chávez

ÍNDICE

Introducción 2
Planteamiento del problema 4
Justificación 5
Objetivos 6
Supuesto 7

1. Capítulo I Conceptos básicos
1.1. Introducción 8
1.2. ¿Qué es un Sistema de Información? 8
1.3. ¿Qué es un Programa de Seguridad de Información? 9
1.4. Conceptos 10
1.4.1. Agente Perturbador 10
1.4.2. Sistema Afectable 10
1.4.3. Mitigación 10
1.4.4. Riesgo 10
1.4.4.1. Riesgos Externos 11
1.4.4.2. Riesgos Internos 11

2. Capítulo II Conceptualización del Plan de Contingencia

2.1. Definición e Inicio 13
2.2. Identificación de Amenazas Probables 17

3. Capítulo III Diseño del Plan de Contingencia

3.1. Inventario de Recursos Críticos 20
3.2. Nexo con Seguridad de la Información 22
3.3. Respaldos de Información 23

4. Capítulo IV Implantación y Control

4.1. Implantación, Entrenamiento y Pruebas 30
4.2. Mantenimiento 32

5. Capítulo V Propuesta General de un Plan de Contingencia

5.1. Plan de respaldo 34
5.2. Plan de emergencia 51
5.3. Plan de recuperación 80

Anexos 84
Conclusiones 91
Glosario 92
Bibliografía 95

Introducción

A medida que la tecnología evoluciona y con ella, la importancia de los sistemas de información de las organizaciones, la seguridad del entorno informático se ha convertido en una de las grandes preocupaciones de los responsables de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los directivos, los cuales deben considerar sus inversiones en medidas de Seguridad Informática, como un gasto necesario que contribuya a mantener la operatividad y rentabilidad de la organización.

Esto implica que los responsables de las áreas informáticas deban explicar con la suficiente claridad las principales consecuencias de una Política de Seguridad insuficiente o incluso inexistente.

Es por ello, que se desea proponer un Plan de Contingencia de Respaldos de Información del Software y la Información de las Organizaciones el cual presenta una metodología para el desarrollo de medidas preventivas, de acción y recuperación en el caso de la materialización de las contingencias inesperadas, con las cuales además se reduzca el impacto y por lo tanto las pérdidas que la empresa pudiera sufrir con su información y el software.

Esto se logra con el Plan de Contingencia el cual esta dividido en tres fases: La primera abarca las actividades que se deben realizar de manera preventiva para reducir el impacto de cualquier riesgo además de los responsables de operarlas. La segunda abarca las actividades que nos sirven para minimizar el impacto del riesgo en el momento que esta sucediendo. Y la tercera implica todas las actividades a realizar para normalizar el estado de la información y el software, además de actualizar el Plan de Contingencia para así generar nuevas medidas preventivas buscando una mejora continua.

Con esto se busca sensibilizar al personal involucrado en las áreas informáticas sobre la relación existente entre las posibilidades del mejoramiento y los riesgos que estos implican para tener el control en caso de alguna eventualidad inesperada.

Planteamiento del problema

Los sistemas de información y la información son muy valiosos, por lo tanto, deben ser tratados como un recurso estratégico (como el capital o la estructura) y se le debe dar la misma protección para asegurar credibilidad junto con calidad y precisión al usuario. La seguridad de la información tiene como meta proteger los activos o recursos de las organizaciones de pérdida y así asegurar la viabilidad de las operaciones en caso de materializarse un riesgo.

Los recursos o activos que deben protegerse de pérdida son la información y el equipo, cuando hablamos de pérdida de estos recursos nos estamos refiriendo a daño o divulgación no autorizada de información (intencional o no) y pérdida de medios físicos. Existen también otras causas de "accidentes" informáticos como son: errores del operador, errores o mal funcionamiento de hardware, errores en el software, errores en los datos, daños a las instalaciones, errores de sistema. Es decir, el colapso de los sistemas de información (por mencionar un ejemplo), puede llevar a una situación de grave crisis a cualquier organización que ha adquirido un cierto grado de dependencia en dichos sistemas.

En la conceptualización común de un desastre nos imaginamos la destrucción del centro de computo o el daño irreversible a los equipos; sin embargo, bajo cualquier perspectiva, la pérdida de la información es un nivel de desastre informático que nunca debe de ocurrir. Las consecuencias de la pérdida de información son: pérdidas económicas por los costos de recuperación de la información, paro de operaciones durante un lapso de tiempo, prestigio de la organización en algunas organizaciones podrían poner en riesgo vidas humanas.

Conociendo cuales son los riesgos a que estamos expuestos y cuales son los recursos que hay que proteger, es posible elaborar una propuesta sobre medidas preventivas que consideramos necesarias para mejorar las posibilidades de continuidad de los sistemas de información.

Justificación

Es importante saber como actuar para evitar la perdida de información o reaccionar ante una catástrofe, ya que agiliza el tiempo y la posibilidad de continuar con las operaciones principales de la organización en caso de algún tipo de interrupción y darle la posibilidad de sobrevivir a un desastre que afecte a los sistemas de información.

Lamentables acontecimientos como atentados o desastres naturales, incendios o en algunos casos la maldad de ciertas personas o un simple fallo en el equipo, hacen necesario contar con un plan de contingencia aplicado a los sistemas de información capaz de devolver el estado natural a una organización. En caso de una emergencia debe asegurarse la disponibilidad de los recursos en cualquier momento, es decir, proveer la forma de restaurar las actividades del negocio y las funciones de sistemas usando la información almacenada dentro de la empresa, lo cual además requiere que la información correcta sea identificada.

Es por ello que los respaldos de información se establecen para sensibilizar al usuario de los riesgos que existen en la pérdida de la misma, deben tener conocimiento sobre el valor que tiene la información y los datos para la institución.

Por lo tanto, el presente trabajo sin pretender dar una visión exhaustiva del tema, busca sentar conceptos de planes de contingencia, copias de seguridad, y de continuidad en entornos informáticos.

Objetivo general

Diseñar un plan de contingencia de la planeación, elaboración y recuperación de la información mediante el análisis y estudio de otras metodologías basadas en seguridad informática y en la elaboración de un plan de contingencia para el software e información de las organizaciones.

Objetivos particulares

1. Identificar los principales riesgos a los cuales se encuentran inmersos el software y la información.
2. Establecer las medidas preventivas antes de que se materialice un riesgo.
3. Establecer las medidas necesarias durante la materialización de un riesgo.
4. Establecer las medidas necesarias después de materializado y controlado el riesgo.

Supuesto

Si una organización cuenta con un Plan de Contingencias para hacer frente a cualquier tipo de interrupción o riesgo que afectan al software e información entonces podrá continuar con sus actividades con el menor impacto posible.

Capítulo I Conceptos básicos

1.1 Introducción

La información y los sistemas que la soportan constituyen activos valiosos e importantes para la Organización. Su seguridad suele ser imprescindible para mantener valores esenciales, sean propios del sector público (servicio, seguridad procedimental, imagen), propios del sector privado (competitividad, rentabilidad) o comunes a ambos (permanencia del funcionamiento, cumplimiento de la legalidad). Dicha seguridad consiste en depositar la suficiente confianza sobre la capacidad de dicha información y sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la Organización.

Cualquier amenaza que se materialice contra al flujo normal de la información en una Organización pone de relieve la dependencia y la vulnerabilidad de toda la Organización. La necesidad de seguridad afecta a todas las formas de información y sus soportes o bien a cualquier método usado para transmitir conocimiento, datos e ideas.

Gran parte de esta preocupación por la seguridad ha sido causada por sucesos concretos que han producido elevadas pérdidas económicas. El interés por evitar la repetición de estas situaciones llevó en los años 70 a la realización de los primeros estudios de seguridad de los sistemas informáticos, liderados por las grandes compañías informáticas mundiales. Los primeros resultados de estos esfuerzos fueron el origen, entre otros, del análisis de riesgos.

Hoy en día se aborda la seguridad de los sistemas de información de forma integral, teniendo en cuenta la complejidad de las comunicaciones y la variedad de los servicios que deben ofrecer los sistemas de información.[1]

1.2 ¿Qué es un Sistema de Información?

A través del procesamiento de información, una compañía crea valor. Por lo tanto, en este caso, la información tiene un valor aún mayor porque ayuda a alcanzar los objetivos de la compañía.
Un sistema de información (SI) representa todos los elementos que forman parte de la administración, el procesamiento, el transporte y la distribución de la información dentro de la compañía.

[1] Daltabuit, Enrique. La Seguridad de la Información. Limusa Noriega Editores. México 2007.

En términos prácticos, el alcance del término "sistema de información" puede variar notablemente entre una organización y otra y, según el caso, puede abarcar todos o algunos de los siguientes elementos:

- Bases de datos de la compañía,
- Software de gestión integral de empresas (ERP, por sus siglas en inglés),
- Herramienta para la Gestión de relaciones con los clientes (CRM, por sus siglas en inglés),
- Herramienta para la Gestión de la cadena de suministro (SCM, por sus siglas en inglés),
- Solicitudes de empleo,
- Infraestructura de red,
- Servidores de datos y sistemas de almacenamiento,
- Servidor de aplicaciones,
- Dispositivos de seguridad.[2]

1.3 ¿Qué es un Programa de Seguridad de Información?

La seguridad de la información tiene como meta proteger los recursos de las organizaciones de pérdida y asegurar la viabilidad de las operaciones de la organización si ésta llegara a ocurrir. Es por ello, que se ha creado un programa de seguridad de información el cual contempla los siguientes aspectos:

a) Clasificación de la información: clasificar la información de acuerdo a su importancia para la empresa.
b) Políticas y procedimientos: clasificación de los puestos, procedimientos de contratación, abandono y transferencia, así como brindar entrenamiento al personal de nuevo ingreso acerca de las medidas de seguridad y mantener actualizado a todo el personal, etc.
c) Seguridad física: incluye los controles de acceso al centro de cómputo. Las amenazas a la seguridad física son los desastres naturales, los accidentes y las acciones deliberadas.
d) Seguridad de las comunicaciones: tanto de voz como de datos, video, etc. por cualquier medio. Las amenazas a la seguridad de las comunicaciones son intercepción, daño en los medios físicos, daño en la infraestructura de la empresa de servicios portadores, etc.

[2] http://es.kioskea.net/contents/systeme-d-information/si-systeme-d-information.php3

e) Seguridad lógica: se refiere al acceso a los sistemas de información y, por ende, a la información misma.

f) Evaluación de riesgos: tiene dos propósitos, (1) cuantificar el daño que sufriría la organización si ocurrieran los tipos de desastre identificados como amenazadores y (2) identificar medidas efectivas y adecuadas en cuanto a costo para reducir la probabilidad de que ocurran estos desastres identificados.
g) Plan de recuperación de desastres o plan de contingencia: tiene dos propósitos, (1) asegurar la disponibilidad de los activos o recursos de una organización posteriormente a la ocurrencia de un desastre y (2) reducir el impacto de un evento hasta un nivel aceptable para la dirección de la empresa.[3]

1.4 Conceptos

1.4.1 Agente Perturbador

Es un fenómeno que puede alterar el funcionamiento normal de los sistemas de información y producir en ellos un estado de desastre. Los agentes perturbadores son de origen natural o humano y tradicionalmente se les llama “calamidades”.

1.4.2 Sistema Afectable

Se trata del sistema compuesto por el hombre y su entorno físico en que pueden materializarse los desastres al presentarse un agente perturbador; incluye la población, los servicios y elementos básicos de la subsistencia, los bienes materiales y la naturaleza.

1.4.3 Mitigación

Es la disminución de los efectos de los impactos de las calamidades.

1.4.4 Riesgo

Es la posibilidad de que ocurra algún evento negativo para las personas y/o empresas.

[3] Rodríguez, Luis Ángel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995. Págs. 14 – 16.

1.4.4.1 Riesgos Externos

Los riesgos externos se definen como todos aquellos que se presentan en el ambiente físico y social que rodea a una instalación de procesamiento de información. Si bien no es posible eliminarlos, sí es factible tomar las medidas necesarias que minimicen la probabilidad de pérdida de información o destrucción de las instalaciones. Este tipo de riesgos pueden ser naturales u ocasionados por el hombre:

a) Los ocasionados por desastres naturales como:

- Inundaciones
- Temblores
- Tornados
- Tormentas eléctricas
- Huracanes

b) Los ocasionados por el hombre:

- Incendios
- Explosiones
- Accidentes laborales
- Contaminación ambiental, etc.

1.4.4.2 Riesgos Internos

Los riesgos internos se generan desde la misma empresa. Por su origen, son más sencillos de prever. Sin embargo, y aun cuando parezca contradictorio, será más fácil que se presenten, ya que el conocimiento de los procedimientos internos de operación hará más sencillo el camino de alguna persona interesada en dañar a la empresa. Por ejemplo:

- Robo
- Sabotaje
- Destrucción
    - De datos / información (software)
    - De recursos (hardware)
- Huelgas
- Corte de energía
- Errores del usuario

- Virus Informáticos[4]

[4] Gratton, Pierre. Protección informática: en datos y programas; en gestión y operación; en equipos y redes; en internet. Editorial Trillas. México, 1998. Págs. 148 - 149.

Capítulo II Conceptualización del Plan de Contingencia

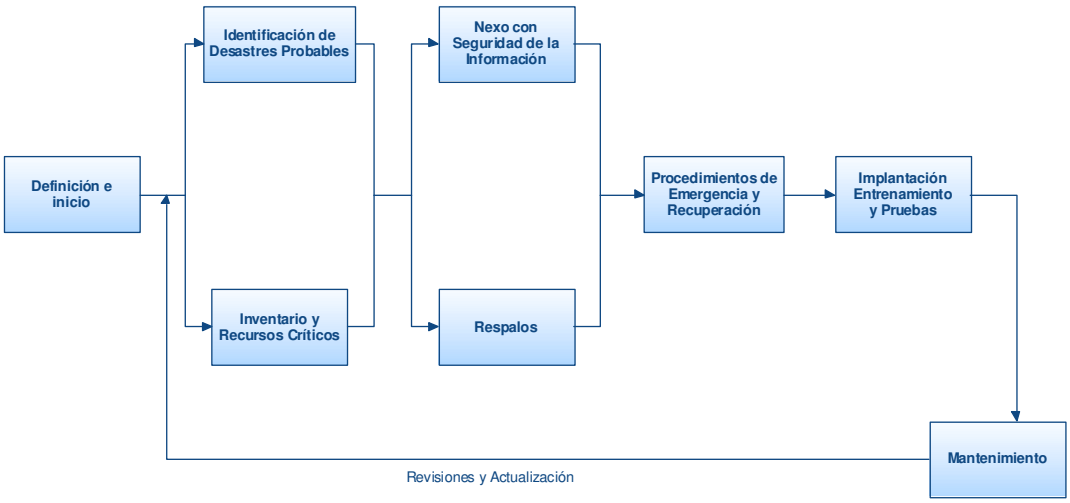

Figura No.1 Metodología de un Plan de Contingencia.

Fuente: Seguridad de la Información en Sistemas de Cómputo.

En esta fase, las acciones se orientan a la formulación de un marco general que permita establecer las bases conceptuales y la planeación inicial sobre la cual se desarrollan las siguientes 2 fases, y se coordine e induzca la participación de los elementos que forman el plan. Esta fase incluye las etapas de:

- Definición e inicio
- Identificación de amenazas probables.

2.1 Definición e inicio

El diseño de un plan de contingencia de respaldos de información es un compromiso importante que requiere de un tiempo considerable y los esfuerzos coordinados de varias personas. La cantidad de tiempo y trabajo que se invierte depende de factores como el tamaño y complejidad de las operaciones del procesamiento de datos así

como la importancia de los sistemas de información en la operación diaria del negocio la experiencia del personal, los procedimientos y la documentación.[5]

Independientemente de los objetivos propios que establezca cada empresa para su plan de contingencia, los objetivos generales del plan son los siguientes:

- Restablecer el proceso de las aplicaciones críticas tan pronto como sea posible.
- Recobrar después el procesamiento total, restaurando completamente las operaciones afectadas por el desastre.
- Restablecer la capacidad total de procesamiento de la empresa.

El propósito del plan es:

- Asegurar la disponibilidad de los activos y recursos de la organización después de la ocurrencia de un desastre.
- Reducir el impacto de un desastre a un nivel aceptable para la empresa.

Una vez que se ha tomado la decisión de hacer un plan de contingencia, el Director de Sistemas debe determinar quién se encargará de desarrollar el plan. Las dos opciones principales son:

1 Que el plan sea desarrollado por un experto en la materia contratado especialmente para esto.

2 Que el plan sea desarrollado por personal de la empresa que probablemente será coordinado por un miembro del área de sistemas, un miembro del área de seguridad o ambos.[6]

[5] Rodríguez, Luis Ángel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995. Págs. 208 - 209.

[6] Sub-Jefatura de Informática. Guía Práctica para el Desarrollo de Planes de Contingencia de los Sistemas de Información. Centro de Edición del INEI. Lima 2001.

Si se decide que el plan sea desarrollado por un consultor externo, se tienen las siguientes ventajas:

- El desarrollo de un plan de contingencia es tan complicado como el de cualquier sistema importante. Por esto, se requiere de una persona dedicada exclusivamente al desarrollo de este proyecto.
- Los consultores poseen conocimientos especializados que pueden facilitar el desarrollo más rápido de un buen plan. Sabe cómo se hace un plan de contingencia, y además sabe quién es quién dentro de la industria de seguridad de información.
- Los consultores, al ser externos a la empresa, miran con un ojo nuevo al proyecto, y se percatan de requerimientos que podrían ser pasados por alto.
- Los planes hechos por consultores, vienen en ocasiones acompañados de un acuerdo de mantenimiento. Por alguna cuota, el consultor regresará con determinada frecuencia a ayudar en las pruebas, entrenamiento y actualización del plan.

Por su parte, la mayor desventaja de contratar a un consultor es su precio: es muy caro, por lo que muchas empresas no estarían en condiciones de pagarlo.

Por otro lado, si se decide que el plan sea desarrollado en casa, se tienen las siguientes ventajas:

- El desarrollo de un plan de contingencia, al formar parte de la empresa, tendrá un acceso más rápido y completo a la información que necesite.
- El desarrollo del plan, como miembro del área de sistemas, tendrá más facilidad para la realización del inventario de hardware y software, así como para la etapa de clasificación de los sistemas de acuerdo a su importancia y consecuentemente para la definición de los procedimientos de respaldos.
- Podrá conocer todas las medidas de seguridad de información implementadas en la empresa sin ninguna reserva.
- Puede utilizar el conocimiento que tiene acerca de sus compañeros de trabajo, para tratar de definir quiénes son las personas más adecuadas para la conformación de los diversos equipos de contingencia.

Por lo que respecta a las desventajas, podemos mencionar las siguientes:

- La persona encargada, en la mayoría de los casos no contará con la experiencia necesaria en el desarrollo de este tipo de proyectos.
- La persona encargada de desarrollar el plan se le asignará esta tarea como una adicional a las que ya venía realizando. Es decir, no contará con tiempo completo para dedicarlo a este proyecto.

A) Si se decide que el plan sea desarrollado por un consultor externo, deben realizarse las siguientes actividades:
    - Selección del consultor: el Director de Sistemas debe revisar las calificaciones y experiencia del consultor, revisar y validar las estimaciones de costo y tiempo del proyecto, preguntar acerca de su relación con los proveedores de bienes y servicios de contingencia o de seguridad de información en general, etc.
    - Negociación con el consultor: tratar de llegar al acuerdo más conveniente para la empresa, en términos económicos.
    - Obtener el plan de trabajo del consultor: de esta manera se podrá controlar que el plan esté listo y funcionando en el menor tiempo posible.

B) Si se decide que el plan sea desarrollado en casa, deben realizarse las siguientes actividades:
    - Investigación y selección de metodología, herramientas automatizadas para planes de contingencia o ambas: deben realizarse algunas actividades tendientes a compenetrarse con el tema. Los vendedores de productos y servicios de recuperación, deben tener información de planes de contingencia y tal vez puedan proporcionársela al coordinador del plan. Además de esto, algunas compañías de hardware y software generan sus propias guías o metodologías para desarrollo de planes de contingencia.

Es importante aclarar que aunque no se conocen bien los requerimientos de protección de los sistemas de la empresa contra desastres, es necesario adoptar una metodología para seguir adelante con el proceso de diseño del plan de contingencia. Por otra parte, si se decide utilizar un programa para creación de planes de contingencia, ya no será necesario seleccionar una metodología, porque obviamente la metodología utilizada será la que use el programa.

Para obtener la aprobación de la Alta Dirección de la necesidad de un plan de contingencia y localizar los recursos necesarios para dar comienzo al proyecto. Existen ciertos puntos que debe considerar:

- La pérdida de disponibilidad de procesamiento puede significar severos desórdenes del negocio.
- Una interrupción prolongada es inaceptable.
- La recuperación no es automática.
- La recuperación no es fácil.
- El desarrollo y mantenimiento del plan de contingencia es una inversión esencial para el negocio.
- No hay alternativa: el plan tiene que desarrollarse.
- Un plan de contingencia no duplica el entorno de trabajo normal. Ese no es su objetivo, la empresa perdería tiempo y dinero tratando de lograr eso. El objetivo es minimizar la pérdida potencial de capacidad de procesamiento de información y mantener a la empresa operando.[7]

2.2 Identificación de amenazas probables

En esta etapa, el objetivo es conocer las principales amenazas que se ciernen sobre el procesamiento de datos de la empresa; así sabremos exactamente de qué queremos protegernos. Identificar y definir las amenazas resulta suficiente para saber dónde debe trabajarse más en la elaboración del plan. Como puede verse, la identificación y definición de desastres probables es clave para el desarrollo de objetivos para las siguientes fases del plan de contingencia.

Debemos considerar: si perdemos nuestro centro de cómputo debido a un desastre, ¿podemos sobrevivir sin él? Si la respuesta es sí, entonces obviamente es necesario un plan de contingencia. Al responder la pregunta anterior, es necesario tener en mente que el regreso a los procedimientos manuales usados antes de la implantación de los sistemas automatizados no es realista.

La automatización probablemente permitió reducir el personal o reasignarlo, y esto da origen a un incremento de la carga de trabajo, por lo que el equipo actual puede no ser suficiente para procesar el trabajo manualmente.

[7] Rodríguez, Luis Ángel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995. Págs. 210 - 214.

Una vez contestada esta pregunta, el diseñador del plan deberá identificar la dependencia de la continuidad de la empresa en las redes de cómputo; esto, en el caso de las empresas que tengan redes de computadoras de cualquier tipo (*LAN, Local Area Network; MAN, Metropolitan Area Network; WAN, Wide Area Network; etc*.).

Cabe hacer notar que los resultados de esta etapa, servirán para justificar en forma realista la necesidad de contar con el plan, y por ende de invertir en él.

En suma, si se diera el caso de que la Alta Dirección de la empresa se mostrara renuente a invertir lo suficiente para asegurar la continuidad de la función de sistemas, entonces sería necesario convencerlos mostrándoles las cifras que representa la pérdida potencial por los desastres cuyos efectos no podrían prevenirse ni mitigarse debido a la ausencia o a la no adecuación del plan de contingencia.[8]

A continuación se presentan las actividades que conforman esta etapa.

La primera actividad consiste en responder esta pregunta: ¿Podemos sobrevivir a un desastre? Pero la respuesta, no debe darla el diseñador del plan, sino los usuarios. Se debe entrevistar a los usuarios de todos los sistemas para conocer la respuesta. Si la respuesta es sí, debemos seguir adelante: es necesario desarrollar el plan de contingencia.

La segunda actividad consiste en una identificación de riesgos externos e internos la cual asegura que se han revisado y analizado todas las amenazas potenciales. El resultado de esta actividad será la base para desarrollar los procedimientos de emergencia en una etapa posterior. Las actividades de prevención serán dirigidas a los riesgos que sean identificados en esta tarea. Los subcapítulos 1.4.4.1 “Riesgos Internos” y 1.4.4.2 “Riesgos Externos” sirven de guía para asegurarse de que esta actividad se realice de una manera completa, tan exhaustiva como se quiera hacer.

El objetivo de esta actividad opcional es saber cómo pueden apoyarnos las instituciones de atención de emergencias en la prevención de desastres que afectan particularmente a nuestra organización. Y de esta manera, no efectuar trabajo innecesario o facilitar el que tiene que hacerse. Por ejemplo, consultar a los organismos locales de atención de emergencias y protección civil. Ellos ya tienen definido cuáles son los desastres naturales de ocurrencia más probable en nuestra zona.

[8]Daltabuit, Enrique. La Seguridad de la Información. Limusa Noriega Editores. México 2007.

Finalmente, hay que mencionar que las empresas que cuenten con redes de área metropolitana o de área amplia, deben poner especial cuidado en la identificación de riesgos a las telecomunicaciones.[9]

[9] Sub-Jefatura de Informática. Guía Práctica para el Desarrollo de Planes de Contingencia de los Sistemas de Información. Centro de Edición del INEI. Lima 2001.

Capítulo III Diseño del Plan de Contingencia

3.1 Inventario de recursos críticos.

En esta etapa hay que definir cuáles serán nuestras operaciones críticas y tienen que ser definidas en función a los componentes de los sistemas de información los cuales son:

Datos, Aplicaciones, Tecnología Hardware y Software, instalaciones y personal.

A continuación se presentan las actividades que hay que realizar para la identificación de recursos críticos:

Identificar los requerimientos mínimos de procesamiento de todos los sistemas

El objetivo de este punto es identificar todos los recursos de hardware, software equipo auxiliar, provisiones, etc., así como los archivos de datos que se requieran para procesar todos los sistemas de la empresa, por ello es necesario identificar:

- Usuarios. Cuántos y cuáles (puesto y nombre).
- Requerimientos y ejecución. Tiempo de ejecución, fechas críticas, modelo del CPU, espacio en el disco de las aplicaciones, memoria principal, comunicaciones y redes.
- Archivos. Archivos de datos, espacio en disco para estos archivos.
- Software. Sistema operativo, (cualquier software que tenga que estar durante la corrida), software necesario para la compilación de las aplicaciones.
- Otros. Impresoras, papel, formas especiales pre-impresas, requerimientos de comunicación de datos, etc.

Realizar un inventario de todos los recursos de cómputo.

Es necesario tener un inventario completo y actualizado de los recursos del procesamiento de datos por dos razones; para realizar una evaluación del daño, ya que ya que con esa lista se podrá determinar rápidamente que recursos siguen operando y cuáles han sido dañados, también podrá determinarse si existe alguna capacidad después del desastre.

Y la segunda razón es la restauración de instalaciones de los daños ocurridos al centro de cómputo por el impacto de un desastre ya que se podrán adquirir los dispositivos destruidos y se puede reproducir las actividades como antes de ocurrir el desastre.

Este inventario debe incluir:

- Software
- Aplicaciones
- Archivos de información
- Medios de almacenamiento (donde se contiene lo anterior)
- Hardware
- Equipo de comunicación y redes
- Documentación: manuales técnicos, manuales de usuario, documentación de las aplicaciones, etc.
- Equipo auxiliar: aire acondicionado, equipo contra incendios, dispositivos de seguridad, etc.
- Diagrama de las configuraciones de redes, configuración de las computadoras, etc.
- Otros: papel, formatos, etc.
- Reportes Impresos de Informes del Sistema.
- Consultas a las Bases de Datos vía Internet.
- Consultas a las Bases de Datos vía LAN.
- Sistema de Backup y Recuperación de Data.
- Sistema de ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.
- Los Servidores de Bases de Datos y Aplicaciones.
- Los Servicios de Red.
- Los Medios de Transmisión.
- Las Topologías de Red.
- Los Métodos de control de acceso.[10]

Establecer los escenarios de funcionamiento de plan de contingencia.

Una vez conociendo cuales son los recursos de la organización, qué importancia tiene, que tipo de desastre se necesita protegerlos, es suficiente para saber el entorno completo para poder definir lo que se considera una contingencia en el procesamiento de sistemas de información de la organización y saber bajo qué condiciones va a entrar en operación el plan de contingencia. Esto debe ser validado por el Director del área de sistemas.

10 www.ongei.gob.pe/seguridad/seguridad2_archivos/Lib5131/Libro.pdf

3.2 Nexo con seguridad de la información.

Se debe recalcar que el plan de contingencia es un subtema que está comprendido dentro del programa de la seguridad de la información, ya que para que exista un plan de contingencia con mejores resultados, debe existir conjuntamente clasificación de información, políticas y procedimientos, seguridad física, seguridad de las comunicaciones, seguridad lógica, evaluación de riesgos, plan de recuperación de desastres o plan de contingencia siendo este último el principal elemento requerido para alcanzar el objetivo de la continuidad del negocio.

Las actividades que conforman esta etapa son las siguientes:

Identificar las medidas de seguridad de la información implantadas actualmente.

Se tiene que identificar cuáles son las medidas de seguridad de la información ya sean lógicas, físicas así como de comunicaciones, con el fin de saber las preventivas de desastre.

El objetivo de tener este conocimiento es:

- Reinstalar las medidas en caso de que los dispositivos que las contengas queden dañados con el desastre.
- Conocer la situación actual de la seguridad de la información, saber si son suficientes para proteger los sistemas críticos o vitales.

Hacer recomendaciones de las medidas que deben ser implantadas.

Una vez conociendo cual es la situación actual de la seguridad de la información de la organización y teniendo en cuenta los riesgos a los que se está expuesto y cuáles son los recursos críticos que hay que proteger, se debe elaborar una propuesta de medidas que se consideren necesarias para mejorar la continuidad de funcionamiento de los sistemas.

Integrar al responsable de seguridad a los equipos de recuperación.

El responsable de la seguridad tiene una visión global de lo que son los riesgos, la gravedad del impacto, la importancia de los sistemas para la labor cotidiana aspectos importantes que serán de gran utilidad para el equipo de plan de contingencia.

De esta manera la relación entre equipo de plan de contingencia y seguridad contribuirá a la realización del trabajo de ambos de manera más efectiva.[11]

3.3 Respaldos.

Los respaldos de información se establecen para sensibilizar al usuario de los riesgos que existen de la pérdida de la misma, debe tener el conocimiento sobre el valor que tiene la información y los datos para la institución ya que representa nuestro trabajo de todos los días, y resulta increíble la falta de precauciones que se tiene para resguardarla, si el monitor, la memoria e incluso la CPU de nuestro computador dejan de funcionar, simplemente lo reemplazamos, y no hay mayores dificultades. Pero si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información.

Es principalmente por esta razón, que se debe respaldar la información que consideré de mayor importancia, sobre sus actividades laborales.[12]

Una vez que se identificaron los recursos clave para procesar los sistemas que se mantendrán en operación, se debe asegurar su disponibilidad de esos recursos aun en estado de desastre.

En general se requiere de respaldos de lo siguiente:

- Datos y documentación para aplicaciones
- Sistema de cómputo con los periféricos necesarios y las conexiones de comunicaciones de datos (hardware)
- Software (sistemas operativo, utilerías, programas de aplicaciones, manuales o documentación necesaria)
- Materiales, formatos, cintas, toner
- Personal que realice el trabajo
- Instalación alterna con el espacio de trabajo adecuado.

[11] Rodríguez, Luis Ángel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995. Págs. 227 - 229.

12 Políticas de uso de los Servicios de TI. El Auditor General del órgano de fiscalización Superior del Congreso del Estado de Guanajuato, Guanajuato, Gto., 16 de Enero 2007.

Definir lo que debe respaldarse y con qué frecuencia.

Es necesario saber con seguridad que información es la que se va a usar en el procesamiento de sistemas posterior a la emergencia, de esta manera podrá conformarse el contenido del *site* de almacenamiento externo.

Se debe considerar que todos los archivos de entrada y salida de los sistemas importantes o críticos tienen que ser respaldados.

- Respaldos de software y documentación (sistema operativo). En caso de tener varios sistemas operativos o versiones se contará con una copia de cada uno de ellos.
- Respaldos de software base. Paquetes y/o lenguajes de programación con los cales han sido desarrollados o interactúan los aplicativos Institucionales.
- Respaldo de software aplicativo. Considerando los programas fuentes, como los programas objetos correspondientes. Se debe considerar también las copias de listado fuentes de los programas definitivos para casos de emergencia.
- Respaldos de datos. Bases de datos, índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del software aplicativo de la organización.
- Inventario actualizado
- Copias de plan de contingencias
- Respaldos de hardware. Se puede implementar bajo dos modalidades:
    1. Modalidad externa. Se realiza mediante un convenio con otra institución que tenga equipos similares que brinden seguridad para procesar nuestra información y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución al materializarse un desastre.
    2. modalidad interna. Si tenemos otro lugar alterno (site) se debe contar con equipo que debe ser utilizado en las emergencias para realizar los compromisos asumidos y dar continuidad del negocio.

En cuanto a la frecuencia con que deben hacerse los respaldos se sugiere:

- Cuando se adquiera un nuevo paquete de software o se instale nuevas versiones, respaldándose también los manuales.
- Cada vez que se ponga una nueva aplicación en producción se debe tener una copia de esta como de su documentación.

- Cada vez que se actualice o modifique el plan de contingencia.
- Cada vez que se actualice el inventario de recursos
- Cuando se incluya un nuevo material o se modifique el material existente requerido para el procesamiento de los sistemas críticos.

Además se debe poner énfasis si existen redes de comunicación y que información se tendrá que respaldar así como quien será responsable de hacerlo.

Selección del site de Almacenamiento externo.

El sitio de almacenamiento externo servirá para guardar los datos y documentación de respaldos con la seguridad de que sobrevivan y que ayuden a la organización para dar continuidad del negocio aun cuando el centro de computo allá sido destruido en su totalidad.

Algunas consideraciones para la elección del sitio externo son las siguientes:

- El site alterno no debe ser dañado por desastres que afectan al centro de computo de la organización.
- El sitio no deberá estar en un sitio de alto riesgo
- Debe tener el espacio lógico y físico suficiente para albergar todo el contenido de manera organizada.

Obtener un centro de cómputo de respaldo.

Se debe considerar un centro de cómputo capaz de soportar el procesamiento de estas aplicaciones durante el desastre.

Existen opciones a considerar, pero la más efectiva consiste en contratar un proveedor de hardware ya que proporcionan equipo disponible

Procedimientos de emergencia y recuperación.

En esta actividad se comprenden los procedimientos de emergencia y recuperación así como los equipos que los ejecutarán y los integrantes de estos equipos.

Las tareas que componen esta actividad son:

Definir los equipos de contingencia.

Las acciones se llevan a cabo para el restablecimiento de un desastre son a cargo de equipos, cada uno con su propia área de responsabilidad, los cuales se deben adaptar a las circunstancias tales como numero, tamaño y sofisticación del centro de cómputo.

Coordinador del plan de contingencia.

Sus funciones son las siguientes:

- Decidir si se declara a contingencia o solo se establecen medidas de seguridad temporales de seguridad.
- Vigilar la actualización del plan y adecuado (mantenimiento, pruebas)
- Vigilar que la instalación de respaldo este en optimas condiciones.

Subcoordinador del plan de contingencia.

Sus funciones son las siguientes:

- Obtener los servicios necesarios durante al contingencia hasta restablecimiento de las operaciones normales.
- Controlar los accesos a site alterno
- Mantener el inventario actualizado del site alterno
- Notificar al agente de seguros.

Equipo de comunicaciones.

Sus funciones son las siguientes:

- Dotar de comunicaciones y telecomunicaciones a la instalación de respaldo y las entidades con las que normalmente tienen comunicación con el fin de evitar discontinuidad en el funcionamiento de los sistemas

Equipo de representantes de usuario.

Sus funciones son los siguientes:

- Dar a conocer los procedimientos de operación durante la contingencia, restricciones, procesos, a las respectivas áreas.
- Verificar que el site alterno este dotado de todo lo necesario para empezar a trabajar.
- Interactuar con empresa y site alterno

Equipo evaluador.

Sus funciones son las siguientes:

- Evaluar el daño al centro de cómputo en general (redes, comunicación, sistemas, información etc.). El inventario inicial servirá de base para ver el daño y rescatar lo que aun puede servir.

Equipo de organización y operación de la instalación de respaldo.

Sus funciones son las siguientes:

- Llevar toda la información pertinente, de acuerdo al plan de contingencia y al coordinador del plan.
- Instalar el hardware y software necesario para empezar a trabajar.
- Operar el sistema, poner énfasis en la seguridad de acceso de los sistemas de la organización.

Equipo de recuperación de instalaciones.

Sus funciones son las siguientes:

- En base al inventario y en el diagnóstico del equipo de evaluación, deberá enfocarse en la recuperación de las instalaciones de cómputo.
- Asegurar la disposición del hardware necesario en las instalaciones de respaldo. (esta tarea se realiza de manera conjunta con el equipo de organización y operación de la instalación de respaldo).

Equipo de apoyo al personal.

Sus funciones son las siguientes:

- Dar asistencia al personal herido
- Alertar a los servicios médicos
- Proveer apoyo a los empleados

Formación de equipos de contingencia.

Cada equipo requiere de los siguientes integrantes:

- Líder. Coordinar las actividades, contar con conocimiento global de todo el plan de contingencia.
- Líder suplente. Suplir al líder en caso de que éste falte.
- Miembros. Integrantes de equipo, los cuales conocen las actividades únicas de equipo en la recuperación de desastres.

Procedimientos de emergencia.

En esta actividad se especifica los pasos a seguir después de un desastre y dar inicio a la recuperación tratando de minimizar los efectos negativos a los procedimientos de cómputo de la empresa.

Los objetivos son:

- Proteger al personal
- Proteger los equipos
- Minimizar la suspensión o procesamiento de cómputo

Estos procedimientos serán ejecutados por el personal que se encuentre en el centro de cómputo quienes darán parte al coordinador del plan de contingencia.

Se deben desarrollar procedimientos contra diferentes efectos producidos en los sistemas por los agentes perturbadores. (Aplicar las medidas para los desastres probables ya identificados).

Hay que considerar dos casos:

- Daños en redes. La estrategia es tener respaldos de equipo.
- Daños en centro de cómputo y equipos centrales. Planear lo que se hará para comunicar las redes con la computadora del centro de procesamiento de datos de recuperación.

Procedimiento de recuperación.

Después de haber realizado las actividades anteriores, tienen que ejecutarse actividades para restablecer el procesamiento de sistema normal.

En el procedimiento de recuperación las actividades son las siguientes:

- Respuesta de emergencia, notificaciones correspondientes (alerta), decisión de implementar plan de contingencia (reconocimiento de daños).
- Organización de equipos de contingencia (coordinación de auxilio), activación del site de respaldo.
- Evaluación del daño, instalación de los sistemas de información y los procedimientos de operación en contingencia (servicios estratégicos, equipamiento y bienes) salvamento del site primario (rescate).
- Reactivación del antiguo site primario o instalación del nuevo y regreso al procedimiento normal, esto es, las actividades a realizar durante el estado de retorno, y debe ser breve y conciso.[13]

[13] Rodríguez, Luis Ángel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995. Págs. 231-252.

Capítulo IV Implantación y control

Una vez que se ha desarrollado el plan de contingencia se procede a continuar con las siguientes actividades:

4.1 Implantación

Comprende las siguientes actividades:

- Realizar una relación de las personas que se de a conocer el plan de contingencia. Hay que tomar en cuenta que la información del plan de contingencia es confidencial, por lo tanto debe cuidarse su distribución total de la información.
- El plan de contingencia debe incluir un directorio telefónico, de todas las personas que estén involucradas en el plan, responsables de centros de computo, agentes de seguros, proveedores de recursos de aire acondicionado, proveedor de equipo de computo, proveedores de equipos de seguridad, proveedor de equipo de comunicaciones, teléfonos de emergencia (cruz roja, bomberos, policía, etc.).
- Obtener la instalación de seguridad y equiparla al inventario anterior.
- Tener contemplado el site alterno para respaldos de información.
- Se debe anexar los procedimientos de procesamiento alterno al plan de contingencia.

Se debe considerar que el éxito de un plan de contingencia depende de las pruebas que se hayan hecho con anterioridad, que haya cumplido con los objetivos y pueda utilizarse en cualquier momento que se necesite.[14]

Entrenamiento

La recuperación exitosa de un desastre depende de que todas las personas involucradas conozcan el papel que desempeñan y las actividades que deben realizar.

Las actividades del entrenamiento contienen los siguientes objetivos:

[14] Gaspar, Juan. Planes de Contingencias La Continuidad del Negocio en las Organizaciones. Ediciones Díaz de Santos. Madrid, Enero 2004.

- Desarrollar el conocimiento y las habilidades requeridas para ejecutar el plan de contingencia
- Incrementar la probabilidad de una recuperación exitosa
- Establecer una relación y comunicación entre la gente involucrada al plan de contingencia

La capacitación y adiestramiento debe ser constante para no olvidar las actividades, considerando que para cada equipo son diferentes y que los miembros del equipo de manejo de desastres deben recibir entrenamiento sobre todo el plan de contingencia.

El programa de entrenamiento debe abarcar los siguientes puntos:

- Describir os equipos de contingencia y sus funciones
- Explicar el flujo de acciones (desde la amenaza hasta la recuperación)
- Definir a cada persona las actividades propias durante la recuperación
- Entrenamiento general de evacuación, primeros auxilios para seguridad de las personas
- Procedimientos de emergencia para operadores y personal de equipo de cómputo.

Para que el entrenamiento sea más exitoso debe considerarse:

- debe ser breve y conciso
- dar la representación con la seriedad que esto implica, y de acuerdo al nivel de conocimiento de la audiencia
- usar los medios disponibles para hacer la representación entendible
- dar solo la información que requiere la audiencia
- involucrar a la audiencia en una cultura de seguridad y de compromiso para realizar el mejor desempeño

Los resultados del entrenamiento pueden medirse con pruebas que se diseñen para el caso, o en todo caso pueden realizarse en la fase de pruebas del plan o mediante simulacros, también se debe detectar si hay fallas y hacer las correcciones.

Toda la información que se desglose en esta etapa será de utilidad para mejorarlo y actualizarlo.

Pruebas

Una empresa no puede considerar el éxito de un plan hasta que no se haya probado. Es por ello que la realización de pruebas es una forma de verificar lo siguiente:

- los procedimientos de recuperación son completos y son funcionales
- los materiales y equipo están disponibles en cualquier momento
- los datos, inventario software están actualizados
- el site alterno cumple con los requerimientos de procesamiento de los sistemas críticos
- el personal ha sido entrenado adecuadamente

Con el fin de organizar las pruebas se debe realizar un cronograma de actividades y el objetivo. La frecuencia de las pruebas debe basarse en la frecuencia de los cambios del entorno de cómputo.

Los requerimientos para la efectividad de las pruebas son:

- establecer el escenario de la prueba.
- establecer los objetivos de la prueba de manera clara.
- definir las normas de la prueba.[15]
- establecer el personal participante y observadores de la prueba.
- documentar la información que se desglose y los resultados.

4.2 Mantenimiento

El plan de contingencia requerirá de mantenimiento continuo. Si el plan no esta actualizado, o no es oportuno, no podrá ser utilizado efectivamente durante una emergencia. Es por esto que debe ser revisado frecuentemente.

Para desarrollar los procedimientos de mantenimiento y actualización del plan, el coordinador del plan de contingencia, debe identificar primero que elementos del plan pueden cambiar con el tiempo. Estos elementos normalmente incluyen:

- Surgimiento de nuevos riesgos

[15] Rodríguez, Luis Angel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995. Págs. 256 – 260.

- Bases de Datos (Aumentar las ya existentes)
- Aplicaciones (Aumentar las ya existentes)
- Software (nuevas adquisiciones o actualizaciones)
- Hardware y equipo de comunicaciones
- Redes
- Documentación
- Procedimientos de seguridad y emergencia
- Personal y/u organigrama
- Backup site y sus condiciones de contratación
- Proveedores
- Procedimientos de procesamiento alterno y las formas o materiales que necesiten (será responsabilidad del líder del equipo de usuarios notificar estos cambios al encargado del mantenimiento del plan de contingencia)

Este aspecto del mantenimiento implica también una buena distribución de las copias del plan, para que todas las personas involucradas tengan copias actualizadas.[16]

[16] Félix, José de Jesús. Plan de Contingencia Informático. México, 2005. http://www.gobiernodigital.miguelhidalgo.gob.mx/plan/D-DGD-09%PLAN%20DE%CONTINGENCIA%20INFORMATICO

Capitulo V Propuesta General de un Plan de Contingencia

5.1 Plan de respaldo

Objetivo General.

Establecer los lineamientos o medidas preventivas necesarias para concientizar al personal de la Organización acerca de la importancia de la información, hardware y software críticos que le permiten crecer y mantenerse competitiva así como enriquecer los procesos y servicios para la disponibilidad de la información, para el cumplimiento de sus actividades en caso de que se presente un desastre natural o causado por los usuarios.

I. Para el equipo de cómputo.

1.1.0. Para la instalación de equipo de cómputo y hardware.

1.1.1. Objetivo.

Lograr el uso adecuado del equipo de cómputo y demás hardware para garantizar el buen funcionamiento de la infraestructura tecnológica de la Organización.

1.1.2. Alcance.

Aplica principalmente a los que proporcionan y usan el equipo tales como directivos, encargados de área y todos los usuarios internos.

1.1.3. Política.

- Todo el equipo de cómputo (computadoras, estaciones de trabajo, y equipo accesorio), que esté conectado a la Red propiedad de la Organización debe de sujetarse a las normas y procedimientos de instalación que emite el departamento de Redes y soporte técnico.
- Cada departamento en conjunto con el Departamento de Sistemas deberá tener un registro de todos los equipos de cómputo propiedad de la Organización.
- El equipo que sea de propósito específico y tenga una misión será destinado únicamente para apoyar las funciones propias de la Organización y requiere estar ubicado en un área que cumpla con los requerimientos de: Seguridad física, las condiciones ambientales, la alimentación eléctrica.
- Los responsables de cada área de los departamentos en conjunción con el departamento de Redes y el Departamento de Sistemas deberán dar

cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos, sistema y misión.

- La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes (Redes y Soporte Técnico, Departamento de Sistemas) o jefe inmediato.
- Las impresoras de red asignadas tendrán uso compartido por un grupo de usuarios por lo que no deberá ser usada como impresora personal, el resguardo de la misma será verificado por el Departamento de Sistemas o por el encargado de área, más cercano al equipo.
- La asignación de una impresora en red y equipo accesorio, será de acuerdo a la justificación plena por cargas de trabajo del área usuaria y a la capacidad de impresión de esta última.
- Los equipos accesorios personales solo serán asignados a usuarios que por su función del puesto así lo requiera y deberá ser solicitado por escrito donde se describa la justificación y deberá ser autorizado por el encargado.
- Los equipos accesorios departamentales asignados tendrán uso compartido por un grupo de usuarios por lo que no deberá ser usada como equipo accesorio personal, el resguardo de la misma será verificado por el Departamento de Sistemas o encargado de área, más cercano al equipo.

1.1.4. Sanción.

Para cualquier empleado o directivo que se haya encontrado violando esta política ya sea accidental o provocada se hará de acuerdo a la gravedad, ya sea notificación por correo, suspensión de labor parcial o definitiva.

1.2.0. Para el mantenimiento de equipo de cómputo y hardware.

1.2.1. Objetivo.

Lograr mantener la PC y demás componentes en óptimo estado de funcionamiento, y poder detectar a tiempo cualquier indicio de fallas o daños en sus componentes.

1.2.2. Alcance.

Aplica principalmente al personal de mantenimiento del equipo de cómputo tales como encargados de área, personal auxiliar (prestador de servicio social) responsable de Redes y soporte técnico.

1.2.3. Política.

- Al departamento de Redes y Soporte Técnico (o auxiliares que el mismo designe), corresponde la realización del mantenimiento preventivo y correctivo de los equipos de cómputo, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin se deberá actuar bajo las normas y procedimientos respectivos.
- Si los equipos son atendidos por terceros, será el Departamento de Redes quien deberá normar al respecto, siempre y cuando sea dentro de la Organización.
- Es responsabilidad de cada usuario notificar a tiempo al personal encargado de mantenimiento, fallas del equipo o alguna otra anomalía.
- El personal técnico de apoyo interno de los departamentos se apegará a los requerimientos establecidos en las normas y procedimientos que el departamento de Redes emita.
- Los responsables de las áreas de cada departamento pueden dar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados por el departamento de Redes y Soporte Técnico, siempre y cuando estén capacitados para hacerlo.
- Corresponde al departamento de Redes y Soporte Técnico dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.
- Por motivos de seguridad queda prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la Organización.
- Queda prohibido sustraer algún componente de la computadora con fines de lucro o con intenciones diferentes al de dar mantenimiento.

1.2.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, hasta suspensión total o reposición del daño.

1.3.0. Para la actualización y reubicación del equipo.

1.3.1. Objetivo.

Contar con equipo actualizado que cubra los requerimientos de las actividades diarias de la organización así como llevar un control de este en existencia en cada área evitando extravíos.

1.3.2. Alcance.

Aplica principalmente al personal encargado de hacer los requerimientos de equipo tales como directivos, encargados de cada área y todos los usuarios internos.

1.3.3. Política.

- Todo el equipo de cómputo (computadoras personales, estaciones de trabajo y demás relacionados), debe procurarse y ser actualizado tendiendo a conservar en buenas condiciones y notificar de nuevas adquisiciones.
- Cualquier cambio que se requiera realizar en los equipos de cómputo de la Organización (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.
- La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el departamento de Redes y Soporte Técnico emita, así como el solicitante tendrá que justificar y notificar el traslado si este se realiza a distinto departamento.
- El equipo de cómputo a reubicar sea de la organización se hará únicamente bajo la autorización del responsable contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo, así como de informar quien será el nuevo responsable o usuario.

1.3.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, hasta suspensión total.

II. Para el control de accesos.

2.1.0. Para el control de acceso al equipo de cómputo (área).

2.1.1. Objetivo.

Llevar a cabo un control de seguridad física al personal interno y personas externas a la Organización.

2.1.2. Alcance.

Aplica a todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

2.1.3. Política.

- Solo personal autorizado podrá acceder a las áreas de los departamentos donde se encuentre equipo cuyo propósito sea confidencial y de la Organización, deberán sujetarse también a las normas que establezca el Departamento de Sistemas.
- Las personas externas cumplirán con las normas y procedimientos que establece la Organización para su ingreso.
- Por supervisión y seguridad, el departamento de Sistemas o personal que designe podrá acceder al equipo de cómputo, los sistemas operativos y su conectividad en la red cuando lo considere necesario.

2.1.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, hasta suspensión total o reposición del daño.

2.2.0. Para el control de acceso remoto.

2.2.1. Objetivo.

Tener una tecnología que permita la centralización de aplicaciones que generalmente se ejecutan entorno al usuario.

2.2.2. Alcance.

Aplica a todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

2.2.3. Política.

- El Departamento de Sistemas es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
- El acceso remoto que realicen personas externas deberán cumplir las normas que emiten en la Organización o el departamento de redes y soporte Técnico.
- La Cuenta de usuario es único al igual que la Clave Personal de Entrada, y el Sistema NO permitirá el uso de la misma cuenta en más de una conexión telefónica a la vez. Es responsabilidad del Usuario mantener la Confidencialidad de su Clave Personal de Entrada.
- La requisición de cambio de Clave Personal de Entrada o Password sólo se hará de manera personal y directa con el Administrador del Servicio.

- No se permite que la cuenta sea usada con fines diferentes a intereses académicos y administrativos del la Institución.
- El Departamento de Sistemas o Redes y Soporte Técnico se reserva el derecho de cancelar temporal o definitivamente una cuenta cuando se haga uso inapropiado del sistema. Se considera uso inapropiado actividades como: molestar a los usuarios con mensajes y charlas electrónicas, piratería, envío de propaganda subversiva, propagación de virus informáticos, uso delictivo, etc.

2.2.4. Sanción.

Aplica para cualquier empleado o directivo (usuario) que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, hasta suspensión total o en todo caso cancelación de su cuenta.

2.3.0. Para el acceso a los sistemas administrativos.

2.3.1. Objetivo.

Tener un marco de lineamientos que normatice la consulta, o acceso a los sistemas de información de la Organización y evitar el filtro de usuarios externos.

2.3.2. Alcance.

Aplica a todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización que hagan uso de la red.

2.3.3. Política.

- Tendrá acceso a los sistemas administrativos solo el personal de la Organización con facultad o con autorización del responsable si se trata de personal de apoyo administrativo o técnico.
- El manejo de información administrativa que se considere de uso restringido deberá ser cifrada o encriptada con el objeto de garantizar su integridad y Disponibilidad.
- La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la red y por las normas y procedimientos establecidos por el departamento de Sistemas.
- Los servidores de bases de datos administrativos son de uso confidencial, por lo que se prohíben los accesos de cualquier persona, excepto para el personal del departamento de Sistemas siempre y cuando tenga justificación para hacerlo.

- Es responsabilidad de los usuarios tener en resguardo adecuado las contraseñas asignadas para sus actividades.

2.3.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total.

2.4.0. Para manejo de información confidencial.

2.4.1. Objetivo.

Definir los lineamientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de la Organización.

2.4.2. Alcance.

Aplica a todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

2.4.3. Política.

- Todos los usuarios, y personal que labore para esta Organización debe tener acceso solo a la información necesaria para el desarrollo de sus actividades o con previa justificación de consulta a otra Información.
- Todo cambio, creación y modificación de información, reportes que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá las facultad de aceptar o rechazar la solicitud
- Todo usuario será responsable de la información que maneje cumpliendo con los lineamientos dados por la entidad, para protegerla y evitar perdidas, accesos no autorizados, exposición y utilización indebida de la misma.
- El personal o usuario debe evitar proporcionar cualquier información confidencial de la entidad a ningún externo sin las autorizaciones respectivas.
- Después de que el trabajador deja de prestar sus servicios a la Organización, se compromete a entregar toda la información respectiva de su trabajo realizado.

- Será responsabilidad de aquel que modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad; así como al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.
- Será responsabilidad de aquella persona estando autorizado para acceder a sistemas y equipos de informática, indebidamente modifique, destruya o provoque perdida de información que contengan, así como al que estando autorizado para acceder a sistemas y equipos de informática, indebidamente copie información que contengan.

2.4.4. Sanción.

Aplica sanción para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total.

2.5.0. Para el uso de Internet.

2.5.1. Objetivo.

Concientizar al usuario sobre el uso del servicio de Internet dentro de la Organización comprometido a la seguridad de información.

2.5.2. Alcance.

Aplica todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

2.5.3. Política.

- Es responsabilidad del usuario el acceso a páginas que atenten a la seguridad o imagen de la Organización; todo el contenido pornográfico y la mercadotecnia sexualmente orientada quedan estrictamente prohibidos en nuestros servidores o ligas a otros sitios con material ofensivo así como violencia, ocio, casinos otros sitios que atenten con la seguridad de la Organización.
- El encargado de cada departamento es el responsable de instalar y administrar los servidor(es), en conjunto con el Departamento de redes y Soporte Técnico.
- Cada departamento o área deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del

uso de la Intranet organizacional, así como las especificaciones para que el acceso a estos sea seguro.

- Los accesos a las páginas web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso que se emite.
- A los responsables de los servidores Web corresponde la verificación de respaldo y protección adecuada.
- Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que el responsable emita.
- La información que aparezca en la página de Internet del la Organización deberá ser aprobado por el responsable respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
- El departamento de Sistemas tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

2.5.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total o se procederá a bloquear los web sites.

2.6.0. Para el uso de correo electrónico.

2.6.1. Objetivo.

Establecimiento de un marco reglamentario para el uso adecuado del correo electrónico para mantener la valoración, imagen y seguridad de la información.

2.6.2. Alcance.

Aplica a todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

2.6.3. Política.

- El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad,

confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de “no repudio”.

Se permite el uso personal del correo electrónico siempre y cuando sea responsable, y:

- No provoque problemas legales a la organización.
- No se utilice para fines lucrativos personales.
- No contravenga las políticas y directrices de la organización.
- No atente contra la imagen de la organización.
- No interfiera con el trabajo de los usuarios.
- Todo usuario que tenga dudas acerca del material que puede enviar o recibir, debe consultarlo con su jefe inmediato.

Se prohíbe:

- Fraude (o intento de fraude) de los mensajes electrónicos.
- Intentar leer, borrar, copiar o modificar correos electrónicos de otros usuarios.
- Intentar enviar mensajes de acoso, obscenos o amenazadores a otro usuario.
- Interceptar el correo electrónico de otros usuarios.
- Enviar correo electrónico, utilizando el nombre y/o la contraseña de otro usuario, sin su debida autorización.
- Enviar mensajes de manera masiva, por ejemplo, cadenas de cartas y relativos a falsos virus, excepto si contienen información de interés organizacional.

2.6.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo al grado de gravedad, que va desde suspensión de días de labor, suspensión total.

III. Para la utilización de la red.

3.1.0. Para el control de acceso a la red y sus recursos.

3.1.1. Objetivo.

Regular el uso del servicio de red de Internet con el fin de optimizar el uso de dichos recursos y servicios y asegurar una mayor calidad en el desarrollo de las funciones administrativas de la Organización.

3.1.2. Alcance.

Aplica todo el personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos que hagan uso de la red de la Organización.

3.1.3. Política.

- Los recursos disponibles a través de la Red serán de uso exclusivo para asuntos relacionados con las actividades de cada departamento.
- Al departamento de redes y soporte técnico corresponde administrar, mantener y actualizar la infraestructura de la Red.
- El responsable de cada área o departamento será quien difunda el reglamento para el uso de la red y de procurar su cumplimiento.
- Todo el equipo de cómputo que esté conectado a la Red de la organización, o aquellas que en forma autónoma se tengan y que sean propiedad de la organización debe de sujetarse a los procedimientos de acceso que emite el departamento redes y soporte Técnico.
- El SSID debe ser configurado de manera que no contenga información que identifique la Organización, el producto, nombres o cualquier otra información que pueda ser utilizada por personas no autorizadas para intentar tener acceso al servicio.
- El acceso lógico al equipo especializado de cómputo conectado a la red es administrado por el departamento de Redes y Soporte Técnico.
- Será responsabilidad del usuario evitar la importación y exportación de datos confidenciales que atenten contra la organización.
- El responsabilidad de cada área o departamento asignar passwords y cuentas intransferibles con restricciones (duración, longitud, bloqueo después de ciertos fallos).
- A cada equipo cliente se le asigna una dirección IP, que no deberá ser modificada ni darse en préstamo a otro equipo.

3.1.4. Sanción.

Los usuarios en violación a esta política están sujetos a sanciones incluyendo la perdida de privilegios, de acceso a la red inalámbrica, acciones disciplinarias, despido de la Organización, y acciones legales correspondientes.

IV. Para el Software

4.1.0. Para el uso de software.

4.1.1. Objetivo.

Llevar un control del uso de software en la Organización para incrementar la seguridad en cada departamento.

4.1.2. Alcance.

Aplica al personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

4.1.3. Política.

- El encargado del Departamento de Sistemas será el responsable de homologar y estandarizar el uso de software requerido para sus actividades, así como de eliminar el que no cumpla satisfactoriamente con las actividades cotidianas del área.
- El encargado de cada área es responsable de notificar los requerimientos de software para cumplir con las actividades, así como de verificar que solo sea de uso exclusivo de la organización.
- Corresponderá al Departamento de Sistemas verificar las normas para el tipo de licencia, cobertura, transferencia, certificación y vigencia.

4.1.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo al grado de gravedad, que va desde suspensión de días de labor, suspensión total.

4.2.0. Para la instalación de software.

4.2.1. Objetivo.

Adquirir e instalar el software adecuado que satisfaga las necesidades de cada departamento.

4.2.2. Alcance.

Aplica al personal, tales como directivos, encargados de cada área y todos los usuarios internos y externos a la Organización.

4.2.3. Política.

- Corresponde al responsable de cada área o departamento emitir las normas y procedimientos para la instalación y supervisión del software para cualquier tipo de equipo.
- En los equipos de cómputo y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licencia apropiada y acorde a la propiedad intelectual.
- Con el propósito de proteger la integridad de los sistemas informáticos es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, firewall y otros que se apliquen).
- La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al departamento de Redes y soporte Técnico.
- Los protectores de pantalla y tapiz de escritorio, serán establecidos por el Departamento de Sistemas y deben ser homologados para todos los usuarios.
- No instalar copias de software pirata. (Además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles con el del usuario, lo cual provocará su inestabilidad).
- Queda prohibido la instalación de software que no cumpla con los requerimientos o actividades cotidianas, sin previa autorización del encargado de área.

4.2.4. Sanción.

Aplica a cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total o en todo caso se actuará conforme al código Penal Federal.

4.3.0. Para la actualización del software.

4.3.1. Objetivo.

Contar con actualizaciones de software que permita la eficacia en las actividades de la Organización.

4.3.2. Alcance.

Aplica a todo el personal, tales como directivos, encargados de cada área.

4.3.3. Política.

- Corresponde al encargado de cada departamento cubrir con los requerimientos de software actual para eficacia de sus actividades.
- Corresponde al encargado de cada departamento verificar cualquier adquisición (antes autorizada por el Departamento de Sistemas) y ser los únicos en actualización del software o personal que el mismo designe.

4.3.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo al grado de gravedad, que va desde suspensión de días de labor, suspensión total.

4.4.0. Para la auditoria Informática.

4.4.1. Objetivo.

Obtener el análisis de la eficiencia de los Sistemas y Recursos Informáticos que conforma, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

4.4.2. Alcance.

Aplica al personal correspondiente o al Departamento de Sistemas, así como del personal que designe para tal actividad.

4.4.3. Política.

- El Departamento de Sistemas o personal que designe es el responsable de realizar revisiones periódicas para asegurar que sólo software debidamente licenciado esté instalado en las computadoras de la Organización.
- Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditoria Informática.
- Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Organización, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoria informática.

- Todos los archivos de auditoria Informática deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

- Todos los archivos de auditorias de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

- Todos los archivos de auditorias deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

- Todas las computadoras deben estar sincronizados y de ser posible tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

4.4.4. Sanción.

Aplica para cualquier responsable de auditoria Informática, personal que designe o personal de la Organización que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total.

4.5.0. Para el software propiedad de la organización.

4.5.1. Objetivo.

Verificar que el software de la organización cumpla con los requerimientos, y cuente con la autorización y licencia en regla.

4.5.2. Alcance.

Aplica a todo el personal encargado de cada área, tales como directivos y responsables.

4.5.3. Política.

- Todo el software adquirido por la organización sea por compra y/o donación es propiedad de la organización y mantendrá los derechos que la ley de propiedad intelectual le confiera.
- El encargado de cada área en coordinación con el Departamento de Sistemas deberá tener un registro de todos los paquetes de programación y software propiedad de la organización.

- Todos los sistemas (programas, bases de datos, interfaces) desarrollados con o a través de los recursos de la organización se mantendrán como propiedad de la misma respetando la propiedad intelectual del mismo.
- Los datos, las bases de datos, la información generada por el personal y los recursos Informáticos de la organización deben estar resguardados.
- Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.

4.5.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total o en todo caso se actuará conforme al código Penal Federal.

4.6.0. Para la instalación antivirus.

4.6.1. Objetivo.

Dotar a todo el equipo de cómputo con herramienta antivirus para disminuir la vulnerabilidad en equipos susceptibles a infección por virus.

4.6.2. Alcance.

Aplica al personal correspondiente del Departamento de Sistemas y/o Redes y Soporte Técnico así como del personal que designe para tal actividad.

4.6.3. Política.

- Cada usuario será responsable de mantener su equipo con herramienta antivirus que sea de la organización o en todo caso otro que este debidamente licenciado.
- El usuario no deberá desinstalar ningún programa antivirus de su computadora ya que deja vulnerable y en riesgo de seguridad ante el peligro de virus.
- Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por el programa Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
- El usuario que cuente con una computadora con recursos limitados, contará con la versión ligera del programa Antivirus organizacional.
- Queda prohibido bajar o instalar otra herramienta antivirus que no este debidamente licenciada o autorizada por los encargados correspondientes.

- El usuario deberá comunicarse con el Departamento de Redes y soporte Técnico así como el Departamento de Sistemas de su dependencia en caso de problemas de virus para buscar la solución.

4.6.4. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total o reparación del daño.

V. Generales.

5.1.0. Objetivo.

Formar a todos los usuarios de la Organización con ética y cultura sobre importancia que es cuidar la seguridad de la información.

5.1.1. Alcance.

Aplica a todo el personal encargado de cada área, tales como directivos y responsables así como usuarios internos y externos a la Organización.

5.1.2. Política.

- Cada uno de los departamentos deberán de emitir los planes de contingencia que correspondan a las actividades críticas que realicen.
- Debido al carácter confidencial de la información, el personal del Departamento de Sistemas deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

5.1.3. Sanción.

Aplica para cualquier empleado o directivo que se haya encontrado violando esta política se hará de acuerdo a la gravedad, que va desde suspensión de días de labor, suspensión total o reparación del daño.

5.2 Plan de emergencia

PROCEDIMIENTO GENERAL DE CONTINGENCIA

Objetivo:

Describir los lineamientos para proteger al personal, la información y los equipos e instalaciones del departamento de sistemas de información ante la presencia de una amenaza.

Alcance:

Aplica desde el momento en que se presente una contingencia, hasta lograr restablecer las operaciones de la empresa a una situación normal para el personal, las instalaciones y equipos del departamento de sistemas de información.

Responsables:

Responsable de elaboración: Jefe de servicios de cómputo.

Responsable de ejecución: Personal del departamento de sistemas de información.

Responsable de aprobación: Gerente de sistemas de información.

Definiciones:

Contingencia en el área de sistemas de información: Situación de emergencia que puede causar daños, por ejemplo, a una computadora, la destrucción total o parcial del Site y pérdida de la información e interrupción de las operaciones.

Recuperación del site: Son las operaciones que se deben realizar para rehabilitar o poner a punto las instalaciones, servidores y equipo.

Site propio: Lugar físico en donde se encuentra instalada la computadora central y los servidores de la red.

Site alterno: Lugar físico en donde se encuentra la computadora central y los servidores de red similar en caso de pérdida temporal del site propio.

5. Procedimiento:

Personal de sistemas de información.

5.1 Al presentarse una contingencia en el área de sistemas de información proceda de acuerdo al tipo de contingencia de que se trata.

Externos:

- Inundaciones
- Temblores
- Incendios

Internos:

- Robo
- Sabotaje
- Destrucción
    - De datos / información
    - De recursos
- Huelgas
- Corte de energía
- Errores del usuario
- Virus Informáticos

5.2 Evalúe los daños que causo la contingencia para determinar si es necesario requerir del site alterno de acuerdo a las siguientes condiciones:

a) Si después de cualquier contingencia equipos y/o por lo menos 2 servidores no están disponibles para operar por haber sufrido un daño o desperfecto, y el tiempo de recuperación es mayor a 3 días laborales continuos.

b) Si se debe apagar el equipo o interrumpir el suministro de energía eléctrica para reparación, reinstalación, inspección etc. y el periodo de esperar es mayor a 3dias laborales continuos.

c) si la red de equipo e instalaciones se efectuara en un periodo mayor a 3 días laborales continuos.

5.3 En caso de no cumplirse las condiciones para uso del site alterno, ejecute las acciones correspondientes para corregir los daños q causo la contingencia hasta que esta termine.

5.4 Si se cumplen las condiciones para requerir del site alterno, ejecute el procedimiento “Uso del site alterno”.

5.4.1 Una vez operando en el site alterno, ejecute las acciones para recuperar el site propio realice el procedimiento “recuperación del site propio”.

5.4.1.1 Cuando el site Propio se restablezca, el gerente del sistema de información, informará al director general y al director de finanzas y administración que se abandonará el site alterno para regresar al propio.

5.5 Una vez que el site propio o ya corregidos los daños de la contingencia, continúe con las operaciones normales de trabajo.

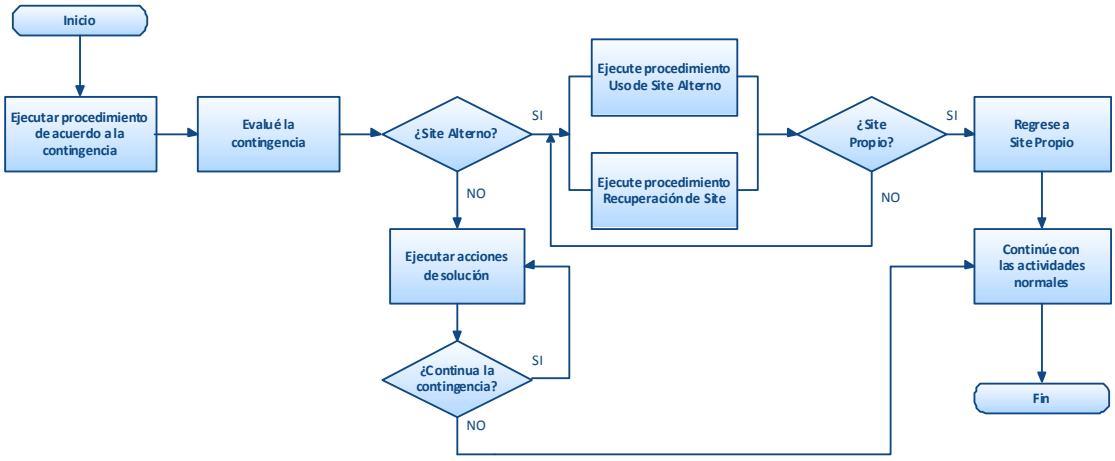

Figura No.2 Procedimiento General de Contingencia.

RIESGOS EXTERNOS:

CONTINGENCIA VS INUNDACIONES.

Objetivo:

Establecer las actividades que se deben seguir al presentarse una inundación, la cual afecta la continuidad de las operaciones de una empresa.

Alcance:

Aplica para el departamento de Sistemas de Información ante la posibilidad de que el agua acabe con los recursos del sistema hasta el traslado al Site Alterno.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[E.1] Daños por Agua	
Activos Afectados: • Equipos informáticos (hardware) • Redes de comunicación • Soportes de información • Equipamiento auxiliar • Instalaciones	Dimensiones: 1. Disponibilidad 2. Trazabilidad de los servicios 3. Trazabilidad de los datos
Descripción: Inundaciones, escapes, fugas: Posibilidad de que el agua acabe con los recursos del sistema.	

Procedimiento:

1. Apague y desconecte equipos y aparatos encontrados en el Site y departamento de sistemas, des energice el Site. Avise al personal del departamento de mantenimiento para que desconecte la energía eléctrica del área.

2. Si es posible, lleve los equipos a un lugar alto para que no se mojen.
3. Evacue el departamento de sistemas de información.
4. Diríjase a algún alto llevando los documentos importantes y su plan de contingencia.
5. Aléjese de los lugares en que se pueden producir deslizamientos.
6. No cruce quebradas o acequias y zonas inundadas.
7. Aléjese de los postes de tendido eléctrico caídos en áreas inundadas.
8. Una vez fuera del edificio, asegúrese de que todos los miembros del departamento estén fuera de las instalaciones.
9. Espere la indicación de acceso al edificio, mientras los especialistas inspeccionan el área, con el fin de prevenir un deslizamiento.
10. No beba agua que no reúna las condiciones higiénicas.
11. No utilice aparatos eléctricos conectados en áreas mojadas o húmedas.
12. Manténgase informado y siga las instrucciones del comité de energía y de las autoridades.
13. Evalúe los daños que causo la contingencia para determinar si es necesario requerir del Site alterno de acuerdo al procedimiento SA_001.

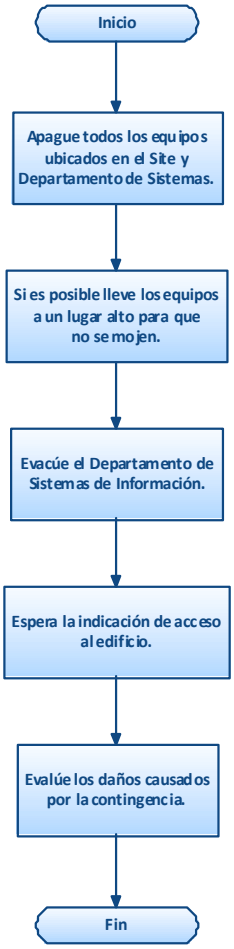

Figura No.3 Contingencia vs Inundaciones.

CONTINGENCIA VS TEMBLORES.

Objetivo:

Establecer las actividades que se deben seguir al presentarse incidentes que se producen sin intervención humana, la cual afecta la continuidad de las operaciones de una empresa.

Alcance:

Aplica para el departamento de Sistemas de Información ante la presencia de fallas geológicas activas y la acción de las placas tectónicas y otros incidentes que se producen sin intervención humana y que afectan las operaciones de la empresa.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[E.2] Daños por Terremotos y/o Temblores	
Activos Afectados: • Equipos Informáticos (Hardware) • Redes de Comunicaciones • Soportes de Información • Equipamiento Auxiliar • Instalaciones	Dimensiones: 1. Disponibilidad 2. Trazabilidad de los Servicios 3. Trazabilidad de los Datos
Descripción: Otros incidentes: Rayo, Tormenta eléctrica, ciclones, avalancha, corrimiento de tierras, etc.	

Procedimiento:

1. Conserve la calma y Baje los interruptores de energía eléctrica.
2. Si es posible lleve los respaldos de datos, programas, manuales y claves.
3. Espere indicaciones de acceso al edificio.
4. Evalúe los daños causados por la contingencia.

5. Traslade los respaldos de datos, programas, manuales y claves, al Site Alterno u oficinas alternas correspondientes con el propósito de reiniciar operaciones, de acuerdo al procedimiento SA_001.
6. Espere indicaciones de acceso al edificio.
7. Restaure la información de las bases de datos y programas.
8. Revise y pruebe la integridad de los datos.
9. Continúe con las actividades normales.

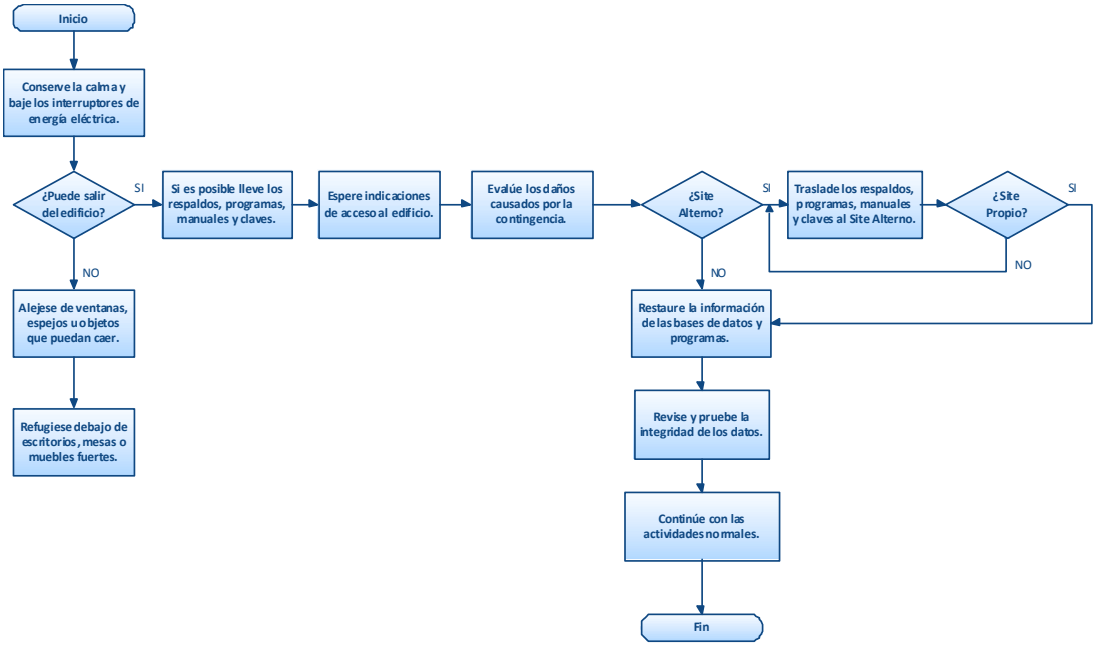

Figura No.4 Contingencia vs Temblores.

CONTINGENCIA VS INCENDIOS.

Objetivo:

Establecer las actividades que se deben seguir al presentarse sucesos que pueden ocurrir de forma accidental o deliberada, derivados de la actividad humana las cuales afectan la continuidad de las operaciones de una empresa.

Alcance:

Aplica para el departamento de sistemas de información ante la presencia de desastres debidos a la actividad humana, tales como incendios, que impiden dar continuidad a las operaciones de la empresa.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

<table>
<tr><td colspan="2">[E.3] Daños por Incendios</td></tr>
<tr><td>Activos Afectados:

• Equipos Informáticos (Hardware)
• Redes de Comunicaciones
• Soportes de Información
• Equipamiento Auxiliar
• Instalaciones</td><td>Dimensiones:

1. Disponibilidad
2. Trazabilidad de los Servicios
3. Trazabilidad de los Datos</td></tr>
<tr><td colspan="2">Descripción:

Incendio: Posibilidad de que el fuego acabe con los recursos del sistema.</td></tr>
</table>

Procedimiento:

1. Conserve la calma y baje el interruptor de energía eléctrica.
2. Si es posible lleve los respaldos de datos, programas manuales y claves.
3. Espere indicaciones de acceso al edificio.
4. Evalúe los daños causados por la contingencia

5. Traslade los respaldos de datos, programas, manuales y claves, al Site Alterno u oficinas alternas correspondientes con el propósito de reiniciar operaciones, de acuerdo al procedimiento SA_001.
6. Espere indicaciones de acceso al edificio
7. Restaure la información de las bases de datos y programas.
8. Revise y pruebe la integridad de los datos.
9. Evalúe los daños causados por la contingencia.

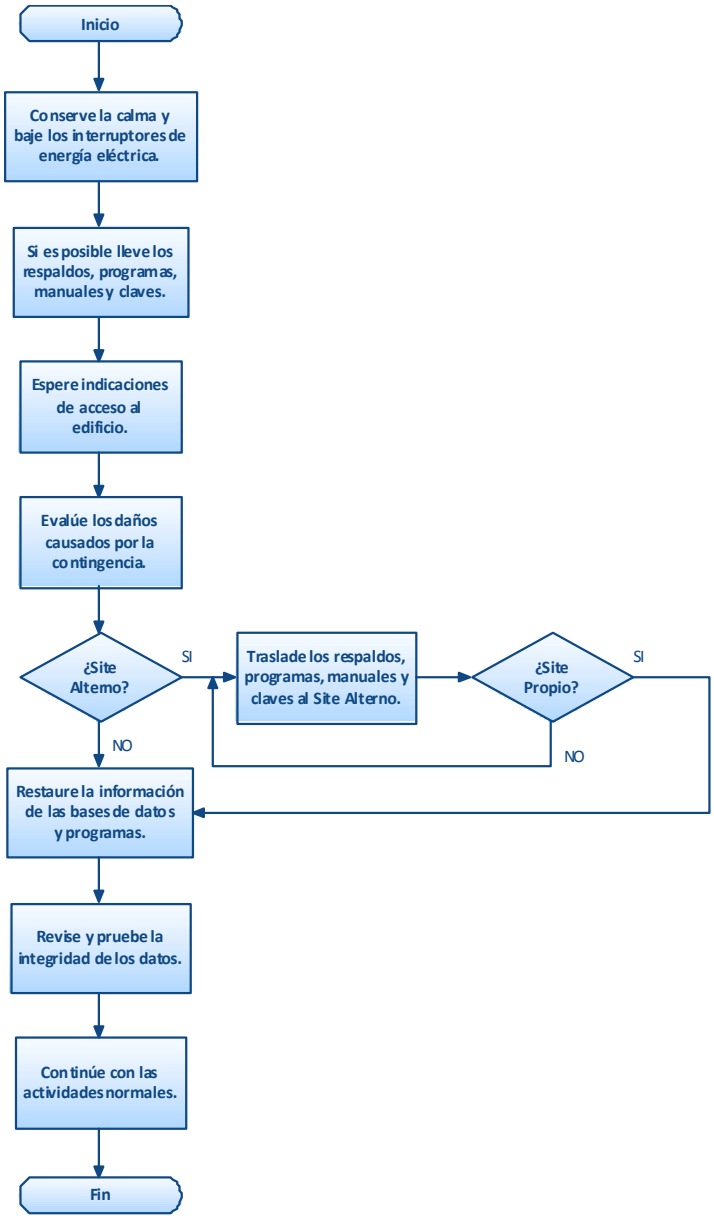

Figura No.5 Contingencia vs Incendios.

RIESGOS INTERNOS:

CONTINGENCIA VS ROBO.

Objetivo:

Establecer las actividades que se deben seguir ante la sustracción ilícita de cualquier recurso y/o información de la empresa.

Alcance:

Aplica para el departamento de sistemas de información ante el robo de un medio indispensable para prestar los servicios que ofrece la empresa.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

<table>
<tr><td colspan="2">[I.1] Daños por Robo</td></tr>
<tr><td>Activos Afectados:

• Equipos Informáticos (Hardware)
• Redes de Comunicaciones
• Soportes de Información
• Equipamiento Auxiliar</td><td>Dimensiones:

1. Disponibilidad
2. Confidencialidad</td></tr>
<tr><td colspan="2">Descripción:

El robo puede realizarlo personal interno, personas ajenas a la empresa o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.</td></tr>
</table>

Procedimiento:

1. Evalúe los daños que causo la contingencia.

2. Instale (sí lo amerita) el sistema operativo y/o programas que hagan falta.
3. Restaure la información de las bases de datos y programas.
4. Revise y/o pruebe la integridad y disponibilidad de los datos.
5. Recupere la información que se localice en los servidores (Software).
6. Si el robo se deriva del equipo (Hardware) se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
7. Corrija las alteraciones que se localicen en los servidores (Hardware).
8. Inicie las operaciones.

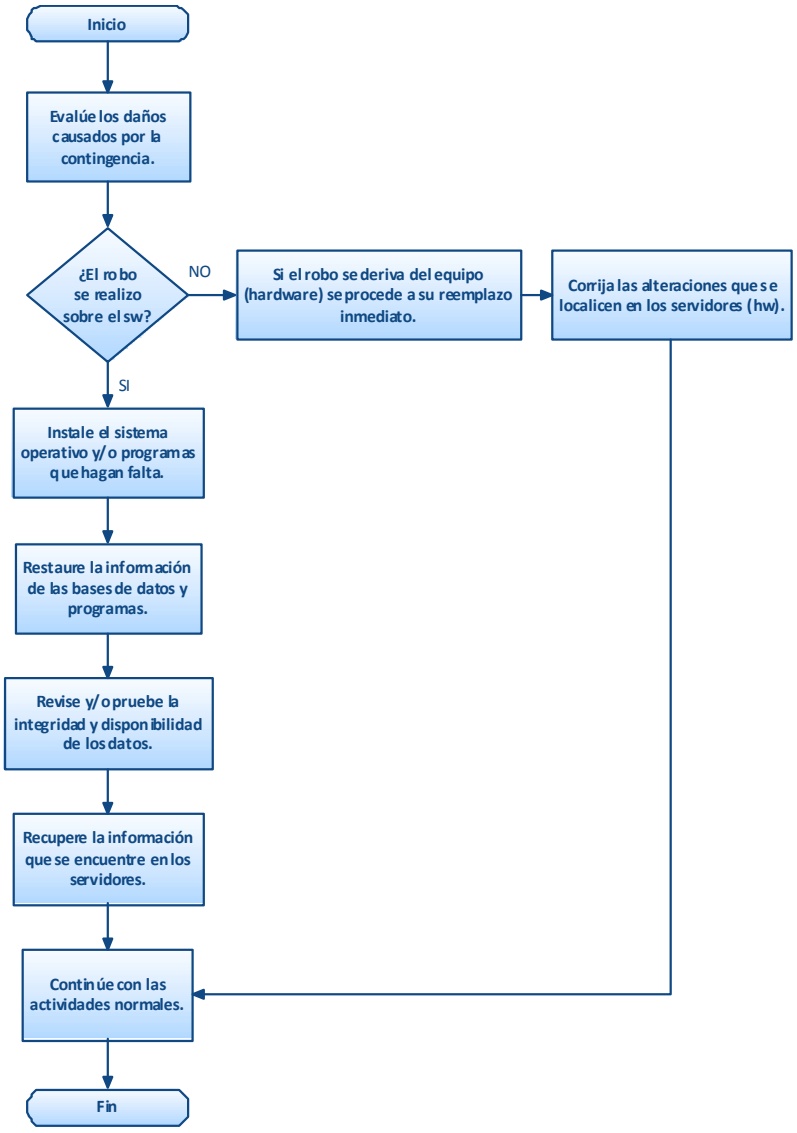

Figura No.6 Contingencia vs Robo.

CONTINGENCIA VS SABOTAJE.

Objetivo:

Establecer las actividades que se deben seguir ante la suspensión mal intencionada de las actividades de la empresa por medio de la destrucción o inutilización de las herramientas de trabajo.

Alcance:

Aplica para el departamento de sistemas de información ante el desperfecto de un medio indispensable para prestar los servicios que ofrece la empresa.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

<table>
<tr><td colspan="2">[I.2] Daños por Sabotaje</td></tr>
<tr><td>Activos Afectados:

• Equipos Informáticos (Hardware)
• Redes de Comunicaciones
• Soportes de Información
• Equipamiento Auxiliar</td><td>Dimensiones:

1. Disponibilidad
2. Confidencialidad</td></tr>
<tr><td colspan="2">Descripción:

Sabotaje: El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones,…</td></tr>
</table>

Procedimiento:

1. Evalúe los daños que causo la contingencia.
2. Verifique que la información de la base de datos y programas se encuentre intacta.
3. Restaure la información de las Base de datos y programas.
4. Revise y/o pruebe la integridad y disponibilidad de los datos.

5. En los casos en que la información eliminada se pueda volver a capturar sin mayor problema se procede conforme a lo siguiente:
   - Capture la información faltante en las bases de datos de los sistemas.
   - Revise y/o pruebe la integridad y disponibilidad de los datos.
6. Inicie las operaciones.

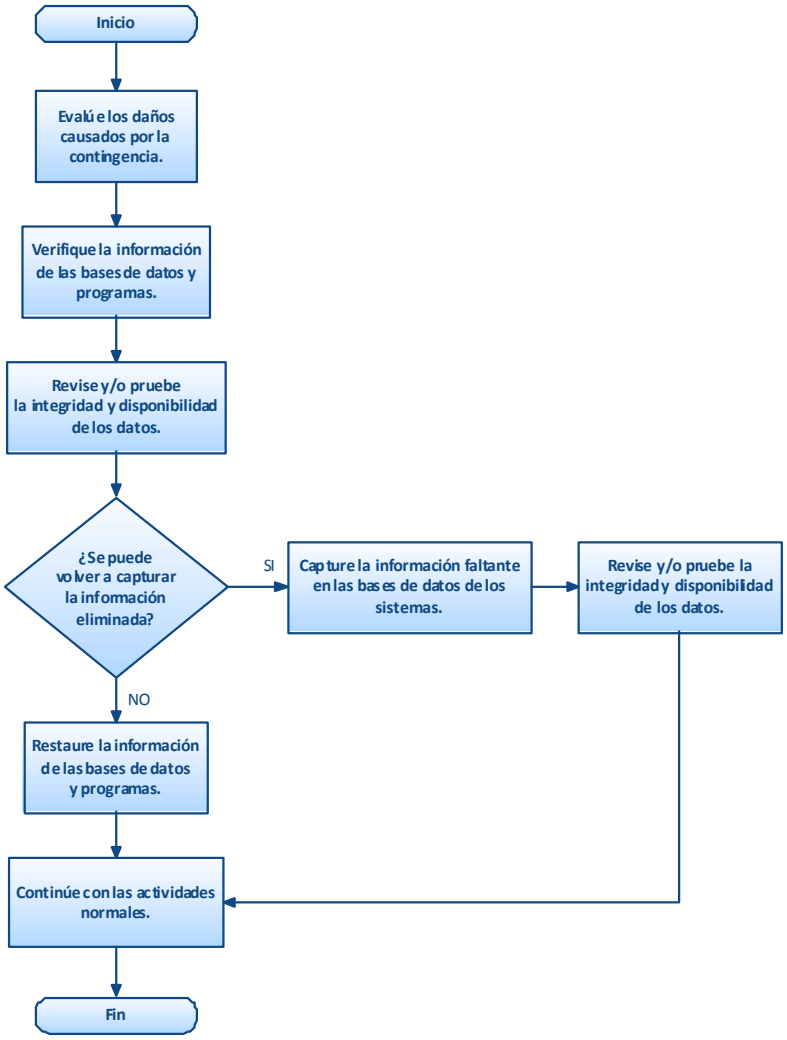

Figura No.7 Contingencia vs Sabotaje.

CONTINGENCIA VS DESTRUCCION DE INFORMACION (SOFTWARE).

Objetivo:

Establecer las actividades que se deben seguir ante la eliminación intencional de información.

Alcance:

Aplica para el departamento de sistemas de información ante la posible destrucción de la información que limite a la empresa a continuar con sus actividades.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[I.3] Daños por Destrucción de Información	
Activos Afectados: • Datos / Información	Dimensiones: 1. Disponibilidad 2. integridad
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	

Procedimiento:

1. Evalúe los daños causados por la contingencia.
2. Revise y/o pruebe la integridad y disponibilidad de los datos.
3. Instale (sí lo amerita) el sistema operativo y/o programas indispensables para la realización de las actividades.
4. Restaure la información de las bases de datos y programas.
5. Corrija las alteraciones que se localicen en los servidores Software.
6. Inicie las operaciones.

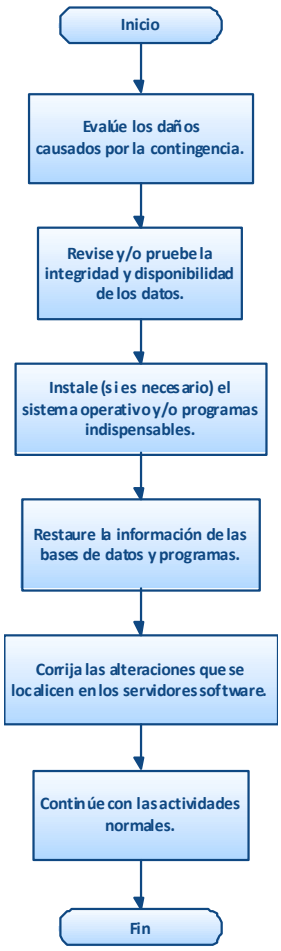

Figura No.8 Contingencia vs Destrucción de Información (Software).

CONTINGENCIA VS DESTRUCCION DE RECURSOS (HARDWARE).

Objetivo:

Establecer las actividades que se deben seguir ante la avería de origen físico o lógico que se presenten en los recursos de la empresa.

Alcance:

Aplica para el departamento de sistemas de información ante la posible destrucción de los recursos que limite a la empresa a continuar con sus actividades.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[I.4] Daños por Destrucción de Recursos	
Activos Afectados: • Aplicaciones (Software) • Equipos informáticos (Hardware) • Redes de comunicaciones • Soportes de información • Equipamiento auxiliar	Dimensiones: 1. Disponibilidad 2. Trazabilidad de los servicios 3. Trazabilidad de los datos
Descripción: Fallos o destrucción en los equipos y/o programas. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	

Procedimiento:

1. Evalúe los daños causados por la contingencia.
2. Revise y/o pruebe la integridad y disponibilidad de los equipos.
3. Si las fallas se derivan del mal funcionamiento de un equipo (Hardware) se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
4. Corrija las alteraciones que se localicen en los servidores Hardware.

5. Inicie las operaciones.

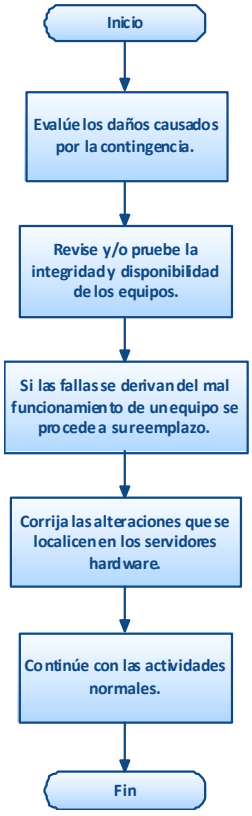

Figura No.9 Contingencia vs Destrucción de Recursos (Hardware).

CONTINGENCIA VS HUELGA.

Objetivo:

Establecer las actividades a seguir al presentarse una huelga que afecte la continuidad de operaciones.

Alcance:

Aplica para el departamento de sistemas de información desde la presencia de huelga hasta el traslado al Site Alterno.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[I.5] Daños por Huelga	
Activos Afectados: • Datos / Información • Personal interno	Dimensiones: 1. Disponibilidad
Descripción: Huelga: Acción emprendida de forma individual, o por un colectivo social, consistente en dejar de hacer alguna actividad o función individual o colectiva, con objeto de ejercer una presión social y alcanzar, así, un objetivo concreto.	

Procedimiento:

1. Al recibir la notificación de que la huelga estallara, el personal del departamento de sistemas de información respalda la información generada en la red y PCs.
2. El operador obtiene los últimos respaldos de información localizados en el servidor correspondiente.

3. El personal de sistemas de información toma los cartuchos de respaldo junto con sus cosas personales, documentos importantes, licencias de software y todo lo que necesite y pueda.
4. Apagar los equipos a su cargo y cierra muy bien el departamento, cajones, gabinetes, etc.
5. El jefe de servicios de computo baja los interruptores de energía o bien avisa al área de mantenimiento para que des energice el departamento de sistemas de información.
6. El jefe de servicios de computo espera el orden del comité general de iniciar los tramites para el uso del site alterno.
7. Una vez recibida la indicación para el uso de site alterno o de cumplirse las condiciones para este, el grupo operativo ejecuta el procedimiento “uso del site alterno” SA_001.

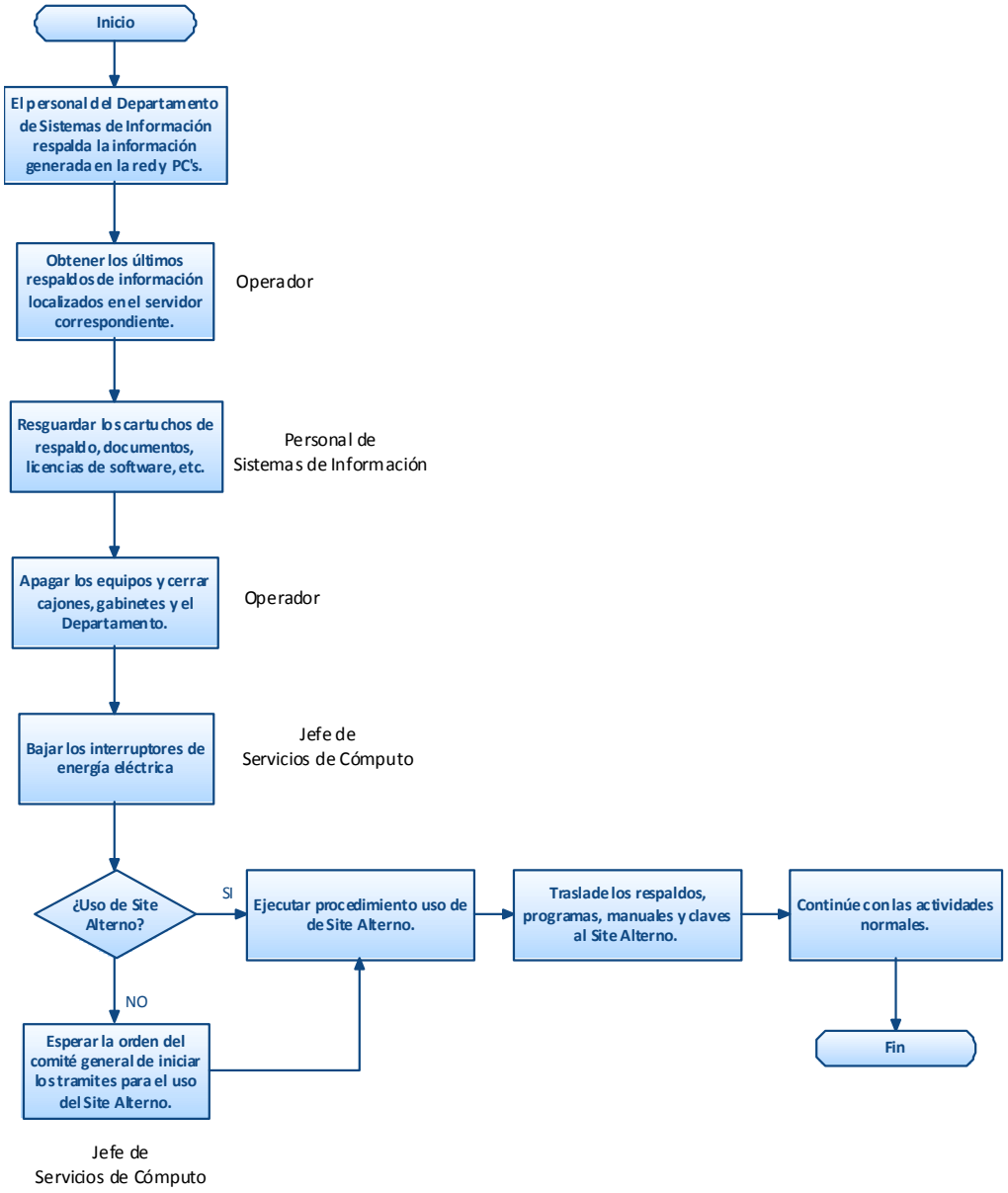

Figura No.10 Contingencia vs Huelga.

CONTINGENCIA VS CORTE DE ENERGÍA.

Objetivo:

Establecer las actividades a seguir al presentarse el cese de la alimentación de la energía eléctrica que afecte la continuidad de operaciones.

Alcance:

Aplica para el departamento de sistemas de información desde la presencia del corte de energía hasta el traslado al Site Alterno.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[I.5] Daños por Corte de Energía	
Activos Afectados: • Equipos informáticos (hardware) • Redes de comunicaciones • Soportes de información (electrónicos) • Datos / Información	Dimensiones: 1. Disponibilidad 2. Integridad 3. Trazabilidad de los servicios 4. Trazabilidad de los datos
Descripción: Corte de energía: Cese de la alimentación de potencia.	

Procedimiento:

1. Revise que la planta de energía cuente con combustible, y se active en su momento.
2. Evalúe los daños que causo la contingencia.
3. Revise y/o pruebe la integridad y disponibilidad de los datos.

4. Si las fallas se derivan del mal funcionamiento de un equipo (Hardware) se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento o en todo caso restaure la información de las bases de datos y programas.
5. Inicie las operaciones.

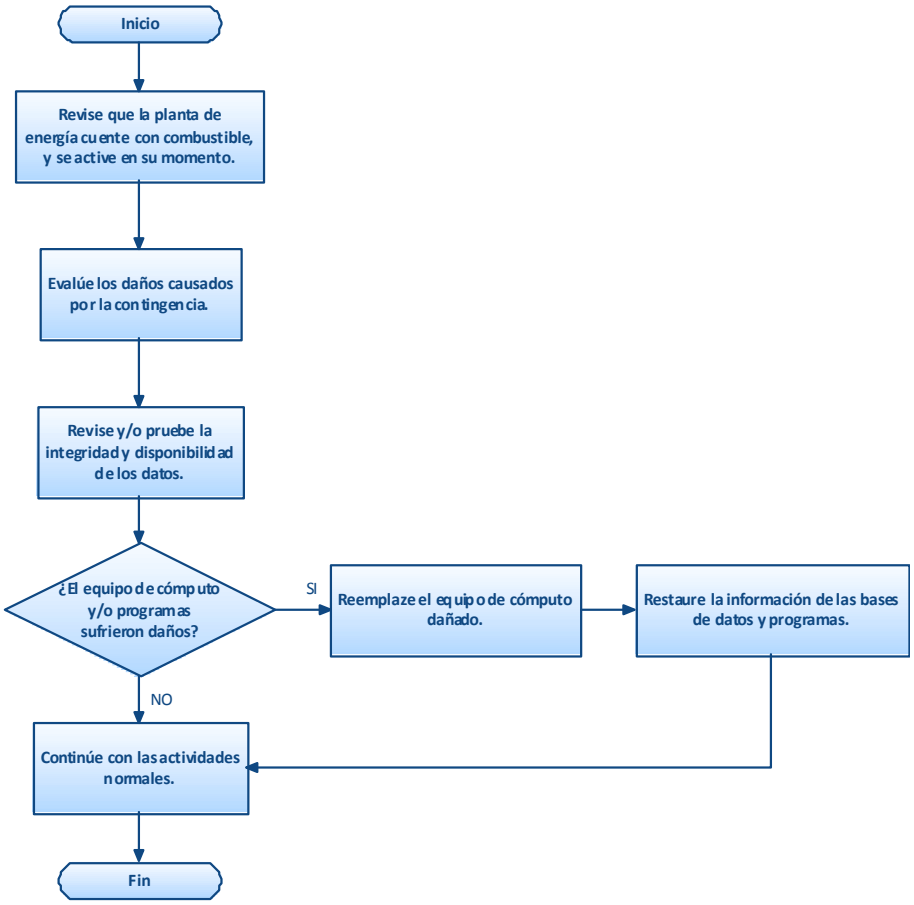

Figura No.11 Contingencia vs Corte de Energía.

CONTINGENCIA VS ERRORES DEL USUARIO.

Objetivo:

Establecer las actividades a seguir al presentarse fallos no intencionados causados por los usuarios.

Alcance:

Aplica para el departamento de sistemas de información desde la presencia del fallo, el cual impide continuar con las actividades normales de la empresa.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[I.6] Daños por Errores del Usuario	
Activos Afectados: • Datos / Información • Servicios • Aplicaciones (Software) • Equipos informáticos (Hardware) • Redes de comunicaciones	Dimensiones: 1. Disponibilidad 2. Integridad 3. Confidencialidad 4. Autenticidad del servicio 5. Autenticidad de los datos 6. Trazabilidad del servicio 7. Trazabilidad de los datos
Descripción: Son aquellos fallos o equivocaciones no intencionales causados por las personas al usar servicios, datos, etc. y/o con responsabilidades de instalación y operación.	

Procedimiento:

1. Evalúe los daños causados por la contingencia.
2. Revise y/o pruebe la integridad y disponibilidad de los equipos.

3. En caso de que el daño sea sobre el software y/o la información sea eliminada o insertada de manera incorrecta se procede a capturarla sin mayor problema conforme a lo siguiente:
   - Instale (si lo amerita) el sistema operativo y/o programas indispensables para la realización de las actividades.
   - Capture los datos faltantes, eliminados o incorrectos en las bases de datos de los sistemas.
   - Revise y/o pruebe la integridad y disponibilidad de los datos.
   - Diríjase a los respaldos de información y actualizar la base de datos.
4. En caso de que los errores se deriven sobre el funcionamiento de un equipo (Hardware) se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
5. Inicie las operaciones.

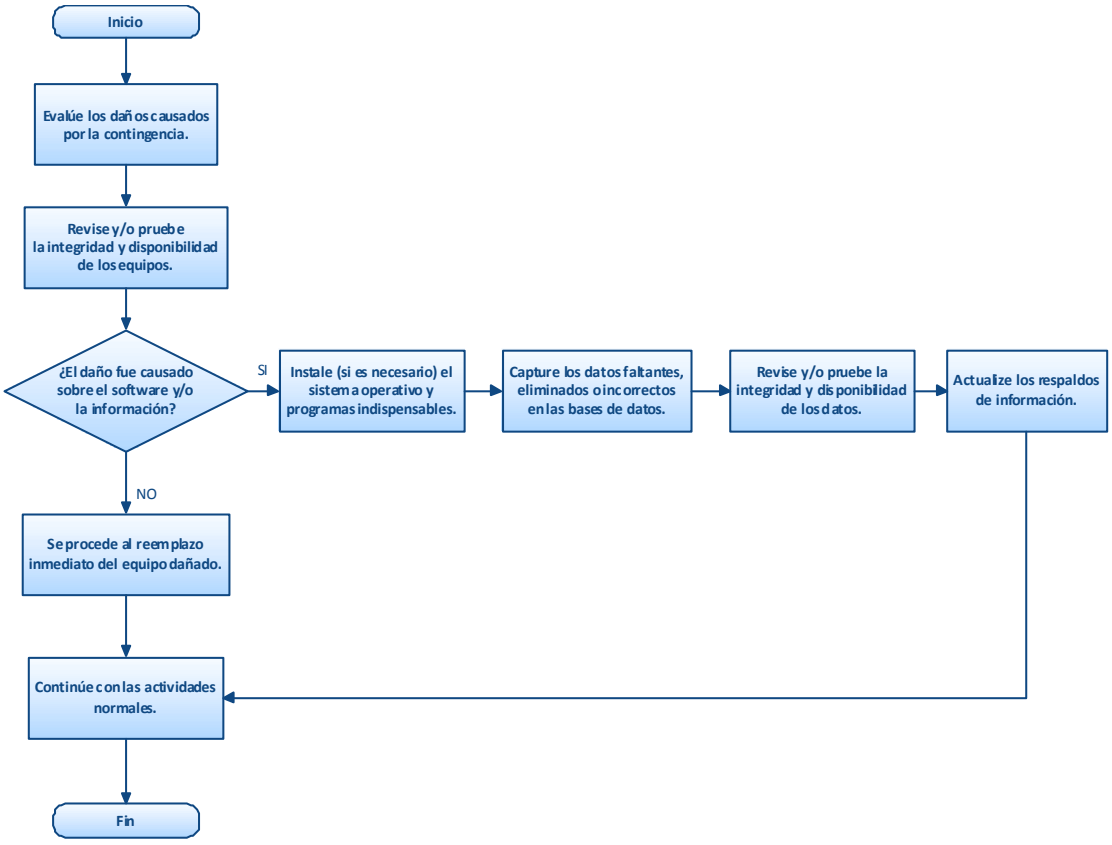

Figura No.12 Contingencia vs Errores del Usuario.

CONTINGENCIA VS VIRUS INFORMÁTICOS.

Objetivo:

Establecer las actividades a seguir al presentarse cualquier anomalía o programas maliciosos que alteren el buen funcionamiento del equipo de cómputo.

Alcance:

Aplica para el departamento de sistemas de información ante la presencia del virus informático, el cual impide continuar con las actividades normales de la empresa.

Responsables:

Responsable de elaboración: Jefe de Servicios de Computo.

Responsable de ejecución: Personal del Departamento de Sistemas de Información.

Responsable de aprobación: Gerente de Sistemas de Información.

[I.7] Daños por Virus Informático	
Activos Afectados: • Datos / Información • Servicios • Aplicaciones (Software)	Dimensiones: 1. Disponibilidad 2. Confidencialidad 3. Integridad
Descripción: Un virus informático: es un programa que puede infectar a otros programas, modificándolos de tal manera que causen daño (borrar o dañar archivos) o afectar su rendimiento o seguridad.	

Procedimiento:

1. En caso de presentarse alguna anomalía por causa de un programa dañino (virus, spyware, gusanos, troyanos, bombas lógicas, etc.) hacer uso del programa antivirus autorizado por la Institución.
2. Evalúe los daños que causo la contingencia.

3. En caso de que el daño sufrido sea mayor, recurrir al personal capacitado (encargado de mantenimiento o personal que el mismo designe) para reparar el daño.
4. En caso de perdida de información o daño de la misma se procede a capturarla sin mayor problema conforme a lo siguiente:
   - Capture los datos faltantes o perdidos en las bases de datos de los sistemas.
   - Revise y/o pruebe la integridad y disponibilidad de los datos.
   - Diríjase a los respaldos de información y actualizar la base de datos.
   - Inicie las operaciones.
5. En caso de que alguna de las aplicaciones sufra anomalías en su funcionamiento se recurrirá al personal capacitado (encargado de mantenimiento o personal que el mismo designe) para que las repare o las reinstale.

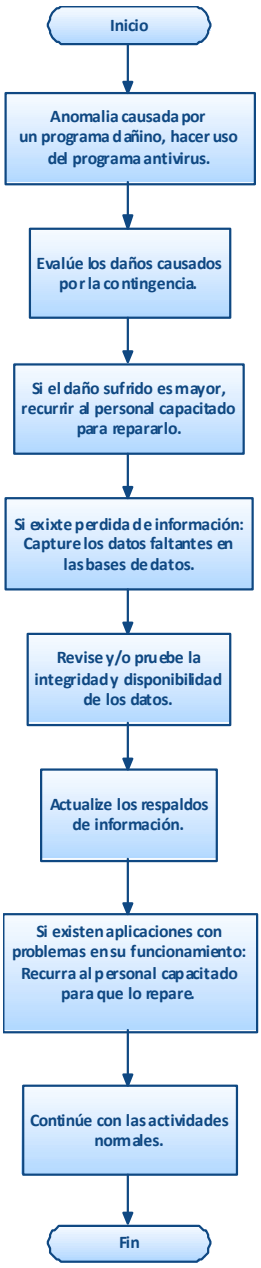

Figura No.13 Contingencia vs Virus Informáticos.

5.3 Plan de recuperación

Para la realización de un plan de recuperación es necesario definir:

- Los equipos necesarios para el desarrollo del Plan.
- Las responsabilidades y funciones de cada uno de los equipos.
- Las estrategias de vuelta a la normalidad.

Organización de los Equipos

Los equipos de emergencia están formados por el personal necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan.

Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se muestran algunos ejemplos de los equipos que pueden formar parte del Plan:

- Comité de Crisis: Encargado de dirigir las acciones durante la recuperación.
- Equipo de Recuperación: Su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.).
- Equipo Logístico: Responsable de toda la logística necesaria en el esfuerzo de recuperación.
- Equipo de las Unidades de Negocio: Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos.
- Equipo de Relaciones Públicas: Encargado de las comunicaciones a los medios de comunicación y clientes.

El personal asignado a cada uno de los equipos puede variar dependiendo del tamaño de la organización y de la estrategia de recuperación seleccionada. Una persona puede pertenecer a más de un equipo, siempre y cuando no existan incompatibilidades en las tareas a realizar.

Equipo Director o Comité de Crisis

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones “clave” durante los

incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente.

Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el Plan de Continuidad.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

Equipo de Recuperación

El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio.

Equipo Logístico

Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al Site Alterno.
- Suministros de oficina.
- Contacto con los proveedores.

Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas.

Equipo de Relaciones Públicas y Atención a Clientes

Se trata de canalizar la información que se realiza al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

- Comunicación con los clientes.

Uno de los valores más importantes de una organización son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.

Equipo de Las Unidades De Negocio

Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.

Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.

Una vez que hemos definido los equipos y se han establecido las funciones que debe desempeñar cada equipo, tenemos que desarrollar los procedimientos que van a seguir.

- Procedimientos de restauración.
- Procedimientos de soporte y gestión.
- Procedimiento del análisis del impacto.
- Procedimientos de vuelta a la normalidad.

Procedimientos de Restauración

Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.

Procedimientos de soporte y gestión

Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

Procedimientos del Análisis del impacto

Pretende realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.

Procedimientos de vuelta a la normalidad

Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento. Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

Una vez solventado el incidente y vuelto a la normalidad, cada equipo deberá realizar un informe de las acciones llevadas a cabo y los tiempos empleados y las dificultades con las que se encontraron, etc.

Toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación del mismo.

Pruebas

El Plan de Continuidad no se considerará válido hasta que no se hayan superado satisfactoriamente las pruebas que aseguren la viabilidad de las soluciones adoptadas. Así como:

- Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la organización.
- Probar la efectividad y los tiempos de respuesta de las pruebas para comprobar que están alineadas con el diseño.
- Identificar las áreas de mejora en el diseño y ejecución de las pruebas.
- Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de la organización.
- Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.
- Concienciación y formación para los empleados a través de la realización de pruebas.

Mantenimiento

Por la propia dinámica de la organización, se van incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas.

La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

ANEXOS

ANEXO I – CUADROS DE RECOPILACION DE DATOS ANÁLISIS DE IMPACTO O CUADRO DE PROCESOS

En este cuadro se recogen los procesos y subprocesos que componen la organización donde se va a desarrollar el Plan de Continuidad.

Proceso	Subproceso	Breve descripción	Frecuencia (Diario/Semanal/Mensual)	Persona responsable

SISTEMAS QUE SOPORTAN EL PROCESO

En este cuadro se recogen los sistemas que soportan el proceso analizado.

Nombre del Sistema	Descripción	Criticidad	Tipo de Sistema (PC/Servidor/ Mainframe)	No. de Equipos con la aplicación	Responsables	Contacto Técnicos

Rangos de Críticos:

1. La organización/departamento no puede funcionar sin el sistema.
2. La organización/departamento no puede funcionar parcialmente sin el sistema.
3. La organización/departamento puede funcionar sin el sistema.

RECURSOS HARDWARE DEL PROCESO

En este apartado se recogen los componentes hardware que soportan los procesos.

Tipo de hardware	Detalles del Modelo/Configuración	Distribuidor	Criticidad	Localización

Rangos de Críticos:

1. La organización/departamento no puede funcionar sin el hardware.

2. La organización/departamento no puede funcionar parcialmente sin el hardware.
3. La organización/departamento puede funcionar sin el hardware.

OTROS ACTIVOS

En este apartado se recogen todos aquellos activos (comunicaciones, datos, infraestructura, etc.), que forman parte del proceso y que son necesarios para dar continuidad al mismo en caso de interrupción.

Descripción	Tipo	Criticidad	Localización

Rangos de Críticos:

1. La organización/departamento no puede funcionar sin el activo.
2. La organización/departamento no puede funcionar parcialmente sin el activo.
3. La organización/departamento puede funcionar sin el activo.

TIEMPO MÁXIMO DE INTERRUPCIÓN

Para cada uno de los procesos, se determinará el tiempo máximo de interrupción, especificando cuántos días puede permanecer el proceso sin incurrir en pérdidas económicas graves.

Proceso	Necesidades de Recuperación	Criticidad

ANEXO II - LISTADO DE RIESGOS

Realizar un listado detallado de los posibles riesgos a los que se encuentre vulnerable la organización, así como complementar esta lista con los nuevos riesgos que se presenten posteriormente. Y así mantenerla actualizada.

ANEXO III – EJEMPLOS DE VULNERABILIDADES

VULNERABILIDADES
Existencia de materiales inflamables como papel o cajas
Cableado inapropiado
Ancho de banda inapropiado
Suministro eléctrico inapropiado
Mantenimiento inapropiado del servicio técnico
Ausencia de mantenimiento
Educación inadecuada del personal en virus y malware
Políticas de firewall inadecuadas
Política de seguridad de la información inadecuada
Ausencia de política de seguridad
Derechos de acceso incorrectos
Ausencia de un sistema de extinción automática de fuegos/humos
Ausencia de Backup
Ausencia de control de cambios de configuración eficiente y efectiva
Ausencia de mecanismos de identificación y autenticación
Ausencia de política de restricción de personal para uso de licencias de software
Ubicación física en un área susceptible de desastres naturales
Carencia de software antivirus
Descarga incontrolada y uso de software de Internet
Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales

Protección física de equipos inadecuada
Personal sin formación adecuada
Incumplimientos legales (LOPD, Ley Sarbanes Oxley, etc.)
Definición de privilegios de acceso inadecuada
Ausencia de un Plan de recuperación de incidentes

ANEXO IV – SA_001 SITE ALTERNO.

Objetivo:

Establecer una guía de actividades para dar continuidad a las operaciones mínimas indispensables en un Site Alterno, en caso de no contar con el propio por una situación de desastre.

Alcance:

Afecta a las áreas descritas en las generalidades del Plan de Contingencia, desde el momento en que la contingencia no permita hacer uso del Site Propio por motivos de desastre, hasta la reanudación de las actividades normales.

Responsables:

Responsable de elaboración: Jefe de servicios de cómputo.

Responsable de ejecución: Personal del departamento de sistemas de información.

Responsable de aprobación: Gerente de sistemas de información.

CONCLUSIONES.

- Un Plan de Contingencia es la herramienta que cualquier empresa debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

- El Plan de Contingencia debe ser un elemento vivo, es decir, deben realizarse pruebas para determinar la eficacia del plan y de los procedimientos de recuperación ante desastres. Las deficiencias deben resolverse y comprobarse inmediatamente.

- En un plan de contingencia, el objetivo consiste en ejecutar varias tareas en el menor tiempo posible. Cualquier deficiencia en la documentación, capacitación o, incluso, en los aspectos administrativos, pone en peligro la continuidad del negocio.

- La puesta en marcha de los planes a seguir es responsabilidad del encargado de la seguridad, pero también debe existir un compromiso por parte de los usuarios del sistema de información, ejecutivos y todas las personas que de alguna u otra forma ayudan a que el sistema cumpla con los requerimientos para el que fue diseñado, manteniendo sobre todo la integridad, disponibilidad y confidencialidad de la información.

- En un Plan de Contingencias se invierte, no se gasta. Se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa

- Aumentar las medidas para garantizar la disponibilidad de los servicios informáticos genera confianza y acerca a los usuarios a la informática.

GLOSARIO.

Amenazas: Las amenazas Informáticas son los problemas más vulnerables que ingresan a nuestra computadora con el hecho de afectarlo.

Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.

Backup: Se refiere a la copia de datos de tal forma que estas puedan restaurar un sistema después de una perdida de información.

Compilación: es un traductor (compilador o intérprete) es un software que lee un programa escrito en un lenguaje (lenguaje fuente) y lo traduce.

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

CRM: Por sus siglas en inglés herramienta para la gestión de relaciones con los clientes.

Desastre o contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Dirección IP: Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora).

Disco Duro: Dispositivo de almacenamiento permanente de información. Este es el que guarda la información cuando apagamos la computadora.

Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Encriptación: Es el proceso mediante el cual una rutina es codificada de tal manera que no pueda ser interpretada fácilmente. Es una medida de seguridad utilizada para

que al momento de transmitir la información ésta no pueda ser interceptada por intrusos.

ERP: Por sus siglas en inglés Software de gestión integral de empresas.

Firewall: es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Gestión de riesgos: selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Intranet: es una red de ordenadores privados que utiliza tecnología Internet para compartir de forma segura cualquier información o programa del sistema operativo para evitar que cualquier usuario de Internet pueda ingresar.

Liga o link: Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor a otro, cuando se navega por Internet o bien la acción de realizar dicho salto.

Operaciones críticas: son todas las actividades de gran importancia para la empresa y que en ausencia de alguna no se podría dar continuidad al negocio.

Recursos críticos: son todos aquellos activos de gran de importancia para la empresa y que en ausencia de alguna no se podría dar continuidad al negocio.

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Site alterno: es el lugar o espacio destinado para darle continuidad a las operaciones en caso de contingencia.

Spyware: es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

SSID: (**S**ervice **S**et **ID**entifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

Trazabilidad de los datos: es una medición para ver ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?.

Trazabilidad de los servicios: es una medición para ver qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

BIBLIOGRAFÍA.

Sitios de Internet

- Kioskea.net (2008). Sistema de Información. Octubre 16, 2008. http://es.kioskea.net/contents/systeme-d-information/si-systeme-d-information.php3

- ONGEI Oficina Nacional de Gobierno Electrónico e Informática. (2009). Enero 07, 2009. http://www.ongei.gob.pe/seguridad/seguridad2_arcgivos/Lib5131/Libro.pdf

- Félix, José de Jesús. (2005). Plan de Contingencia Informático. México, 2005. http://www.gobiernodigital.miguelhidalgo.gob.mx/plan/D-DGD-09%PLAN%20DE%CONTINGENCIA%20INFORMATICO

Libros

- Daltabuit, Enrique. La Seguridad de la Información. Limusa Noriega Editores. México 2007.

- Rodríguez, Luis Ángel. Seguridad de la información en sistemas de cómputo. Editorial Ventura. México, 1995.

- Gratton, Pierre. Protección informática: en datos y programas; en gestión y operación; en equipos y redes; en internet. Editorial Trillas. México, 1998.

- Sub-Jefatura de Informática. Guía Práctica para el Desarrollo de Planes de Contingencia de los Sistemas de Información. Centro de Edición del INEI. Lima 2001.

- Políticas de uso de los Servicios de TI. El Auditor General del órgano de fiscalización Superior del Congreso del Estado de Guanajuato, Guanajuato, Gto., 16 de Enero 2007.

- Gaspar, Juan. Planes de Contingencias La Continuidad del Negocio en las Organizaciones. Ediciones Díaz de Santos. Madrid, Enero 2004.