UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TEMA:

"ANÁLISIS E IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA BASADO EN LA METODOLOGÍA ITIL, EN EL PARQUE INFORMÁTICO DEL GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA"

TESIS PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

POSTULANTES:

- **SÁNCHEZ LOZADA NARCISA PILAR**
- **PILATASIG REMACHE MARIELA DE LOS ANGELES**

DIRECTOR DE TESIS:

ING. PATRICIO NAVAS MOYA

Latacunga, Diciembre 2010

AUTORÍA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de las Autoras, Egresadas: Sánchez Lozada Narcisa Pilar y Pilatasig Remache Mariela de los Ángeles.

Sánchez Lozada Narcisa Pilar

C.C. Nº 180339668-6

Pilatasig Remache Mariela de los Ángeles

C.C. Nº 050248749-9

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración:

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso Profesional de la Universidad Técnica de Cotopaxi, informo que las postulantes: Sánchez Lozada Narcisa Pilar, Pilatasig Remache Mariela de los Ángeles han desarrollado su Tesis de Grado de acuerdo al planeamiento formulado en el plan de Tesis con el tema: **"Análisis e implementación de un plan de contingencia basado en la metodología ITIL, en el parque informático del Gobierno Municipal del Cantón Latacunga"** cumpliendo con los objetivos planeados.

En virtud de lo antes expuesto, considero que la presente Tesis se encuentra habilitada para presentarse al acto de la defensa de Tesis.

Latacunga, 4 de Noviembre de 2010

Atentamente,

Ing. Patricio Navas Moya.
DIRECTOR DE TESIS

CERTIFICADO DE LA INSTITUCIÓN

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA
UNIDAD DE SISTEMAS

CERTIFICACIÓN

Yo, Eduardo Jaramillo Guerra con CI Nº 170715427-2, Jefe de la Unidad de Sistemas del Gobierno Municipal del Cantón Latacunga, Certifico que las señoritas: SANCHEZ LOZADA NARCISA PILAR con CI Nº 180339668-6 y PILATASIG REMACHE MARIELA DE LOS ANGELES con CI Nº 050248749-9, egresadas de la Universidad Técnica de Cotopaxi de la Especialidad Ingeniería Informática y Sistemas Computacionales han concluido con el ***ANALISIS E IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA BASADA EN LA METODOLOGÍA ITIL EN EL PARQUE INFORMÁTICO DEL GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA.***

Dicho trabajo ha sido entregado sujetándose a las especificaciones y requerimientos técnicos solicitados.

Es todo cuanto puedo certificar, pudiendo las interesadas hacer uso lícito del presente documento como lo creyeren conveniente.

Latacunga, 29 de octubre del 2010

Atentamente,

Egdo. Eduardo Jaramillo,
JEFE DE LA UNIDAD DE SISTEMAS

GOBIERNO MUNICIPAL DEL CANTON LATACUNGA
UNIDAD DE SISTEMAS

AGRADECIMIENTO

Al culminar con esta noble y honrada preparación académica, agradezco a Dios por haberme dado la oportunidad de prepararme en esta prestigiosa Institución que acido la cuna del saber y el aprender.

A mis padres, que han sembrado en mí las mejores semillas como son: la bondad, el respeto, y la nobleza; semillas que germinaran como el trigo para el bienestar y el adelanto de nuestra sociedad.

A los docentes que han sabido muy acertadamente dictar sus cátedras y que confiaron en mí capacidad, por lo que en adelante no defraudare porque han sido y serán el Alma Mater de la Universidad Técnica de Cotopaxi.

Mi eterna gratitud para quienes me apoyaron en todo momento, amigos, compañeros y de manera especial a mis Maestros testigos de triunfos y fracasos.

Al Ing. Patricio Navas Moya, que con su elevado conocimiento académico dirigió la elaboración de la Tesis.

A las Autoridades del Gobierno Municipal del Cantón Latacunga, de manera especial al Ing. Eduardo Jaramillo Director del Departamento de Sistemas por la colaboración que supo brindarnos para la elaboración de este Proyecto de investigación.

NARCISA S.

AGRADECIMIENTO

Primeramente doy infinitamente gracias a Dios, por haberme dado fuerza y valor para terminar mis estudios profesionales.

Agradezco también la confianza y el apoyo de mis padres y hermanos, porque han contribuido positivamente para llevar a cabo este difícil trabajo.

A todos los maestros de la Universidad Técnica de Cotopaxi que me impartieron sus valiosos conocimientos, y me ayudaron a crecer como persona y hoy como profesional.

A nuestro Director de tesis Ingeniero Patricio Navas quien con sus conocimientos nos ayudo a culminar con éxito nuestro trabajo de tesis

Un agradecimiento muy especial, al Gobierno Municipal del Cantón Latacunga, por habernos proporcionado la información necesaria para realizar nuestro trabajo de tesis.

MARIELA P.

DEDICATORIA

A mis padres quienes con nobleza y entusiasmo depositaron en mi su apoyo y confianza, desde el inicio de mi vida supieron educarme con amor y paciencia, inculcándome los mejores valores para ser una persona de bien siendo para mí el pilar fundamental durante la vida universitaria puesto que me apoyaron en todo momento con abnegación para poder llegar a cumplir mi meta tan anheladas.

A las personas que Dios me dio como hermanos, las cuales estuvieron pendientes de que llegue a la terminación de mis estudios, ustedes siempre serán mis mejores amigos.

A mí querido esposo Edwin que amo con todo mi corazón, y gracias por brindarme el apoyo necesario para seguir adelante y poder culminar con mis estudios.

NARCISA S.

DEDICATORIA

Este trabajo de tesis que representa un esfuerzo por superarme tanto en mi vida profesional como en lo personal, se lo dedico:

A Dios por que tiene el don de concederme primeramente la vida, que a su vez me da fortaleza espiritual en los momentos difíciles, como también el regalo más hermoso mis dos tesoros Alison y Neiser que son la razón de mi vida.

Muy especialmente con todo mi amor a mis padres quienes me han enseñado con su ejemplo a rebasar todas las barreras que la vida nos presenta, a querer ser mejor cada día, a entender que no hay nada imposible y que sólo hay que esmerarse y sacrificarse, si es necesario, para lograr las metas que nos planteamos.

A mis hermanos que me brindaron su apoyo incondicional y que de una u otra forma contribuyeron a lograr este objetivo.

MARIELA P.

ÍNDICE GENERAL

CONTENIDO **PÁGINAS**

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

CAPÍTULO II

TRABAJO DE CAMPO

CAPITULO III
PROPUESTA

PROPUESTA DE IMPLEMENTACIÓN DE UN MANUAL DE PLAN DE CONTINGENCIA EN EL GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA PROVINCIA DE COTOPAXI

ÍNDICE DE TABLAS

TABLA **PÁGINAS**

ÍNDICE DE GRÁFICOS

GRÁFICOS PÁGINAS

RESUMEN

El presente trabajo investigativo comprende la importancia de implementar un plan de contingencia basado en la metodología ITIL en el parque informático del Gobierno Municipal del Cantón Latacunga (GMCL).

Para determinar los parámetros que rigen el plan de contingencia se establecen Fortalezas, Oportunidades, Debilidades y Amenazas que tienen el nivel de seguridad informático del Gobierno Municipal del Cantón Latacunga, además se Maximizamos riesgos a nivel físico y lógico en el cual se establece parámetros que permiten proteger la infraestructura y la información.

El objetivo del plan de contingencia plantea procedimientos alternativos a la forma de operar normal de una organización. Esta herramienta ayuda a que los procesos críticos del GMCL continúen funcionando a pesar de una posible falla en los sistemas computacionales, o en cualquier evento que se presente.

El presente trabajo deja como constancia un manual en el Gobierno Municipal del Cantón Latacunga para ayuda del Personal Administrativo, que servirá como guía en el memento que exista una contingencia.

SUMMARY

This research includes the importance of implementing a contingency plan based on ITIL in the informatics systemin Municipal Government of the Latacunga town. (GMCL).

In order to determine the parameters governing the contingency plan set Strengths, Weaknesses, Opportunities and Threats which have the computer security level of the Municipal Government of the Latacunga, besides the risk is maximized at the physical and logical parameters that establishes to protect the infrastructure and information.

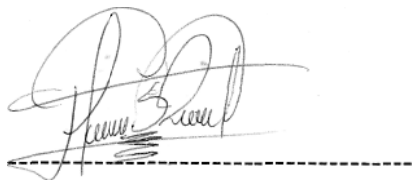
The aim of the contingency plan proposes alternative procedures to the normal mode of operation of an organization. This tool helps GMCL critical processes continue to operate althouth it has a possible failure of computer systems, or any event that arises.

This work left as a manual record in the Municipal Government of the Latacunga town to support administrative staff, which will guide on how to give a solution to the moment there is a contingency.

CERTIFICACIÓN DE TRADUCCIÓN

Yo, Lie. Hipatia Soraya Proaño Álvarez, portadora de la Cédula de Ciudadanía 0502638786, en calidad de Profesional del Área de Inglés, tengo a bien **CERTIFICAR:** que las egresadas de la Universidad Técnica de Cotopaxi, señoritas: Sánchez Lozada Narcisa Pilar portadora de la Cédula de Ciudanía N° 180339668-6 y Pilatasig Remache Mariela de los Ángeles portadora de la Cédula de Ciudadanía N° 050248749-9, han realizado la debida corrección con mi persona del Summary de la Tesis de Grado con el Tema: **"ANÁLISIS E IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA BASADO EN LA METODOLOGÍA ITIL EN EL PARQUE INFORMÁTICO DEL GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA",** el cual se encuentra bien estructurado, por lo que doy fe del presente trabajo.

Por tal motivo faculto a las peticionarias hacer uso del presente certificado como a bien lo consideren.



Licda. Hipatia Proaño
PROFESOR

Latacunga, Noviembre 2010

INTRODUCCIÓN

En la actualidad los cambios tecnológicos adquieren cada vez mayor importancia al interior de las organizaciones, por lo cual se hace necesario o indispensable contar con un plan de contingencias, que garantice el restablecimiento del correcto funcionamiento de los servicios en el menor tiempo posible, ante cualquier eventualidad.

La acción y reacción debe ser la adecuada durante un proceso critico de riesgos, para ello se debería estar en constante prueba, renovación, mantenimiento y retroalimentación del plan de contingencia, nada en la naturaleza es constante siempre se encuentra en continuo cambio, de ahí la importancia en mantener actualizando todos los puntos señalados anteriormente de manera que permita actuar en forma inmediata y oportuna en el momento en que se presente un nivel de riesgo.

Hoy en día lo complejo de los sistemas de información hace que los datos estén expuestos al fenómeno de los virus por el constante movimiento que se dan de un punto a otro. El plan de contingencia debe encaminarse a establecer políticas de seguridad no solo a nivel físico, sino también a nivel lógico.

El motivo de la presente Tesis es desarrollar un estudio del estado actual de la seguridad informática, que en la realidad es un nivel de importancia; para ello se debe considerar la seguridad como un problema que tarde o temprano estamos expuestos y el cual deben invertir tanto capital humano como económico y tecnológico que permita prevenir el daño de información e infraestructura.

El presente trabajo de investigación está establecido en tres capítulos, distribuidos de la siguiente manera:
El capítulo I concerniente a la fundamentación teórica, donde se indica algunos temas informáticos que van dentro del mismo para el desarrollo de la implementación del plan de contingencia

En el capítulo II, se hace referencia a una breve descripción de la Institución, Gobierno Municipal del Cantón Latacunga y al trabajo de campo, donde se aplico los instrumentos de investigación como son: la encuesta realizada al personal del Departamento de Sistemas del Gobierno Municipal del Cantón Latacunga y la entrevista realizada al Administrador del Departamento de Sistemas del Gobierno Municipal del Cantón Latacunga, posteriormente se efectuó el procesamiento de datos, por medio de la tabulación de los mismos, así como su presentación por medio de graficas de pastel, interpretación y análisis de los resultados obtenidos, los mismos que sirvieron de base para la comprobación de la hipótesis planteada.

En el capítulo III, relacionado con la propuesta de investigación se presenta de manera detallada el análisis e implementación del plan de contingencia basado en la metodología ITIl, así como también se enuncia las conclusiones y recomendaciones finales del trabajo de investigación, siendo estos los resultados del trabajo de campo realizado en el Gobierno Municipal del Cantón Latacunga, además se incluye la bibliografía y el glosario de términos para su correcto entendimiento del presente documento.

Finalmente se puede manifestar que se ha cumplido con las expectativas tanto de los investigadores como de los Administradores del Departamento de Sistemas del GMCL, puesto que se logro cumplir a cabalidad con todos los requerimientos técnicos solicitados.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

1.1. Plan de contingencia

1.1.1. Introducción

En realidad, la historia del Plan de Contingencia se presenta ante probables eventos que pueden ser medibles, se debe tener un plan de contingencia, el cual por lo general viene soportado, prevenido y además documentado por las seguridades que previene probables siniestros o ataques a la integridad de la red o de la información. Es importante mencionar que siempre se debe considerar la posibilidad de que los aparatos electrónicos pueden verse afectados por diversos factores como pueden ser eventos naturales o simplemente por descuido. Para este caso se debe tener un plan de contingencia el cual no debe afectar severamente al sistema diario de una empresa o de la Institución.

En algunas ocasiones el prevenir probables eventos aun debidamente analizados con tiempo, las consecuencias de llegar a buenos términos no siempre dependen del administrador de la red, el desarrollo de planes de contingencia de los sistemas de información que comprende: la identificación de riesgos, Calificación de la probabilidad de que ocurra un riesgo, Evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.[1]

[1] http://www.monografias.com/trabajos24/plan-contingencia/plan-contingencia.shtml

Los Planes de Contingencias le permitirán mantener la continuidad de los sistemas de información frente a eventos críticos, de su entidad y minimizar el impacto negativo sobre la misma, para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

Existen diversas situaciones que se deben contemplar a futuro y tener a la mano una probable solución inmediata. Los riesgos que se enfrentaban en la planeación anterior eran desastres con baja frecuencia pero muy alto impacto.

Hoy los riesgos son casi todos de muy alto impacto por las implicaciones que tienen en la empresa ampliada (usuarios de la institución) y de muy alta ocurrencia. Ya todas las empresas están expuestas a ataques con virus, problemas de seguridad en la información, calidad del software, almacenamiento de datos inapropiado, arquitecturas tecnológicas complejas y hasta políticas poco efectivas de administración de recursos que pueden abrirle las puertas a una catástrofe con el mismo impacto en la institución (y hasta mayor) que el impacto causado por una amenaza física como un incendio o un terremoto.

1.1.2. Definición

Según la dirección electrónica: **http://www.ocp.com.ar/plan-de-contingencia.php**: El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos el equipo informático y la información contenida en los diversos medios de almacenamiento[2].

En base al criterio de las investigadoras el Plan de Contingencia es: un conjunto de acciones de los posibles riesgos.

[2] http://www.ocp.com.ar/plan-de-contingencia.php

1.1.3. Características

- ✓ Un buen plan de contingencia debe ser exhaustivo aunque no demasiado detallado; debe guardar un equilibrio entre dar cabida a todos los temas importantes sin inundar el plan de detalles.
- ✓ Debe estar bien estructurado, ser de fácil lectura y, muy importante, cómodo de actualizar. Gran parte del plan estará pensado para la acción, por lo que deberá tener un trazado que muestre claramente lo que hay que hacer, por quién y cuándo.
- ✓ El documento debe tener vida, actualizándose, corrigiéndose y mejorándose constantemente. No se trata de un documento que deba ser revisado exhaustivamente y en fecha fija, sino de un documento que esté en permanente estado de cambio.
- ✓ Es el control de las contingencias y riesgos que se pueden presentan en el área de sistemas.
- ✓ Estas contingencias se pueden evitar atreves de planes y programas preventivos específicos, en los que se detallan las actividades antes, durante y después de alguna contingencia.
- ✓ En estos planes se incluyen los simulacros de contingencias, los reportes de actuaciones y las bitácoras de seguimiento de las actividades y eventos que se presenten en el área de sistemas.

1.1.4. Etapas de un plan de contingencia

Según la dirección electrónica: **http://www.ocp.com.ar/plan-de-contingencia.php.** Las etapas **s**on las siguientes:

Análisis de Riesgos. En esta etapa se determina nuestros límites y se estructuran para su posterior planeación de todos los elementos que interaccionan con el área en la cual se realizara el plan de contingencia, en síntesis "Medir para conocer".[3]

[3] RUSSELL, Ackoff, Plan de contingencia, México, 1981.

Protección de la Instalación. Poder determinar las estrategias comunes de prevención de desastres y de protección en general. En otras palabras la "unificación de los criterios" dentro de la organización.

Estrategia de Respaldo de Sistemas. De la información obtenida por la planificación, poder determinar cuál es el mecanismo para realizar los respaldos y escoger el más conveniente.

Estrategia de Respaldo de Redes. Como motor de la comunicación los sistemas de red, deberán ser revisados cuidadosamente, su: funcionamiento, estructuración, comunicación y sus servicios de tal manera que se pueda rápidamente ser restaurados.

Toma de decisiones en caso de emergencia. Son todas aquellas actividades que se realizan para la recuperación en caso de emergencias, esta etapa se liga de manera directa a la planeación en caso de contingencias.

Mantenimiento y pruebas del plan. En esta etapa se obtendrá el plan de contingencia, pero el cual es necesario:

- ✓ Mantenerlo actualizado.
- ✓ Gente preparada y capacitada en este plan.
- ✓ Ser probado e identificar fallas y errores del mismo.

1.1.5. Ventajas

- ✓ La idea es no ser la única entidad que posea equipo de determinadas marca en el país. Esto es peligroso, ya que en caso de averías o fallas del equipo puede ser difícil y en algunos casos hasta imposible seguir operando sus sistemas de información.

- ✓ Tener conocimientos de si dentro de los posibles “Backups”, existen instituciones dispuestas a respaldar el conjunto de las operaciones de la entidad en sus instalaciones.
- ✓ Verificar cuales institución comparten la tecnología usada por la compañía para la cual labora, con miras a concertar acuerdos de respaldo con ellas.
- ✓ La base tecnológica global, entiéndase: red de comunicaciones, software ambiental y entrenamiento de personal debe estar cubierta. Es decir nada ni nadie debe ser imprescindible.

1.2. Red Eléctrica

1.2.1. Introducción

Para que funcionen adecuadamente, las computadoras necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Por lo general las computadoras toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente Esta corriente es bastante fuerte, siendo una **corriente alterna** (AC), ya que alterna el positivo con el negativo. La mayor parte de las computadoras incluyen un elemento denominado **fuente de alimentación**, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de las computadoras.

La fuente de alimentación es un componente vital de cualquier computadora, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si se detecta una falla en la fuente de alimentación principal.
Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos.
Un corte de la alimentación de la unidad principal puede:

- ✓ **Hacer que desaparezca la información que hay en la RAM**. Los datos recién introducidos o recién editados que no se hayan grabado, se pierden.
- ✓ **Se interrumpe el proceso de escritura en el disco**. Se puede perder información de importancia que necesita el sistema operativo, como puede ser la localización de un archivo, dando como resultado que pierdan o desorganicen archivos.
- ✓ **Puede "aterrizar" un disco fijo.** La cabeza de lectura -escritura de la mayor parte de los discos fijos se separa automáticamente del disco cuando se desconecta la unidad, pero puede ocurrir en algunos sistemas que la cabeza "aterrice" sobre la superficie del disco y la dañe, dando lugar a que se pierdan datos e incluso, resulte dañado físicamente el disco.
- ✓ **Interrumpir impresión.** Cuando vuelva la tensión se han de continuar los procesos de impresión. En algunos casos se ha de volver a comenzar el proceso de impresión.
- ✓ **Se interrumpen las comunicaciones.** Cuando vuelve la corriente, los datos que se estaban transfiriendo entre las computadoras deben de ser comprobados para tener exactitud, y los archivos que se estaban transmitiendo puede que haya que volver a transmitirlos.

1.2.2. Definición

Según la dirección electrónica:
http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf Se denomina red eléctrica al conjunto de medios formados por generadores eléctricos, transformadores, líneas de transmisión y líneas de distribución utilizados para llevar la energía eléctrica a los elementos de consumo de los usuarios.[4]

1.2.3. Determinación de fallas

Las fallas de tipo eléctricos son muchas, las cuales se pueden mencionar a continuación:

- ✓ **Problemas con transformador:** Este problema posiblemente sea el de mayor envergadura, por lo que la falla se determina prácticamente con la falta de suministro eléctrico.
- ✓ **Problemas del tablero general:** Se recomienda que el tablero este adecuadamente rotulado de acuerdo a los circuitos que protege, en el caso del CRA/AI, el tablero general se distingue con facilidad (es una caja color gris empotrado en la pared), el cual, tiene como objetivo proteger de un cortocircuito a los dispositivos conectados a él.
- ✓ **Problema con la tierra:** Si existe problemas con la tierra, es decir, hay inducción de corriente parásita, la única forma de medir la tierra es hacer mediciones con un Ohmiómetro, por lo que la medición deberá hacerlo personal capacitado.
- ✓ **Problemas con el interruptor de las lámparas fluorescentes:** En muchas ocasiones, el interruptor de las lámparas fluorescentes del AI puede fallar, una prueba sencilla es que al accionar en modo encendido y

[4] http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf

no encienden las lámparas existiendo fluido eléctrico al interior del AI, entonces se puede deducir que el interruptor está fallando.

1.2.4. Sistemas alternos de solución.

- ✓ **Mantener en buen estado el U.P.S. (Sistema Ininterrumpible de poder).** Este equipo se utiliza, cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable.
  El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico. Esta unidad hace transparente a las interrupciones de fracciones de segundo que inevitablemente detiene a los sistemas y le permite seguir trabajando durante varios minutos. Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos.
- ✓ **Tablero de Control.** El tablero de control debe ser diseñado de acuerdo al voltaje y corriente que se propone soportar, y debe ser equipado con los dispositivos necesarios de protección contra fallas (térmicos) para proteger al generador de daños, cuando hay fallas o sobrecargas en el sistema.
- ✓ **Extensiones Eléctricas y capacidades** Las computadoras a veces ocupan rápidamente toda la toma de corriente. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- ✓ Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.
- ✓ Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar a limitar el daño ante fallas eléctricas.
- ✓ Adquiera toma corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar tanto con enchufes de patas planas, como cilíndricas.

- ✓ Tanto los toma corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

1.3. Red de datos

1.3.1. Introducción

Red de datos es el conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores.

La Red de Área Local (LAN), lo que limita su cobertura de servicios estrictamente, a través de un proveedor de servicios, se puede tener acceso a la Red Internacional (Internet) para utilizar este recurso como herramienta pedagógica en el proceso enseñanza – aprendizaje y pueda actualizarse algunos temas incluidos en la curricular de cada materia. El objetivo de la Red es el de compartir recursos de Hardware y Software de tal forma de maximizar el uso de los dispositivos. Es por ello, que debe ser de suma importancia el poder detectar las fallas en la red de datos.

1.3.2. Definición

Según el libro de: **RODRIGUEZ Jorge, Introducción a las Redes de Área Local, McGraw Hill, México, 2000. Pag. 23-28.** Dice que: Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos

dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas y archivos. [5]
En base al criterio de las investigadoras la red de datos es: La que permite transmitir información de una computadora a otra.

1.3.3. Diseño de la red de datos

La red de datos posee una topología estrella, el cual posee un dispositivo electrónico que permite interconectar cada nodo (host), este dispositivo se denomina switch de datos, el cual, está instalado en un gabinete de seguridad.
Este switch de datos debe estar encendido para que este dispositivo pueda enviar la información en cada nodo.

La información es transmitida gracias a que cada computadora posee una tarjeta de Red (NIC), el cual es un dispositivo que se encuentra al interior de la computadora.

1.3.4. Detección de fallas

- ✓ **Por problemas eléctricos**: Si hay problemas de suministro de fluido eléctrico, posiblemente se apague el elemento activo de comunicaciones, por lo tanto, el resultado será una caída en la red de datos.
- ✓ **Por problemas en el switch de datos:** Si el elemento activo tiene una falla de tipo eléctrico este no encenderá y se tendrá un problema similar al caso anterior.
- ✓ **Por problemas de puerto:** es posible que por alguna variación de voltaje, se queme una cantidad limitada de puertos, se recomienda verificar los led que indican conectividad.

[5] RODRIGUEZ Jorge, Introducción a las Redes de Área Local, McGraw Hill, México, 2000. Pag. 23-28

- ✓ **Por problemas en la tarjeta de Red:** puede existir la posibilidad de que la tarjeta de Red este fallando, una forma rápida de verificar su funcionamiento es identificar si el led de la tarjeta de Red está funcionando, en caso contrario es posible que la NIC no esté operando adecuadamente. Otro caso probable es que este desactivado desde el sistema operativo.

1.3.5. Estructura básica de una red de datos.

En su estructura básica una red de datos está integrada de diversas partes:

- ✓ En algunas veces de un armario o gabinete de telecomunicaciones donde se colocan de manera ordenada los Hubs, y Pach Panels.
- ✓ Los servidores en los cuales se encuentra y procesa la información disponible al usuario, es el administrador del sistema.
- ✓ Los Hubs, los cuales hacen la función de amplificador de señales, y a los cuales se encuentran conectados los nodos.
- ✓ Los "Pach Panel's", los cuales son unos organizadores de cables.
- ✓ El "Pach Cord", el cual es un cable del tipo UTP solo que con mayor flexibilidad que el UTP corriente (el empleado en el cableado horizontal), el cual interconecta al "Pach Panel" con el "Hub", así como también a los tomas o placas de pared con cada una de las terminales (PC's).

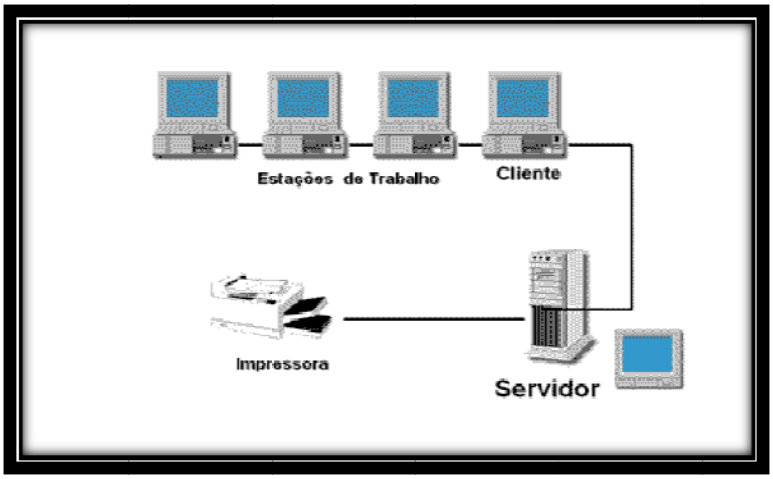
1.3.6. Tipos

1.3.6.1. Redes de área local (LAN)

Constituye una forma de interconectar una serie de equipos entre si. Una LAN no es más que un medio compartido (como un cable al que se conectan todas las computadoras y las impresoras) utilizando un HUB o Switch en un área pequeña que solo requiere comunicación interna entre sus equipos.

Además las LAN proporcionan al usuario varias funciones avanzadas, Administración de los usuarios, y el control de los recursos de la red entre otros.

GRAFICO 1.1: RED DE AREA LOCAL (LAN)



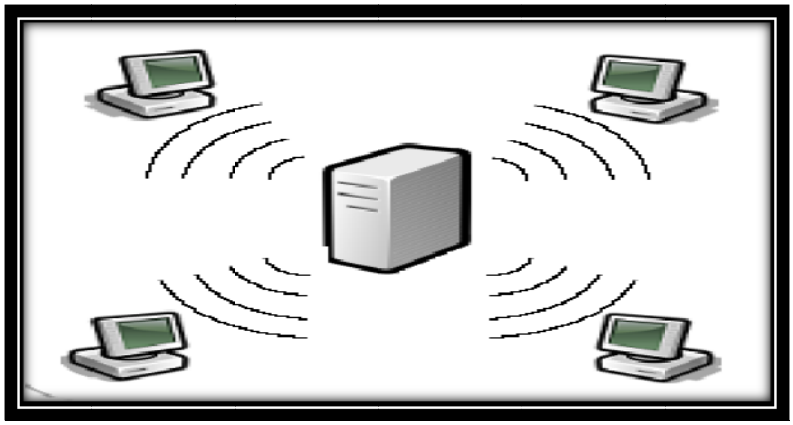
FUENTE:http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf

1.3.6.2. Redes de área extensa (WAN)

Cuando llegamos a un cierto punto donde nuestra red LAN y MAN llegan a ser una herramienta básica de trabajo e importante dentro de nuestra organización provoca que tengamos la necesidad de comunicar nuestros de mas puntos los cuales quedan fuera del alcance de el cableado o de una antena, provoca que tengamos que adquirir nuevo servicios y equipos de comunicación para poder comunicar los demás puntos, en pocas palabras debemos extender nuestra red a WAN.

La velocidad de las señales electrónicas en la mayoría de los medios es cercana a la velocidad de la luz, y esto impone un límite inferior a la latencia de las transmisiones para las transmisiones de larga distancia

GRAFICO 1.2: RED DE AREA EXTENSA (WAN)



FUENTE: http:// 4.bp.blogspot.com/.../RXbaO0kv-BY/s320/WAN.png

1.3.7. Ventajas de las redes.

Una LAN da la posibilidad de que los PC's compartan entre ellos programas, información, recursos entre otros. La máquina conectada (PC) cambia continuamente, así que permite que sea innovador este proceso y que se incremente sus recursos y capacidades.

Las WAN pueden utilizar un software especializado para incluir mini y macro - computadoras como elementos de red. Las WAN no esta limitada a espacio geográfico para establecer comunicación entre PC's o mini o macro - computadoras. Puede llegar a utilizar enlaces de satélites, fibra óptica, aparatos de rayos infrarrojos y de enlaces.

1.4. Problemas del servidor

1.4.1. Definición

Los problemas en el servidor son muchos desde problemas de configuración en el DNS, el DHCP, el ISA Server, el IIS y aún con el protocolo de comunicaciones, además, de agregar problemas de Hardware, tales como, problemas con los discos

duros, tarjetas de Red, Motherboard, entre otros. El objetivo, es poder detectar que tipo de problema posee el servidor y con ello, determinar que acción tomar, en ese sentido.

1.4.2. Fallas generales que pueden darse en el server.

Por problemas de Hardware:

- ✓ Fuente de Poder.
- ✓ Sistemas de almacenamiento.
- ✓ Tarjetas de Red.

1.5. Extensiones y periféricos

1.5.1. Definición

En informática, término utilizado para dispositivos, como unidades de disco, impresoras, módem o joysticks, que están conectados a un ordenador o computadora y son controlados por su microprocesador. A pesar de que el término periférico implica a menudo el concepto de “adicional pero no esencial”, muchos de ellos son elementos fundamentales para un sistema informático. Los teclados, las pantallas y los ratones se consideran también dispositivos periféricos; sin embargo, al ser las fuentes primordiales de entrada y salida, se pueden considerar, más bien, como extensiones del sistema.

1.6. Servidor de internet

1.6.1. *Introducción*

El servicio de Internet permite tener acceso a los recursos de Internet tales como bibliotecas electrónicas, bases de datos, cursos en línea, entre otros.

Los componentes del servicio a Internet son los siguientes: servidor proxy, router y conectividad dado por el ISP. El servidor proxy es un servidor de comunicaciones que permite compartir el acceso a Internet a todas las computadoras del AI, este servicio es entregado por el ISA Server, el cual, al ser configurado en forma adecuada permitirá que todos los nodos de la Red de datos del AI tengan acceso a Internet. El Router es un elemento activo que permite comunicar la red de datos del AI a los servidores de comunicaciones del proveedor de Internet y con ello tener acceso a cualquier servidor que publique información en la Red Internacional.

1.6.2. Definición

Es la maquina principal de la red. Se encarga de administrar los recursos de esta y el flujo de la información. Algunos servidores son dedicados, es decir, realizan tareas específicas. Por ejemplo, un servidor de impresión está dedicado a imprimir; un servidor de comunicaciones controla el flujo de datos, entre otros.
Para que una máquina sea un servidor es necesario que sea una computadora de alto rendimiento en cuanto a velocidad, procesamiento y gran capacidad en disco duro u otros medios de almacenamiento.

1.6.3. Detección de fallas.

- ✓ El servidor proxy genera diversas fallas generando problemas de conexión a Internet, estas fallas son ocasionadas por el mal funcionamiento del sistema operativo.
- ✓ Una forma de detectar que esta fallando el servidor de comunicaciones, es realizar pruebas de acceso a Internet con una computadora que tenga acceso a este servicio sin pasar al Server, para ello, la computadora cliente debe estar debidamente configurado.
- ✓ La conectividad por parte del ISP puede generar problemas, desde su planta externa hasta el router y este a su vez puede tener problemas de Hardware o de Firmware.

1.6.4. Alternativas de solución

- ✓ **Por problemas del sistema Operativo de Red:** bajar el último parche (service pack) disponible en Microsoft.com, otra forma es realizar un diagnóstico para verificar que parche necesita el Server, para ello, utilizar el servicio de Windows Update.
- ✓ **Si el problema es de conectividad por parte del ISP**, será necesario utilizar un MODEM y una línea telefónica como una salida de emergencia para tener acceso a Internet.

1.6.5. Tipos de servidores

En la actualidad existen una variedad de servidores para múltiples aplicaciones, que son utilizadas para instituciones públicas y privadas en las cuales podemos citar los siguientes:

- ✓ Servidor de Base de Datos
- ✓ Servidor Web
- ✓ Servidor de aplicaciones.
- ✓ Servidor de dominio
- ✓ Servidor de correos.
- ✓ Servidor de antivirus
- ✓ Servidor de archivos

1.7. Metodología ITIL

1.7.1. Introducción

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL), es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías de Información. Esta metodología fue desarrollada a petición del Gobierno del Reino Unido a finales de los 80 y

recoge las mejores prácticas en la gestión de los Sistemas de Información. Desde entonces se ha ido extendiendo su uso en toda la empresa privada.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus planes y objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios y centros informáticos de calidad que se correspondan con los objetivos del negocio y de la organización, y que satisfagan los requisitos y las expectativas de los usuarios y clientes.

A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del coste, y el resto se invierte en el desarrollo del producto (u obtención). De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de coste aceptable.

1.7.2. Definición

Según la dirección electrónica:
http://www.monografias.com/trabajos31/metodologia-itil/metodologia itil.shtml: es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías.[6]
En base al criterio de las investigadoras la metodología ITIL es: Una Biblioteca de Infraestructura de Tecnologías de Información.

1.7.3. Características de ITIL

La forma más fácil y rápida de definir ITIL es la siguiente:

- ✓ Es un marco de trabajo de procesos IT no propietario.
- ✓ Es independiente de los proveedores.
- ✓ Es independiente de la tecnología.
- ✓ Está basado en los resultados de las mejores prácticas.

1.7.4. Beneficios de ITIL

- ✓ Permite que las mejoras en calidad sean medibles.
- ✓ Provee una manera consistente de trabajar.
- ✓ Permite estandarizar la terminología.
- ✓ Mejora los procesos de comunicación.
- ✓ Mejora la satisfacción de los clientes y sus expectativas.

[6] http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml:

1.7.5. Ventajas de ITIL para los clientes y usuarios

- ✓ Mejora la comunicación con los clientes y usuarios finales a través de los diversos puntos de contacto acordados.
- ✓ Los servicios se detallan en lenguaje del cliente y con más detalles.
- ✓ Se maneja mejor la calidad y los costos de los servicios.
- ✓ La entrega de servicios se enfoca mas al cliente, mejorando con ello la calidad de los mismos y relación entre el cliente y el departamento de IT.
- ✓ Una mayor flexibilidad y adaptabilidad de los servicios.[7]

1.8. Desastres

1.8.1. *Definición*

Según la dirección electrónica:
http://www.recoverylabs.com/prensa/2007/02_07_expansion.htm. Es un Factor Externo al ser Humano de orden Natural o Tecnológico que puede presentarse en un momento y lugar específico También se puede considerar como un desastre a la interrupción prolongada de los recursos informáticos y de comunicación, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Según el criterio de las investigadoras el desastre es: una medida preventiva que define un proceso de recuperación de los datos.

[7] http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

1.8.2. Análisis del desastre

El análisis de un problema o desastre que antecede para la toma de una acción, de un estudio, de un área de trabajo que conduce casi siempre a la especificación de un nuevo sistema y su posterior diseño.

El proceso de desarrollo y la formación de ciertos campos específicos se destacan los siguientes:

- ✓ **Teoría de desastre.-** ha dado el soporte teórico a los estudios aplicados, a través de la investigación de los resultados de estudios metodológicos y fundamentales.

- ✓ **Ingeniería de desastres.-** dedicado a elaborar las medidas estructurales y técnicas, así como diseñar y adaptar las tecnologías necesarias para afrontar los desastres, reduciendo los riesgos latentes como atendiendo las situaciones de emergencia.

- ✓ **Gestión de desastres.-** busca mejorar y, en su caso, diseñar las estructuras organizacionales y organismos sociales, así como establecer los procesos de gestión, atreves de la elaboración de las metodologías pertinentes, el análisis de la toma de decisiones y el establecimiento de sistemas de soporte informático para determinar y enfrentar los problemas de prevención y atención de emergencia.

1.8.3. Tipos de desastres

Los desastres pueden ser de diversas características, a continuación se detallan en la tabla 1.1, los desastres más probables juntos con sus incidentes, los cuales pueden ser ocasionados por el hombre como por la naturaleza del medio físico en el que se encuentra ubicado el centro de procedimientos o lo que está bajo riesgo.

Estadísticas recientes sobre los tipos más comunes de desastres.

TABLA 1.1 TIPOS DE DESASTRES

TIPOS	INCIDENTES FRECUENTES
Fuego	Varios
Daños por agua	Tubería rota, goteras en el techo y drenajes tapados.
Eléctricos	Corto circuitos, mala instalación, sobre voltajes.
Fenómenos naturales	Tormentas, inundaciones.
Seguridades	Virus, password del sistema.
Errores en el software:	Mala instalación de los programas.
Errores en el hardware	No requieren el debido mantenimiento.
Interrupción de servicio en la red:	Cableado mal estructurado.

1.8.4. Recuperación de desastres

En la tecnología de la información, recuperación de desastres se define como un conjunto de acciones que se toman en el caso de que un desastre mayor ocurra, causando cortes imprevistos y la posible pérdida de datos importantes. Los procedimientos y planes de acción para el caso de una posible falla o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora. Cuando ocurra una contingencia es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. Los procedimientos de planes de recuperación

de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Los desastres pueden incluir casos relacionados con las computadoras tales como ataques de hackers y virus de computadoras, cuestiones eléctricas tales como fallas en el suministro eléctrico y cortes de cables subterráneos resultando en esos fracasos, y los desastres naturales tales como incendios, inundaciones y terremotos.

El error humano también puede causar pérdida de datos y piezas vitales de información como las redes y los sistemas de computadoras pueden estar caídos por un tiempo. Hay, sin embargo, pasos que pueden ser tomados para planear para la recuperación del desastre y ayudar a prevenir la ocurrencia de esos desastres.[8]

1.9. Seguridad informática

1.9.1. Definición

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

Es evidente que es necesario establecer una política adecuada de copias de seguridad en cualquier organización; al igual que sucede con el resto de equipos y sistemas, los medios donde residen estas copias tendrán que estar protegidos

[8] http://www.recoverylabs.com/prensa/2007/02_07_expansion.htm

físicamente; de hecho quizás deberíamos de emplear medidas más fuertes, ya que en realidad es fácil que en una sola cinta haya copias de la información contenida en varios servidores.

1.9.2. Tipos de seguridades

1.9.2.1. Seguridad física

Cuando se quiere tener un equipo seguro es importante considerar todos los aspectos que están involucrados. Uno de ellos y sin duda, uno de los más importantes es la seguridad que se brinda en el entorno donde está ubicado el equipo.

El punto más débil que tienen la mayoría de los equipos es su consola. Siempre se asume que la persona que está ubicada en frente de la consola, es la persona que administra el equipo o tiene pleno conocimiento del funcionamiento del mismo. Desde la consola se pueden realizar tareas como:

- ✓ Apagar el equipo y dejar sin servicio a los usuarios
- ✓ En el caso de Linux reiniciar el equipo en un modo en particular (nivel de ejecución 1)
- ✓ Insertar un diskette dentro del equipo y arrancar el mismo leyendo del diskette, para acceder con otro sistema operativo.
- ✓ Acceder a la configuración de hardware del equipo (BIOS)[9]

[9] PERKINS, Charles, Seguridad de información; Madrid, Ediciones MCGRAW-HALL tercera Edición 2003.

1.9.2.2. Seguridad lógica

Es la configuración adecuada del sistema para evitar el acceso a los recursos y configuración del mismo por parte de personas no autorizadas, ya sea a nivel local o vía red. Mucha gente considera que seguridad es solamente la seguridad lógica, pero este concepto es erróneo.[10]

Entre los puntos más importantes a tomar en cuenta para la seguridad lógica tenemos (algunos aplican principalmente a servidores, otros a cualquier ordenador):

- ✓ Utilización de un sistema operativo relativamente seguro (NT, 2000, UNIX, Linux, entre otros.)
- ✓ ELECCION DE BUENOS PASSWORDS (es el principal)
- ✓ Activado del protector de pantalla con password cuando el equipo queda desatendido y hacer logoff antes de retirse del mismo
- ✓ Utilización de un buen firewall
- ✓ Utilización de antivirus y detectores de troyanos
- ✓ Utilización de dispositivos de identificación por biométrica (huellas dactilares, escaneo de retina, reconocimiento de voz).

1.10. Controles informáticos

1.10.1. Definición

Según la dirección electrónica:
http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml#_Toc475957356. Los Controles se establecen en las actividades, con el fin de involucrar las acciones conducentes a reducir los riesgos. Estos deben ser

[10]http://www.segu-info.com.ar/logica/seguridadlogica.htm

suficientes, comprensibles, eficaces, económicos y oportunos. Conocer la naturaleza de los riesgos, la frecuencia y las consecuencias que traen, permite establecer la mejor forma de tratarlos a través de una acción de prevención o mecanismos de Control, de tal forma que las actividades y el proceso mantengan el curso trazado para alcanzar los objetivos de la entidad.

1.10.2. Tipos de controles

1.10.2.1. Controles preventivos

Actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos.

1.10.2.2. Controles detectivos

Se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o computarizados. Generalmente sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos.

Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los servidores públicos.

1.10.2.3. Controles correctivos

Permiten el restablecimiento de la actividad después de ser detectado un evento no deseable y la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan y permiten mejorar las

deficiencias; por lo general actúan con los controles Detectivos, implican reprocesos y son más costosos porque actúan cuando ya se han presentado hechos que implican pérdidas para la entidad. La mayoría son de tipo administrativo y requieren políticas o procedimientos para su ejecución.[11]

1.11. Análisis de riesgo

1.11.1. Introducción

El análisis de riesgo es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización o empresa. Es la identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con un sistema de información (activos) para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede afectar a la organización.

Es importante crear escenarios de ataque, imaginar amenazas a los activos, pensar cómo un atacante se enfrentaría a nuestros sistemas o activos. Es importante plantear diferentes situaciones dependiendo del perfil técnico del atacante o de sus recursos técnicos y humanos. Estos escenarios de ataque o dramatizaciones son importantes para evaluar impactos y riesgos.

El análisis de riesgo supone más el hecho de calcular la posibilidad de que ocurran casos negativos. La evaluación de riesgos y presentación de propósitos se prepare

---

11 http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml#_Toc475957356

de acuerdo al listado de los riesgos y las alternativas de solución que permitan minimizarlos.

1.11.2. Definición

Los análisis de riesgos, por tanto, tratan de estudiar, evaluar, medir y prevenir los fallos y las averías de los sistemas técnicos y de los procedimientos operativos que pueden iniciar y desencadenar sucesos no deseados (accidentes) que afecten a las personas, información, los bienes y el medio ambiente. El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles.

1.11.3. Tipos de análisis de riesgos

Con carácter previo, y en función de lo comentado en entradas anteriores, podemos clasificar los riesgos según la existencia o no con carácter previo de salvaguardas o controles dentro de la organización:

1.11.3.1. Riesgo intrínseco

Evaluado antes de aplicar las salvaguardas y existente, por tanto, en todas las organizaciones con independencia del sector en el que operen.

1.11.3.2. Riesgo Residual

Evaluado después de aplicar las salvaguardas. Una vez identificados los riesgos, el siguiente paso es decidir qué tipo de análisis de riesgos elegir, según la posibilidad o no de cuantificar económicamente los daños producidos en una organización tras producirse un impacto.
Esta aproximación nos ofrece dos vías:

- ✓ **Análisis de riesgo cuantitativo**: Un modelo cuantitativo habitual es aquel en el que las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto, en función de la estimación del coste económico que supone para la organización.

- ✓ **Análisis de riesgos cualitativo**: Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en términos subjetivos (Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo). Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores (pérdidas económicas efectivas, pérdida de conocimiento, pérdida de competitividad, interrupción de negocio, pérdida de información.

1.11.4. Técnicas de análisis de riesgos

- ✓ Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- ✓ Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- ✓ Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- ✓ Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- ✓ Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- ✓ Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.

1.11.5. Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

1. Construir un perfil de las amenazas que esté basado en los activos de la organización.
2. Identificación de los activos de la organización.
3. Identificar las amenazas de cada uno de los activos listados.
4. Conocer las prácticas actuales de seguridad
5. Identificar las vulnerabilidades de la organización.

    - Recursos humanos
    - Recursos técnicos
    - Recursos financieros

6. Identificar los requerimientos de seguridad de la organización.
7. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.
8. Detección de los componentes claves
9. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

    - Riesgo para los activos críticos
    - Medidas de riesgos
    - Estrategias de protección
    - Planes para reducir los riesgos.[12]

[12] http://www.estade.org/desarrollosustentable/EIA%20OCP/Sec%206/Sec6_final_maa_Rev.%202_fin.pdf

CAPITULO II

TRABAJO DE CAMPO

2.1. Gobierno Municipal del Cantón Latacunga

2.1.1. Antecedentes

El Gobierno Municipal del Cantón Latacunga fue construido en el año de 1910 y concluye en 1936. En su estructura interna se utilizó piedra pómez, material propio de la región. En la primera planta encontramos elementos dóricos y en la segunda elementos corintios que le dan un estilo neoclásico. En su interior existe un elegante salón decorado, junto a sus graderías de piedra dos sobrias pinturas murales con temas de carácter cívico-patrióticos.

El Gobierno Municipal del Cantón Latacunga, esta tallada con piedra volcánica o "pómez", como se puede ver en La Catedral o en la Municipalidad, ambientadas con estrechas calles adoquinadas, resaltadas por los vivos colores de las típicas fachadas de sus viviendas y el polvoriento paisaje circundante. El Gobierno Municipal del Cantón Latacunga está ubicado entre las calles Sánchez de Orellana junto al parque “Vicente León” en el centro de la ciudad.

2.1.2. Funciones

- ✓ Recabar y preparar información económica, financiera y administrativa para las gestiones con autoridades y dependencias municipales.
- ✓ Ilustrar criterios sobre temas estratégicos de la Municipalidad.
- ✓ Efectuar consultas económicas, financieras y administrativas de cualquier índole para preparar resoluciones.
- ✓ Realizar contactos políticos e institucionales para manejo municipal.

2.1.3. Políticas

Se adoptan las siguientes políticas de trabajo:

- ✓ Concertación de los diferentes actores sociales, para el logro de una participación efectiva en el desarrollo de la ciudad;
- ✓ Movilización de esfuerzos para dotar al Municipio de una infraestructura administrativa, material y humana que permita receptar y procesar adecuadamente los efectos de la descentralización;
- ✓ Fortalecimiento y desarrollo municipal, a base de un óptimo aprovechamiento de los recursos y esfuerzos sostenidos para mejorar e incrementar los ingresos de recaudación propia, impuestos, tasas, contribuciones, etc., que permita el autofinanciamiento de los gastos, mediante un proceso de gerencia municipal;

2.1.4. Objetivos.

Se establece los siguientes objetivos institucionales:

- ✓ Procurar el bienestar de la colectividad y contribuir al fomento y protección de los intereses locales;
- ✓ Planificar e impulsar el desarrollo físico del cantón y de sus áreas urbanas y rurales;

- ✓ Acrecentar el espíritu de integración de todos los actores sociales y económicos, el civismo y la confraternidad de la población para lograr el creciente progreso del cantón;
- ✓ Coordinar con otras entidades, el desarrollo y mejoramiento de la cultura, la educación, la asistencia social, turismo, medio ambiente y seguridad ciudadana;
- ✓ Investigar, analizar y recomendar las soluciones más adecuadas a los problemas que enfrenta el Municipio, con arreglo a las condiciones cambiantes, en lo social, político, cultural y económico;

2.1.5. Misión.

El Gobierno Municipal del Cantón Latacunga, tiene por misión esencial planificar, implementar y sustentar las acciones de desarrollo del Municipio. Dinamizar los proyectos de obras y servicios con calidad y oportunidad, que aseguren el desarrollo social y económico de la población, con la participación directa y efectiva de los diferentes actores sociales, dentro de un marco de transparencia y ética institucional y el uso óptimo de los recursos humanos altamente comprometidos, capacitados y motivados

2.1.6. Visión.

El Gobierno Municipal del Cantón Latacunga, se constituirá en un ejemplo del desarrollo y contará con una organización interna altamente eficiente, que proporcione productos y servicios compatibles con la demanda de la sociedad, capaz de asumir los nuevos papeles vinculados con el desarrollo, identidad cultural y de género, descentralizando y optimizando los recursos.

2.1.7. Valores.

Los valores institucionales o corporativos son el conjunto de principios, creencias, reglas que regulan la gestión de la organización. Constituyen la filosofía de la institución y el soporte de la cultura organizacional

- ✓ Lealtad
- ✓ Responsabilidad
- ✓ Honestidad
- ✓ Confiabilidad
- ✓ Respeto
- ✓ Eficiencia
- ✓ Oportunidad

2.1.8. Estructura Orgánica

La estructura orgánica del Gobierno Municipal del Cantón Latacunga, comprende los siguientes niveles:

- ✓ Organismo auxiliar (Cabildo Ampliado)
- ✓ Nivel político y de decisión.
- ✓ Nivel asesor
- ✓ Nivel de apoyo
- ✓ Nivel operativo, y
- ✓ Organismo adscrito desconcentrado.

Organismo Auxiliar

El organismo Auxiliar según la ley, es al que le corresponde emitir dictámenes sobre los asuntos de extraordinario interés que les sean sometidos a su consideración por el concejo municipal.

- ✓ El Cabildo Ampliado.

Nivel político y de decisión

Son los encargados de ejercer el gobierno y la administración municipal y constituyen el máximo nivel de autoridad dentro del cantón, en orden al cumplimiento de los fines del Municipio, de conformidad con la ley de Régimen Municipal y la Constitución Política de la República.

Están conformados por las siguientes unidades:

- ✓ El Concejo

- ✓ El Alcalde

Nivel Asesor

Constituyen los cuerpos técnicos consultivos del Municipio, sus relaciones de autoridad son indirectas con respecto a las unidades de operación, están conformados por las siguientes unidades:

- ✓ Las Comisiones
- ✓ Procuraduría Sindica
- ✓ Auditoría Interna
- ✓ Coordinación General
- ✓ Auditoría de Gestión Ambiental
- ✓ Prospección estratégica y proyectos
- ✓ Relaciones Públicas.
- ✓ Secretaría General

Nivel de apoyo

Son aquellos que prestan ayuda a los demás órganos de la Municipalidad. Sus relaciones de autoridad son también indirectas con respecto a las unidades de operación.

Estas conformadas por las siguientes unidades de apoyo:

- ✓ Gestión Administrativa
- ✓ Gestión Financiera

Órganos adscritos desconcentrados

Son aquellos que se mantienen dependientes de la Municipalidad, pero que han sido creados para efectuar un fin específico.

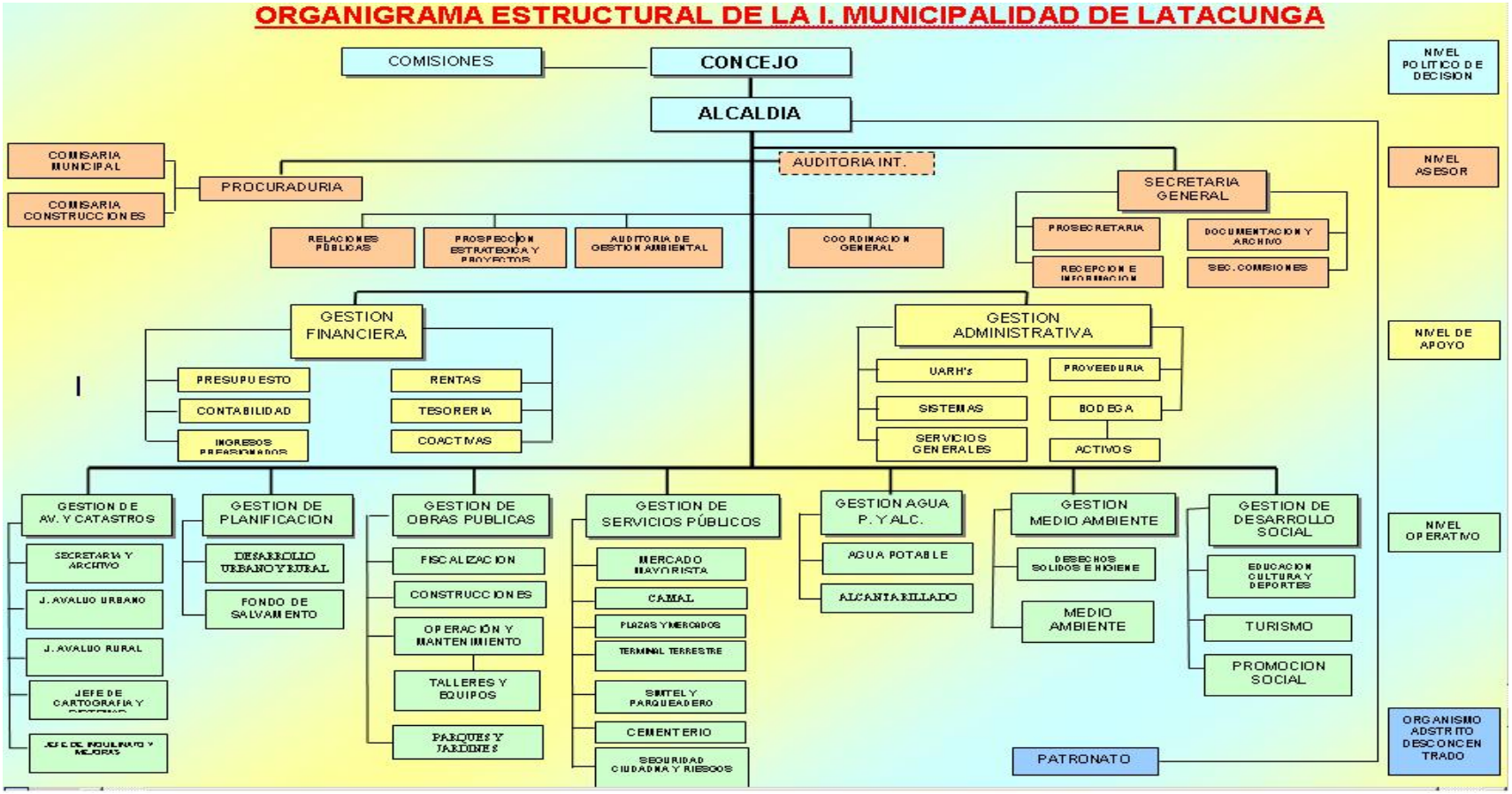
- ✓ Patronato Municipal de Amparo Social[13]

[13] http://www.latacunga.gov.ec

2.1.9. Organigrama Estructural

GRAFICO Nº 2.1: Organigrama Estructural

FUENTE: Grupo Investigador



2.1.10. Análisis FODA

El diagnóstico de la situación actual se realizo con la participación del Administrador del departamento informático y personal que labora en el GMCL.

TABLA Nº 2.1 MATRIZ FODA

FUENTE: Grupo Investigador

FORTALEZAS (+)	OPORTUNIDADES (-)
1. Personal dispuesto a Capacitarse. 2. El GMCL práctica valores 3. Laboratorio de cómputo adecuado 4. Ubicación geográfica de la Institución 5. Infraestructura de la Institución	1. Se dictan seminarios en la Instituciones. 2. Apoyo de las Autoridades 3. Acuerdos con Organismos Institucionales
DEBILIDADES (-)	AMENAZAS (-)
1. Falta de motivación a al personal del GMCL 2. Falta de capacitación especializada en las áreas especificas. 3. Falta de acondicionamiento de laboratorio de cómputo	1. Descuido al personal que labora dentro de la Institución 2. Despreocupación de las Autoridades. 3. Descuido de las Autoridades Institucionales.

2.2. Población y Muestra

En el Gobierno Municipal del Cantón Latacunga no existe una población extensa, razón por la cual no amerita el cálculo respectivo para la muestra.

TABLA Nº 2.2 PERSONAL INVOLUCRADO EN LA INVETIGACIÓN

FUENTE: Grupo Investigador

SUJETOS	**N°**
Administrador del área de redes	3
Departamento de Unidad de Sistemas	2
Jefe de analista de sistemas	3
Técnico de mantenimiento	4
Analista Programador	1
TOTAL	**13**

La investigación del proyecto: **ANALISIS E IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA BASADO EN LA METODOLOGIA ITIL, EN EL PARQUE INFORMÁTICO DEL GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA,** llevó a la necesidad de aplicar los instrumentos de investigación como son las entrevistas y encuestas, realizadas con el fin de recolectar la información necesaria para el desarrollo del proyecto planteado.

En lo referente a la entrevista se tomo como muestra al Administrador del Departamento de Sistemas del Gobierno Municipal del Cantón Latacunga, con el único fin de obtener un conocimiento profundo; de cómo se aplicara la Implementación de un Plan de Contingencia basado en la metodología ITIL, y cómo podrá influir en los procedimientos.

Como también se aplicaron encuestas a los Señores de cada uno de las áreas de trabajo: jefe del área de redes, jefe de Unidad de Sistemas y personal; muestra que involucra a todos los responsables directos de llevar en adelante el manejo y la seguridad de los equipos, señalando los problemas y dando soluciones a los

mismos para que la Implementación del Plan de Contingencia pueda ser desarrollada de una mejor forma.

2.3. Análisis de los resultados de la entrevista realizada al Administrador del Departamento de Sistemas del Gobierno Municipal del Cantón Latacunga.

ENTREVISTA DIRIGIDA AL ADMINISTRADOR DEL DEPARTAMENTO DE SISTEMAS DEL GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA, ING. EDUARDO JARAMILLO.

Para la Entrevista se planteó un objetivo principal como recopilar la información necesaria que permita determinar las necesidades que existe en el área Informática del Gobierno Municipal del Cantón Latacunga, con la implantación de un Plan de Contingencia, basado en la metodología ITIL, el mismo que servirá para recuperar la información de una manera rápida y segura.

El Administrador del departamento de sistemas considera que es importante cooperar con el avance tecnológico y más aún si va en beneficio del Gobierno Municipal del Cantón Latacunga, ya que la Institución es muy importante porque se encarga de impartir sus servicios a la comunidad.

El Administrador afirma que en la actualidad cuentan con recursos técnicos y económicos para el mantenimiento de los equipos; además las personas encargadas deben siempre de cuidar, ya que el beneficio es para ellos, y de esta manera puedan desarrollar las actividades diarias.

De igual manera el Administrador argumenta que, al contar con un manual de Plan de Contingencia en la Institución es importante ya que en el momento de que exista un imprevisto se podrá solucionar al instante, además la información

que maneja la Institución es delicada y confidencial, razón por la cual toda Institución pública o privada deben tener dicho Plan.

Interpretación

Después de haber realizado la entrevista al Administrador del departamento de Sistemas del Gobierno Municipal del Cantón Latacunga, es conveniente algunos aspectos; como grupo investigador consideramos importante desarrollar el proceso de la realización de un Manual de Plan de Contingencia, basado en la metodología ITIL, que beneficiara sin lugar a duda a la Institución.
Los Administradores, están completamente de acuerdo con la implementación de un Plan de Contingencia, dentro de la Institución; porque con este proyecto se podrá solucionar problemas en el momento que exista un imprevisto o siniestro, y de esta manera se podrá solucionar los problemas que se presenten.

2.3.1. Análisis e interpretación de resultados de las encuestas realizadas al personal del Departamento de Sistemas del Gobierno Municipal del Cantón Latacunga.

Anexo N° 1 (Encuestas)

A continuación se muestra los resultados obtenidos luego de la aplicación del instrumento de investigación, como es la encuesta a los señores Administradores del Gobierno Municipal del Cantón Latacunga**,** los mismos que son presentados a través de tablas, para luego hacerlo por medio de gráficas en pastel y finalmente efectuar el análisis e interpretación de los resultado

1: La información por su nivel de importancia que se genera en el Gobierno Municipal del Cantón Latacunga es:

TABLA N° 2.3

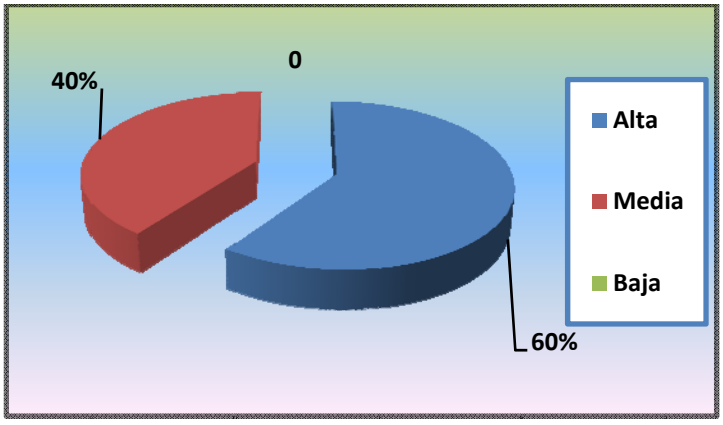
INFORMACIÓN QUE SE GENERA EN EL GMCL.

Opciones	Valor	%
Alta	24	60%
Media	16	40%
Baja	0	0
TOTAL	**40**	**100%**

FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

GRÁFICO N° 2.2

RESULTADO DE LA INFORMACIÓN QUE SE GENERA EN EL GMCL



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS:

Al analizar los datos tabulados se deduce que el 60% es alto y 40% es media, los encuestados creen que la información que se genera en el Gobierno Municipal del Cantón de Latacunga es de vital importancia que la información que se genera dentro de la Institución debe ser de una forma rápida y correcta en el momento de ejecutarse

2: En caso que se dañe su PC la información puede ser recuperada en: Cortó plazo o mediano plazo.

TABLA N°2.4

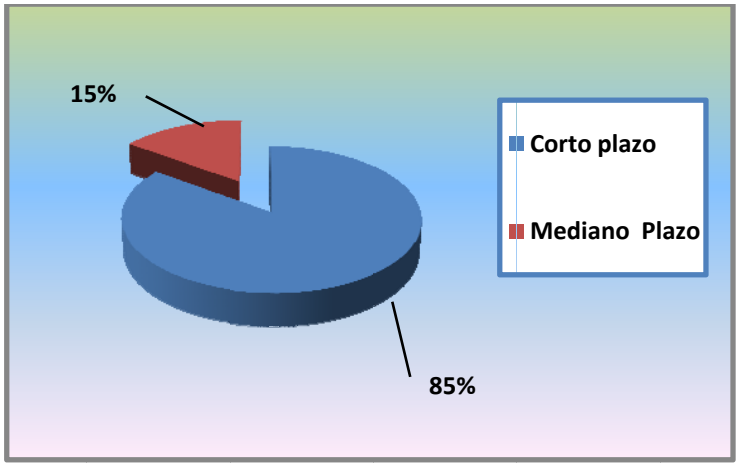
RECUPERACIÓN DE INFORMACIÓN

Opciones	Valor	%
Corto plazo	34	85%
Mediano Plazo	6	15%
TOTAL	**40**	**100%**

FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

GRÁFICO N°2.3

RECUPERACIÓN DE INFORMACIÓN



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Los encuestados al respecto de la recolección de la información indican que un 85% consideran que en caso que se dañen los equipos de computo la información debe ser recuperada a corto plazo , mientras que el 15% manifiesta que se lo realice a mediano plazo, mediante esto no tendrán ningún tipo de inconvenientes.

3: En caso de algún siniestro la información debería ser respaldada

TABLA N° 2.5

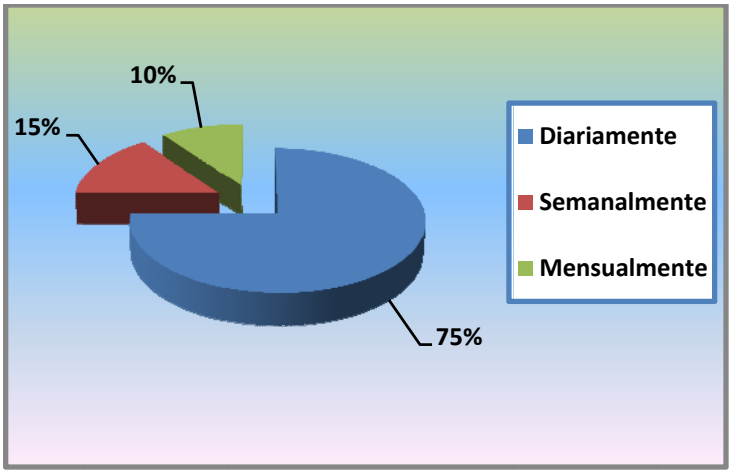
RESPALDO DE INFORMACIÓN

Opción	Valor	%
Diariamente	30	75%
Semanalmente	6	15%
Mensualmente	4	10%
TOTAL	**40**	**100%**

FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

GRÁFICO N° 2.4

RESPALDO DE INFORMACIÓN



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Según los datos recolectados se interpreta que el 75% diariamente, 15% semanalmente y el 10% mensualmente de las personas encuestadas, el 75% nos indican que se debe sacar los respaldos diariamente de cada dependencia para así no tener ninguna clase de inconvenientes y se esta manera se facilite el manejo de la información.

4: El personal informático está capacitado para cubrir daños.

TABLA N° 2.6

PERSONAL CAPACITADO

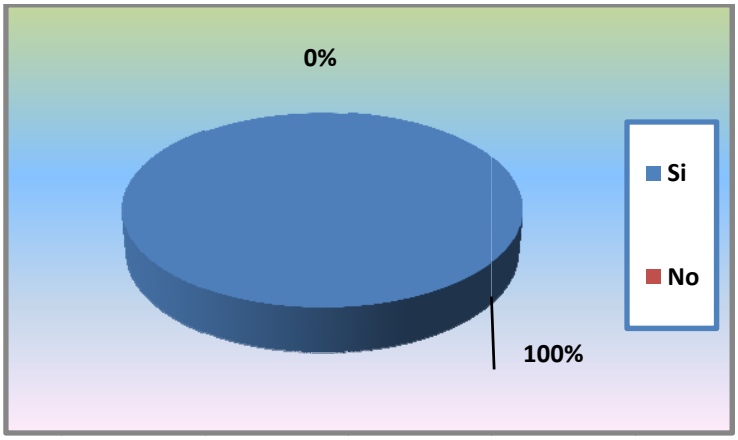
Opciones	Valor	%
Si	40	100%
No	0	0
TOTAL	**40**	**100%**

FUENTE: Encuestados

REALIZADO POR: Grupo Investigador

GRÁFICO N° 2.5

PERSONAL CAPACITADO



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Estos datos permiten conocer que un 100% de los encuestados tienen los conocimientos capacitados para cubrir toda clase de daños que se presenten en cada una de las dependencias, además podemos indicar que el personal se encuentra en condiciones para laborar en dicha entidad.

5: Piensa usted que el manejo de la información que actualmente tiene el Gobierno Municipal del Cantón Latacunga es:

TABLA N° 2.7

MANEJO DE LA INFORMACIÓN DEL GMCL

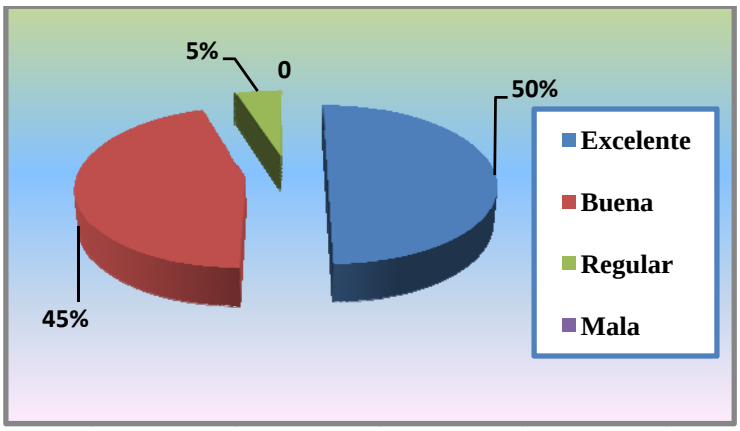
Opción	Valor	%
Excelente	20	50%
Buena	18	45%
Regular	2	5%
Mala	0	0%
TOTAL	**40**	**100%**

FUENTE: Encuestados

REALIZADO POR: Grupo Investigador

GRÁFICO N° 2.6

MANEJO DE LA INFORMACIÓN GMCL



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Con los datos recolectados se conoce que el 50% de los encuestados nos indican que el manejo de la información que actualmente tiene el Gobierno Municipal del Cantón Latacunga es excelente, un 45% buena y un 5% regular, debido a varios factores que ellos nombran como negativos para el ágil manejo de la información.

6: Consideran de que los respaldos se los realicen a nivel departamental.

TABLA N°2.8

MANEJO Y SEGURIDAD DE INFORMACION

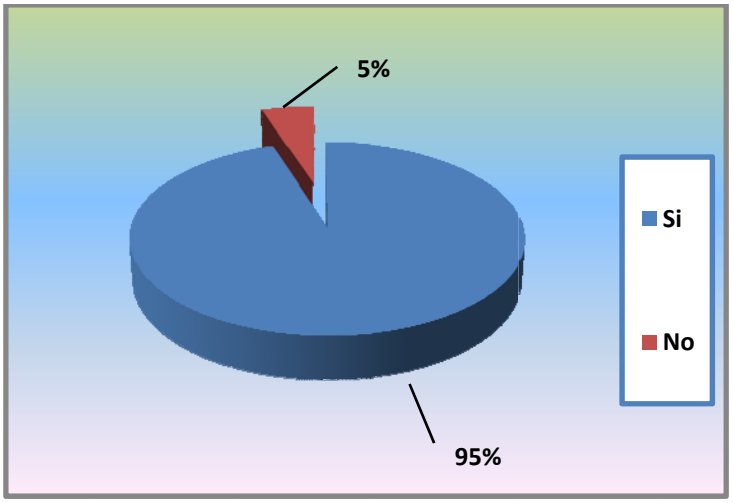
Opciones	Valor	%
Si	38	95%
No	2	5%
TOTAL	**40**	**100%**

FUENTE: Encuestados

REALIZADO POR: Grupo Investigador

GRÁFICO N°2.7

MANEJO Y SEGURIDAD DE INFORMACION



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Estos datos permiten conocer que el 95% de los encuestados consideran que los respaldos se los realicen a nivel de cada dependencia, ya que en el momento que exista algún tipo de inconveniente o pérdida de información entre en funcionamiento los respaldos obtenidos, y de esta manera facilitar la información rápida y efectiva que necesita cada dependencia. El 5% no considera que se saquen respaldos en cada dependencia.

7: Cree usted que es factible utilizar un Plan de Contingencia para obtener mayor seguridad en la recolección de datos.

TABLA N°2.9

PLAN DE CONTINGENCIA

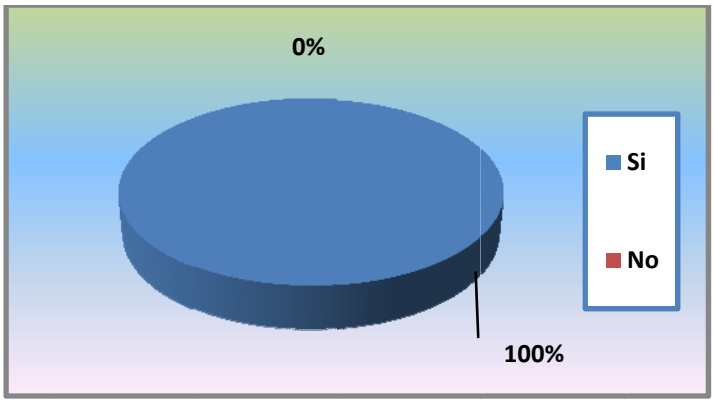
Opción	Valor	%
Si	40	100%
No	0	0%
TOTAL	**40**	**100%**

FUENTE: Encuestados

REALIZADO POR: Grupo Investigador

GRÁFICO N°2.8

PLAN DE CONTINGENCIA



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De acuerdo a los datos obtenidos se conoce que el 100% de los señores encuestados consideran que el Gobierno Municipal del Cantón Latacunga se encuentra en total acuerdo, que realicemos la implantación de un plan de contingencia basada en la metodología ITIL. Por cuanto el plan de contingencia facilitara y permitirá obtener la recuperación de la información de datos, manejo y seguridad.

8: Opina usted que con la implementación de un Plan de Contingencia, Mejorará el control, manejo y recuperación de la información

TABLA N°2.10

RECUPERACIÓN DE LA INFORMACIÓN

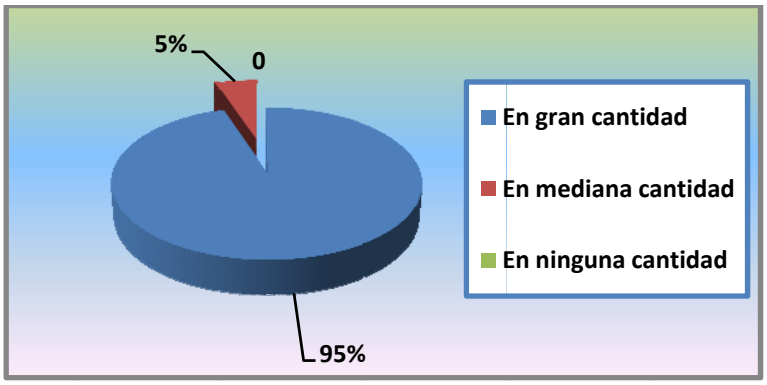
Opción	Valor	%
En gran cantidad	38	95%
En mediana cantidad	2	5%
En ninguna cantidad	0	0%
TOTAL	**40**	**100%**

FUENTE: Encuestados

REALIZADO POR: Grupo Investigador

GRÁFICO N°2.9

RECUPERACIÓN DE LA INFORMACIÓN



FUENTE: Encuestados
REALIZADO POR: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De acuerdo a las encuestas realizadas se logro identificar que el 95% nos da a conocer que con la implantación de un plan de contingencia basada en la metodología ITIL, se mejorará la recuperación y control de la información. Lo cual da la pauta al grupo de investigadores para que se aumente la posibilidad de manejar información hasta llegar a la excelencia.

2.4. Comprobación de la hipótesis

2.4.1. Enunciado

"La implementación de un plan de contingencia basado en la metodología ITIL, podrá mejorar posibles riesgos a los cuales pueden estar expuestos los equipos de procesamiento e información contenida en los diversos medios de almacenamiento".

2.4.2. Comprobación

De acuerdo a las respuestas de la entrevista realizada por el grupo investigador, hacia el Administrador del departamento informático, referente a la automatización de la recolección de campo, podemos concluir que el proyecto propuesto evidentemente cumplirá con las expectativas trazadas por las postulantes, las cuales están basadas en los directivos del Gobierno Municipal del Cantón Latacunga.

2.5. Conclusiones

- ✓ El Gobierno Municipal del Cantón Latacunga debe ir avanzando de acuerdo a los nuevos equipos y por ende la tecnología.

- ✓ Se pudo conocer de qué manera manejan la información dentro de la Institución.

- ✓ Logramos identificar que es necesaria que el Departamento de sistemas del GMCL debe tener un manual de plan de contingencia, ya que este permitirá aplicar en el momento que exista algún contratiempo.

CAPÍTULO III

PROPUESTA

PROPUESTA DE IMPLEMENTACIÓN DE UN MANUAL DE PLAN DE CONTINGENCIA EN EL GOBIERNO MUNICIPAL DEL CANTÒN LATACUNGA PROVINCIA DE COTOPAXI.

3.1. Presentación

En la propuesta se detalla todos los elementos necesarios para comprender los problemas que a diario se presentan, además tomando en cuenta las importantes ventajas y desventajas que en la investigación se han notado, sobre lo que es un Plan de Contingencia, para la investigación, se toma en cuenta como factor principal que brinda en la actualidad la calidad de servicio en el Gobierno Municipal del Cantón Latacunga, a los usuarios, trabajadores en general directivos que forman parte de la Institución, ya que fueron un grupo esencial para obtener una correcta información.

Actualmente la ciencia y la tecnología son muy significativas para los distintos campos de trabajo sobre todo cuando va progresando de una manera muy rápida, tal es el caso del Plan de Contingencia basado en la metodología ITIL, el mismo que hoy en día será utilizado en la dependencia de sistemas del Gobierno Municipal del Cantón Latacunga para brindar las seguridades necesarias que a diario se presenta, es por esta razón que se ha realizado esta investigación amplia sobre cómo recuperar la información.

La metodología ITIL brinda una oportunidad detallada de un número de prácticas importantes, a través de una amplia lista de verificación, tareas, procedimientos y responsabilidades que pueden adaptarse a cualquier organización. En algunos casos hasta se han definido las prácticas como procesos que cubren las actividades más importantes de las organizaciones de servicio. Es una de las oportunidades para trabajar y desarrollar aplicaciones que se cree un software con sus correspondientes aplicaciones y que se pueda usarse dentro de la dependencia de sistemas del Gobierno Municipal del Cantón Latacunga.

Al momento de aplicar la metodología ITIL se obtendrá grandes beneficios, y de esta manera nos permitirá afrontar los principales problemas de las próximas tecnologías, se creara y mantendrá una aplicación de calidad para dicha Institución para cubrir todas las necesidades que se presenten día a día.

3.2. Justificación

En la actualidad la tecnología avanza consecuentemente, esto nos quiere decir que es un estudio frecuente la misma que está desarrollando, además ayudara a tener una recuperación de información mediante la aplicación de la metodología ITIL; también ayudaría al Gobierno Municipal del Cantón Latacunga y a los integrantes de la misma fomentar el desarrollo de la tecnología.

Aplicando la investigación general de los servicios de la metodología ITIL, una de ellas que beneficiaran tanto a los usuarios como a los Administrativos; además por medio de la red desarrollar aplicaciones que vayan acorde con las actividades que realizan dentro de cada dependencia.

Las herramientas que se pueda integrar para el desarrollo de la metodología ITIL permitirán que los usuarios y otros representantes identifiquen las aplicaciones avanzadas, actividades de colaboración y de investigación.

Durante el desarrollo de este tema se tomara en cuenta las siguientes etapas que se detallan a continuación; Análisis de Riesgo, Protección de la instalación, almacenamiento fuera del sitio, estrategia de respaldo de sistema, estrategia de respaldo de redes, toma de decisiones en caso de emergencia, mantenimiento y prueba del plan

Para realizar el avance de la investigación se cuenta con la colaboración del personal Administrativo de la dependencia de sistemas, mediante esto lograremos obtener una información importante para la aplicación de la presente investigación y así poder tener una propuesta clara sobre la integración y la realización de aplicaciones de la metodología ITIL.

Se ha considerado que al aplicar este tema es factible y necesario para la Institución, ya que estamos avanzando continuamente y de esta manera contar con un Plan de Contingencia basado en la metodología ITIL, lo cual les permitirá aplicar en un momento necesario; además les ayudara a tener una recuperación en el momento que exista una pérdida de información.

3.3. Objetivos

3.3.1. Objetivo General

Implementar un Plan de Contingencia basado en la metodología ITIL, que beneficiara al Gobierno Municipal del Cantón Latacunga Provincia de Cotopaxi.

3.3.2. Objetivos Específicos

- ✓ Mejorar los problemas que se presentan dentro del parque informático.
- ✓ Aplicar un manual con la información necesaria en el momento que exista una contingencia.
- ✓ Tratar de minimizar los riesgos dentro de la Institución.

3.4. Enfoque general de lo que contendrá el plan de contingencia.

El plan de contingencia que se aplicara en el Gobierno Municipal del Cantón Latacunga tendrá medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de la Institución. Lo fundamental de este Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos informáticos y la información contenida en los diversos medios de almacenamiento, por lo que se hará una investigación de cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Realizando una investigación general el Plan de Contingencia tiene por objeto establecer las acciones que se deben de ejecutar frente a la ocurrencia de eventos imprevistos que pueden ser de carácter técnico, accidental o humano, con el fin de proteger la vida humana y los recursos tecnológicos. El propósito es reducir el

impacto que pueda provocar un desastre y posteriormente restablecer el nivel de operaciones tecnológicas. Además se establecen controles y políticas que minimizan los riesgos informáticos.

Se puede definir a un plan de contingencias como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad. El plan de contingencia es una herramienta que ayudará a prevenir los procesos críticos de la Institución. El Plan de Contingencias abarcará los siguientes aspectos:

- Plan de Reducción de Riesgos
- Plan de Recuperación de Desastres.
    - Establecimiento del Plan de Acción.
- Actividades durante el Desastre.
    - Plan de Emergencias.
    - Evaluación de Daños.
    - Ejecución de Actividades
    - Evaluación de Resultados.
    - Retroalimentación del Plan de Acción.

3.5. Matriz De Los Riesgos Que Tiene El Gobierno Municipal Del Cantón Latacunga

En la matriz se describen los potenciales riesgos que puede presentar el parque informático del Gobierno Municipal del Cantón Latacunga, cada uno de los riesgos se encuentran ubicados en las etapas indicadas en la matriz, además realizamos un análisis general de lo que contiene cada una de las fases del cuadro que se expone a continuación.

RIESGOS	NIVELES		
INFRAESTRUCTURA	ALTO	MEDIO	BAJO
I1. Caídas de Tención	x		
Humedad		x	
Corto Circuito	x		
Vulnerabilidad de robos	x		
Incendios	x		
Pisos falsos		x	
HARDWARE			
H1. Hardware desactualizado	x		
No cuentan con los accesorios informáticos	x		
No existe un adecuado mantenimiento	x		
Fallas técnicas en los equipos de cómputo	x		
Servicio técnico del servidor	x		
Costos de los suministros		x	
SOFTWARE			
Perdidas de información en la base de datos	X		
Descentralización de aplicaciones	X		
Aplicaciones en diferentes plataformas tecnológicas			X

RIESGOS	**NIVELES**		
Bases de datos sin respaldos automáticos	X		
Licenciamiento insuficiente	X		
REDES			
Cableado estructurado inadecuado	X		
Insuficientes puntos de red	X		
Red eléctrica en mal estado	X		
Red de datos	X		
Administración del internet	X		
Ancho de Banda insuficiente para el personal municipal		X	
Incomunicación entre Municipio y Bodegas	X		
PERSONAL			
Personal capacitado	X		
Capacitación	X		
Asignación no adecuada		x	
No disponen de personal técnico capacitado	X		
Descentralización de funciones		x	
Manejo de áreas criticas	X		

3.6. Enfoque general de la matriz

3.6.1. Infraestructura

La infraestructura con que cuenta el Municipio de Latacunga en la actualidad no se ajusta a lo que debe ser un edificio que pueda contar con instalaciones eléctricas adecuadas, es por eso que con mucha frecuencia se dan caídas severas de voltaje. De igual manera, no existe una adecuada administración de las instalaciones eléctricas, en lo que tiene que ver a la presente investigación es urgente asignar cuando menos un corta pico y con el tiempo asignar un UPS el cual garantizaría el flujo de corriente eléctrica y mantener la integridad de los equipos. El análisis a estos eventos determina que pueden ser evitados y controlados por planes de emergencia, así como la implementación de medidas de prevención y control.

Las operaciones informáticas del Gobierno Municipal del Cantón Latacunga, se detendrían puesto que los equipos de cómputo en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría una dificultad en las operaciones del día.

Las conexiones a tierra que deben tener los servidores no son los adecuados toda vez que por lo antiguo de la edificación del municipio se hacía imposible el enterrar una malla que ayude a precautelar la integridad de la infraestructura tecnológica.

Al tratarse de una entidad pública siempre debe trabajar sus dependencias con las puertas abiertas lo que estaría expuesta siempre a sufrir robos esto hace referencia al factor de riesgo interno de un sujeto o sistema expuesto a una amenaza

correspondiente a su predisposición a ser afectado o de ser susceptible a sufrir una pérdida. La diferencia de la vulnerabilidad de los elementos expuesta ante un evento determina el carácter selectivo de la severidad de las consecuencias de dicho evento sobre los mismos.

Un incendio es una ocurrencia que puede afectar principalmente a la estructuras, los incendios en los edificios pueden empezar con fallos en las instalaciones eléctricas, estructuras especialmente aquellas en las que no se cumplen las normas básicas de seguridad. Todo el personal debe ser capacitado y además conocer muy bien las instrucciones de cualquier extinguidor en caso de llegar a usarlo.

Para evitar este riesgo y otros, se recomienda la instalación de un Sistema de Piso Falso. Este requerimiento se utiliza para los cables del equipo, ya que muchas veces tienen que cruzarse los cables para llegar a las maquinas, así estos pasaran por debajo del piso sin riesgo a que el personal que labora se tropiece con ellos y provoque interrupciones en el funcionamiento de los servidores o pueda llegar a descomponer o afectar algún otro equipo.

3.6.2. Hardware

Es importante que la Institución cuente con las actualizaciones periódicas para el hardware, y dar de baja los equipos una vez que hayan cumplido su vida útil o estos se hayan depreciado ya que esto garantiza el evitar los problemas del Gobierno Municipal del Cantón Latacunga. Además no cuentan con accesorios informáticos básicos que ayuden a resolver los problemas que se presenten en cada dependencia en forma inmediata. Mantener una sobre existencia razonable de máximos y mínimos en los lugares de almacenamiento para mejorar una carencia de suministro.

Es importante que dentro de la Institución exista una protección física de los equipos de cómputo, ya que al no contar con la misma podrían ocurrir problemas; por eso es necesario que solo el personal de la Jefatura de Sistemas tenga acceso, esto con la finalidad de evitar cualquier fallo ocasionado por personal ajeno. Los equipos de cómputo deben tener una clave de acceso y su debida seguridad por contraseña, deberá de ser cambiada periódicamente dicha contraseña. Donde se encuentren los servidores debe existir seguridad.

Las fallas técnicas y humanas han hecho recapacitar a las organizaciones sobre la necesidad de auxiliarse con herramientas que le permitan garantizar una rápida vuelta a la normalidad ante la presencia de cualquier eventualidad, por lo tanto, los mecanismos de seguridad de la información buscan proteger a la información de las diversas amenazas a las que se ve expuesta y supone un importante avance a la hora de superar todas aquellas adversidades que pueden provocar importantes pérdidas de información. A la dependencia de sistemas le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

3.6.3. Software

En la actualidad el Gobierno Municipal del Cantón Latacunga cuenta con una página web la misma que es administrada desde las oficinas de la AME lo que se haría urgente es centralizar el sitio en un servidor de la institución para poder realizar sus diseños y actualizaciones con el propio personal del departamento de sistemas.

Otro de los problemas que cuenta el departamento de sistemas es que las aplicaciones son elaboradas en diferentes plataforma tecnológicas, lenguajes de

programación y bases de datos por lo que la administración se hace mucho más difícil.

Las pérdidas de información de las bases de datos puede proceder de muchas fuentes; tanto de origen humano y problemas laborales, entre otros, como de origen técnico; fallas del hardware, del software, entre otros. Es casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden ser catastróficas para los intereses de cualquier organización.

El personal que labora dentro de la Institución deberá tomar medidas preventivas para proteger la información y de esta manera no ocurre ninguna incidencia que los comprometa. La pérdida de información sin una correcta planificación e implementación de medidas de seguridad, podría requerir de una alta inversión en tiempo e incluso dinero para su recuperación. Dentro de la Institución esto es aún más grave ya que la disponibilidad de la información es fundamental para el correcto desarrollo de sus actividades diarias.

Descentralización de aplicaciones pueden ocasionar graves problemas en la información y programas que se encuentran en el Servidor, o de otras estaciones de trabajo deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado que permita su recuperación, garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible

3.6.4. Redes

Es importante que los cables se encuentren con una protección segura es decir que estén ubicados por canaletas para así no tener ningún problema de cortocircuitos, y mediante esto prevenir daños en los equipos de cómputo. Las fallas del sistema

de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración.

Para que funcionen adecuadamente las computadoras se necesitan de una fuente de alimentación eléctrica, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

La Red de datos es la que permite transmitir información de una computadora a otra. Es por ello, que debe ser de suma importancia el poder detectar las fallas en la red de datos. El objetivo de la Red es de compartir recursos de Hardware y Software.

A poco tiempo se hace urgente que los administradores puedan adquirir un mayor ancho de banda para el servicio de internet y que la pagina web pueda ser mucho más ágil de lo que ahora puede ser.

3.6.5. Personal

Todo el personal que labora dentro del departamento de Jefatura de sistemas deberá estar capacitado para afrontar cualquier caso de problema. Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con todos sus compañeros dentro de cada área. Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso

de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedad.

Las autoridades deberán tomar todas las debidas precauciones para que tomen muy encuentra las necesidades que existe en cada uno de los departamentos, ya que es muy necesario realizar un programa de capacitación para el personal que labora dentro de la Institución, que servirá como guía en el momento que exista algún inconveniente en las diferentes áreas.

La Institución no disponen de personal técnico capacitado para poder desarrollar los problemas que se presenten en dicha área, por ende surge la necesidad de depender de otras Instituciones, ya que facilita el trabajo rápido y seguro a las personas encargadas, además la persona que lo realiza no imparte sus conocimientos al personal de dicha Institución. Sin embargo surgen muchos inconvenientes por falta asignaciones no adecuadas. Los accesos a las áreas de críticas deberán de ser clasificados de acuerdo a las normas que dicte el Gobierno Municipal del Cantón Latacunga y de esta manera evitar el ingreso de personas no autorizadas y por ende llegar a un acuerdo con su comité de seguridad informática.

3.7. Conclusión general de todas las áreas

La investigación está dividida en cinco etapas, la cual realizaremos un análisis en general. En la primera de ellas se realizó un análisis de riesgo efectuado como resultado de las caídas de tención que son los eventos que tienen mayor probabilidad de ocurrencia., los cortos circuitos son fallas estructurales. El análisis a estos eventos determina que pueden ser evitados y controlados mediante la implementación de planes de emergencia, así como la implementación de medidas de prevención y control.

Se define la Seguridad de Datos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con sus colegas dentro de cada área, en lo referente a la utilización del software y elementos de soporte relevantes.

Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres emergencias o períodos de ausencia ya sea por vacaciones o enfermedades. La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

Las redes constan de dos o más computadoras conectadas entre sí y permiten compartir recursos e información. La información por compartir suele consistir en archivos y datos. Los recursos son los dispositivos o las áreas de almacenamiento de datos de una computadora, compartida por otra computadora mediante la red. Una red mucho más compleja conecta todas las computadoras de una empresa o compañía en el mundo. Para compartir impresoras basta con un conmutador, pero si se desea compartir eficientemente archivos y ejecutar aplicaciones de red.

3.8. Plan General De Prevención Para Todas Las Áreas

3.8.1. Soluciones A Los Riesgos Que Se Presentan En La Matriz

INFRAESTRUCTURA.

Caídas de tención

Soluciones:

- ✓ Realizar las instalaciones de una manera adecuada, y de esta manera evitar inconvenientes dentro de la Institución.
- ✓ Instalar corta picos para mayor seguridad en los equipos informáticos y así evitar indecentes en el sistema eléctrico.
- ✓ Realizar censos de carga periódicamente para verificar si la carga instalada se ajusta a la realidad de la instalación.

Humedad

Soluciones:

- ✓ Las maquinas deben estar en un lugar seguro para que no tengan ningún tipo de problema.
- ✓ Asegurar que existan controles adecuados para las condiciones ambientales que reduzcan el riesgo por fallas o mal funcionamiento del equipo.
- ✓ Se debe proveer un lugar especifico donde exista calefacción, ventilación y aire acondicionado, que se dedique en el área de maquinas en forma exclusiva.

Cortocircuito

Soluciones:

- ✓ Las instalaciones eléctricas deben estar bien instaladas para su normal funcionamiento.
- ✓ Los materiales a utilizar en una instalación eléctrica deben ser de buena calidad.
- ✓ Todas las instalaciones deben tener un aislamiento adecuadamente.

Vulnerabilidad a robos de datos

El conocimiento de las señales y los métodos de robo ayudarán a los jefes de área a estar más conscientes de los posibles problemas.

Soluciones:

- ✓ Tener seguridad en la información que se maneja dentro de cada dependencia; es decir en (flash Memory, CD y servidores entre otros).
- ✓ La institución debe contar con guardias de seguridad para el bien de la comunidad.
- ✓ Dar énfasis a las políticas de seguridad de la Empresa.
- ✓ Al entrar y salir de las instalaciones se deberá observar previamente de que no exista ningún individuo sospechoso.

Incendios

Soluciones:

- ✓ Es necesario realizar capacitaciones al personal de cada dependencia en caso de que exista una emergencia el personal pueda hacer uso de los extinguidores**.**

- ✓ En este caso hay que tomar las precauciones necesarias, como la instalación de extinguidores, para que cuando se presente este tipo de

problema se tenga un recurso a la mano y poder controlar de alguna forma este conflicto.

- ✓ Coordinar este tipo de actividades con los señores miembros del Cuerpo de Bomberos para una solución acertada

Pisos falsos

Soluciones.

- ✓ Se requiere implementar arquitecturas flexibles para cableado eléctrico y/o estructurado garantizando una excelente presentación.
- ✓ Se deberían manejar diferentes estructuras, aprovechando los accesorios disponibles.

HARDWARE

Hardware Actualizado

Soluciones:

- ✓ Es necesario realizar las actualizaciones en los equipos, para de esta manera evitar posibles problemas.
- ✓ Deberían contar con equipos de última generación para tener un desarrollo rápido dentro del mismo.

Falta de suministros informáticos

Soluciones:

- ✓ El departamento de sistemas debe contar con los suministros necesarios para que en el momento que exista un desperfecto en el computador sean instalados inmediatamente.

- ✓ Es mejor prevenir posibles daños que después proceder a arreglar los fallos ocasionados por la falta de elementos básicos

No existe un adecuado mantenimiento.

Soluciones:

- ✓ Es necesario primero realizar un cronograma de mantenimiento tanto preventivo como correctivo con la finalidad de dar solución a posibles eventualidades que se pueden presentar.

- ✓ Es necesario realizar mantenimiento preventivo, este se aplica a un ordenador para evitar futuros errores y problemas que se presenten. Por ejemplo la acumulación de polvo en los componentes internos, las partículas de grasa y aceite entre otros.

- ✓ Realizar mantenimiento correctivo, consiste en la reparación de los componentes de la computadora. Por ejemplo una soldadura, el cambio de una tarjeta ya sea de sonido o video entre otros.

- ✓ Debe existir un adecuado mantenimiento y de esta manera evitar que los equipos informáticos sufran cualquier daño.

Fallas técnicas en los equipo de computo

Soluciones.

- ✓ Actualización diaria de antivirus para no tener problemas.
- ✓ Compra de licencias de antivirus corporativo para que de esta manera estén controlados a nivel de servidores y de ahí actualizar a cada computador.
- ✓ Utilizar y manipular de una manera correcta el computador para de esta manera no tener inconvenientes.
- ✓ Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

Servicio técnico de servidor

Soluciones.

- ✓ Es factible que la persona encargada de realizar el servicio técnico de manejo de servidores debe estar capacitado para el desenvolvimiento del mismo.
- ✓ Además deberían contar con un lugar específico para desarrollar el respectivo servicio técnico.

Costos de los suministros.

Soluciones.

- ✓ La institución debería solventar todo lo necesario para el desenvolvimiento del mismo para así no tener problemas en el momento de entregar los suministros que necesiten.
- ✓ Los suministros que se adquirieran deberán ser revisados por las personas encargadas y de esta forma evitar algún desperfecto en el momento de ser utilizado.

SOFTWARE

Perdidas de información en la base de datos

Soluciones:

- ✓ Es importante tener respaldo en un lugar seguro y en diferentes partes, es decir en un servidor secundario de backup, también puede ser en un disco externo.
- ✓ Se debe contar con medidas de seguridad en la información que se maneja diariamente en la institución.

Descentralización de aplicaciones

Soluciones:

- ✓ Es importante sacar respaldos en el Backups que se encuentra fuera de la Institución ubicado en lugar seguro y donde se encuentra protegida toda la información.
- ✓ Deben proteger la información mediante claves de acceso y a través de un plan de respaldo adecuado que permita su recuperación.

Aplicaciones en diferentes plataformas tecnológicas

Soluciones:

- ✓ Generar inmediatamente una migración de plataformas tecnológicas en todas las aplicaciones y cualquier aplicación que aquí se genere venga ya con estas nuevas sugerencias

- ✓ Deben proteger la información mediante claves de acceso y a través de un plan de respaldo adecuado que permita su recuperación.

REDES

Cableado estructurado inadecuado

Soluciones:

- ✓ Se debe plantear tener cableado estructurado CERTIFICADO por la EIA/TIA sea este 568 A o B o si se lo puede manejar seria bueno adquirir el 569 o 570.
- ✓ Cada uno de estos cables deben tener su propia protección y aislantes ya sea con mangueras, tubos Pvc o canaletas dependiendo el caso.
- ✓ Cada equipo de cómputo debe contar con un regulador de corriente para evitar problemas o daños en caso de falla eléctrica

Insuficientes puntos de red

Soluciones:

- ✓ Se debe verificar que los cables estén correctamente conectados.
- ✓ Se debe contar con una adecuada instalación de un sistema de cableado de datos.

Red eléctrica en mal estado.

Soluciones.

- ✓ La red eléctrica debe contar con cableado adecuado y seguro para su normal funcionamiento.
- ✓ Los cables deben estar con su conexión adecuada para que no sufran ningún daño los equipos.

Red de datos

Soluciones.

- ✓ Para que su funcionamiento sea fundamental deberían prevenir fallas en la red y de esta manera no tener contratiempos en el momento que el personal este manipulando el área de redes.

Administración del internet

Soluciones

- ✓ Deberían contar con banda ancha para tener una mejor rapidez en el momento de desarrollar sus actividades.

PERSONAL

Personal no capacitado

Soluciones:

- ✓ Una de las soluciones es capacitar al personal para adecuarlo a la organización, o viceversa, es decir que las empresas se adecuen a lo que el mercado laboral les ofrece.
- ✓ Es importante que el personal sea capacitado periódicamente para el cumplimiento de sus funciones.

Capacitación

Soluciones:

- ✓ Es importante generar cursos de capacitación a nivel de usuarios de computadores en herramientas básicas.
- ✓ Solicitar a las autoridades Municipales que se auspicie la participación del personal de sistemas en eventos, foros, congresos tecnológicos con la finalidad de actualizar sus conocimientos.

Asignación no adecuada

Soluciones:

- ✓ Es necesario que en cada dependencia cuenten con el personal adecuado para realizar cada una de las actividades que se presenten.

- ✓ Deben contar con suficiente personal en cada dependencia para desarrollara cada una de las actividades encomendadas por el jefe de área.

No dispones de personal técnico capacitado

Soluciones:

- ✓ Deben contar con el personal adecuado para que de esta manera no tengan que depender de otras empresas, ya que en el momento que exista un daño

tenga que solicitar el apoyo necesario para solucionar el problema presentado.

- ✓ Cada empresa debe contar con personal altamente calificado, para de esta manera no depender de otras empresas.

Descentralización de funciones

Soluciones:

- ✓ Todo el personal deberá ayudarse mutuamente en el momento de que exista algún contratiempo en cada una de las dependencias.

Manejo de áreas criticas

Soluciones:

- ✓ Mantener como política de la institución todas las áreas identificadas.
- ✓ Las dependencias que no tengan relación directa con personal no autorizada debe estipular estrictamente.
- ✓ El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta el GMCL.
- ✓ En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.

3.9. Políticas de seguridad informática

El respaldo de información es un proceso muy importante que debe de tener cada Empresa este debe de realizarse en sus computadoras, sea un equipo portátil o un equipo de escritorio. El contar con respaldos permite al usuario en algún momento dado recuperar información que haya sido dañada por virus, fallas en el equipo o por accidentes. La pérdida de información provoca daños de fondo como los mencionados a continuación:

- ✓ Fugas de Información

- ✓ Clientes decepcionados
- ✓ Reputación de perdida

La seguridad informática generalmente consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que la información que se considera importante no sea fácil de acceder por cualquier persona que no se encuentre autorizada.

La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física, virus informáticos, fallos de electricidad, caídas de red, hackers y errores humanos.

La seguridad informática tiene como objetivos:

- ✓ Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- ✓ Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- ✓ Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- ✓ Actualizar constantemente las contraseñas de accesos a los sistemas de computo

3.9.1. Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- ✓ Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- ✓ Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- ✓ Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- ✓ Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- ✓ Definición de violaciones y sanciones por no cumplir con las políticas.
- ✓ Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

3.9.2. Algunos parámetros para establecer políticas de seguridad informática

- ✓ Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- ✓ Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- ✓ Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.
- ✓ Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas

3.9.3. Tipos de copias de seguridad informática.

3.9.3.1. Copias de seguridad normal:

Una copia de seguridad normal incluye todos los archivos seleccionados y pone a cada archivo una marca que se indica que se ha hecho una copia de seguridad del mismo.

3.9.3.2. Copia de seguridad diaria:

Una copia de seguridad diaria incluye todos los archivos seleccionaos que se hayan modificado el día en que se realizo la copia diaria.

3.9.3.3. Respaldo Total o Completo

Un respaldo completo es un respaldo donde cada archivo es escrito a la media de respaldo. Si los datos a respaldar nunca cambian, cada respaldo completo creado será una copia de exactamente lo mismo.

3.9.3.4. Copia de seguridad incremental:

Los respaldos incrementales primero revisan para ver si la fecha de modificación de un archivo es más reciente que la fecha de su último respaldo. Si no lo es, significa que el archivo no ha sido modificado desde su último respaldo y por tanto se puede saltar esta vez. Por otro lado, si la fecha de modificación es más reciente, el archivo ha sido modificado y se debería copiar.

3.9.3.5. Copia de seguridad diferencial:

Los respaldos diferenciales son similares a los respaldos incrementales ya que copian archivos que han sido modificados. Los respaldos diferenciales son acumulativos — en otras palabras, con un respaldo diferencial, una vez que un archivo ha sido modificado continuo siendo incluido en todos los respaldos diferenciales subsecuentes (hasta el próximo respaldo completo).

3.9.4. Ventajas de Hacer un Respaldo

- No es necesario ningún dispositivo de almacenamiento para el respaldo
- No es necesario separar o subdividir así como tampoco es necesario ordenarlos de ningún modo.
- Todo el proceso es automático.
- No importa si no está en función el computador, recupera la información de todos modos.

3.9.5. Tiempo disponible para efectuar los respaldos de seguridad

El tiempo disponible para efectuar los respaldos de seguridad es importante, ya que el soporte utilizado, unidad de grabación y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas, y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar accesos o modificaciones sobre los datos objeto de la copia, por esta razón los respaldos se los deberá realizar fuera del horario laboral.

3.10. Metodología para el plan de contingencia

El diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y gastos considerables, sobre todo si se está partiendo de cero. Una solución comprende las siguientes actividades:

1. Debe ser diseñada y elaborada de acuerdo con las necesidades de la empresa.
2. Puede requerir la construcción o adaptación de un sitio para los equipos computacionales.
3. Requerirá del desarrollo y prueba de muchos procedimientos nuevos, y éstos deben ser compatibles con las operaciones existentes. Se hará participar a personal de muchos departamentos diferentes, el cual debe trabajar en conjunto cuando se desarrolle e implemente la solución.

4. Implicará un compromiso entre costo, velocidad de recuperación, medida de la recuperación y alcance de los desastres cubiertos.

A continuación se muestran las principales actividades requeridas para la planificación e implementación de una capacidad de recuperación de desastres.

1. Identificación de riesgos
2. Evaluación de riesgos
3. Asignación de prioridades a las aplicaciones
4. Establecimiento de los requerimientos de recuperación
5. Elaboración de la documentación
6. Verificación e implementación del plan
7. Distribución y mantenimiento del plan

3.11. Identificación de riesgos

La primera fase del plan de contingencia, el análisis de riesgos, nos sitúa en el lugar de un asesor de una compañía de seguros. En esta fase, la preocupación está relacionada con tres simples preguntas: ¿qué está bajo riesgo?, ¿qué puede ir mal? y ¿cuál es la probabilidad de que suceda?

3.11.1. ¿Qué está bajo riesgo?

La primera de estas preguntas, ¿qué está bajo riesgo?, necesita incorporar todos los componentes del sistema susceptibles de ser dañados, dando lugar a la pérdida de conectividad, computadoras o datos. Un diagrama de la arquitectura de todos los componentes del sistema facilitará la realización de un inventario de los elementos que pueden necesitar ser restituidos tras un desastre. No hay que olvidar que también el software necesita ser reemplazado, y que todos los productos software relevante han de ser identificados.

El sistema de aplicación puede no encontrarse preparado para su uso si alguno de sus componentes no está disponible; en tal caso, es aconsejable estar constantemente a la expectativa de los nuevos elementos que pueden haberse

olvidado. Por ejemplo, una aplicación para acceso remoto no funcionaría si los cables no están disponibles para conectar los módem.

Uno de los aspectos menos agradables a tener en cuenta, y que a menudo se pasa por alto, es que las personas esenciales se vean afectadas por el desastre y sea necesario recurrir a otras para realizar sus labores. Al menos, los manuales de las aplicaciones más importantes para la empresa deberían encontrarse disponibles en un sitio externo.

3.11.2. ¿Qué puede ir mal?

Lo más difícil en el plan de contingencia es responder a la pregunta, ¿qué posiblemente pueda ir mal? La respuesta a tal cuestión varía desde lo evidente hasta lo casi increíble. Las clases más obvias de desastres son los desastres naturales que conllevan tormentas de todo tipo o los acontecimientos geológicos como terremotos o volcanes. En cada localidad existe la posibilidad de tener mal tiempo.

Los propios incendios constituyen uno de los peores desastres posibles. El calor, el humo y el agua que rodea a los incendios son tremendamente perjudiciales para los sistemas informáticos. Los dispositivos de almacenamiento se deterioran fácilmente debido a las altas temperaturas y el humo. La eliminación de los residuos tóxicos tras el incendio de una oficina puede llevar meses, incluso años.
Deben considerarse mecanismos alternativos de acceso a la red en el caso de que, por alguna razón, sea imposible acceder al edificio, incluso aunque el edificio puede estar en pie y operacional.
Los errores humanos son una de las causas más probables de la pérdida o deterioro de los datos. Si un error de este tipo provoca la pérdida de un sistema en la red, tiene el mismo efecto que cualquier otro tipo de desastre, y como tal debe ser tratado.

3.11.3. ¿Cuál es la probabilidad de que suceda?

Si se tuviera una cantidad ilimitada de recursos y fuera posible protegerse contra todas las calamidades, esta pregunta carecería de interés. Sin embargo, no se dispone de recursos infinitos; de hecho, los recursos son bastante escasos. Por lo tanto, se deben seleccionar los tipos de desastres contra los que se intentará protegerle.

Responder a la pregunta: ¿cuál es la probabilidad de que suceda? también requiere de ciertas consideraciones presupuestarias. Ello puede ayudar a asumir distintos escenarios de presupuesto para comprender cuáles son los costos de compromiso para diferentes niveles de protección y preparación. Finalmente, se puede estar expuesto a ciertas amenazas cuya protección no está al alcance del presupuesto, pero, al menos, se es consciente de su existencia y, por lo tanto, es posible mejorar el plan en un futuro.

3.12. Evaluación de riesgos

Es el proceso de determinar el costo para la organización de sufrir un desastre que afecte su actividad. En el caso de los sistemas informáticos, la preocupación principal es comprender la cantidad de pérdida financiera que puede provocar la interrupción de los servicios, incluyendo los que se basan en las redes.

Los costos de un desastre pueden clasificarse en las siguientes categorías:

- Costos reales de reemplazar el sistema informático
- Costos por falta de producción.
- Costos por negocio perdido
- Costos de reputación.

El costo real de los equipos y el software es fácil de calcular, y depende de si se dispone de un buen inventario de todos los componentes de la red necesarios.

Los costos de reputación son más difíciles de evaluar y, sin embargo, es conveniente incluirlos en la evaluación. Estos costos se producen cuando los clientes pierden la confianza en la empresa y se llevan su negocio a otro sitio. Los costos de reputación crecen cuando los retardos en el servicio a los clientes son más prolongados o frecuentes.

3.13. Establecimiento de requisitos de recuperación

La clave de esta fase del proceso de elaboración del plan de migración es definir un periodo de tiempo aceptable y viable para lograr que la red esté de nuevo activa. Tal y como se ha planteado en la sección anterior, la preocupación básica debería ser disponer de las aplicaciones más importantes en primer lugar.

Es muy importante concederse una cantidad de tiempo adecuada y no realizar estimaciones poco realistas sobre las propias posibilidades. Es necesario asegurarse de que se dispone de tiempo para recuperar las cintas localizadas en la instalación de almacenamiento exterior y para adquirir los sistemas necesarios.

3.14. Elaboración de la documentación

Crear un documento que mucha gente pueda tener como referencia es quizás lo más difícil del plan de contingencia. No hay que engañarse: implicará un esfuerzo significativo para algunas personas, pero ayudará a aprender cosas sobre el sistema y puede que algún día salve la empresa.

Los recursos necesarios para escribir y mantener un plan de contingencia representan más de lo que puede realizarse en ratos libres y después de horas de oficina. La dirección de la organización debe apoyar la iniciativa para que sea un éxito. Uno de los problemas del plan de contingencia en un entorno de comunicaciones es que la tecnología de redes cambia tan rápidamente que resulta

difícil permanecer al día. Esto incluye nuevos dispositivos, así como nuevos sistemas de aplicación que introducen su propio nivel de complejidad en este campo. Dado el hecho de que la tecnología de red evoluciona tan rápidamente, debería planificarse la actualización del plan de contingencia periódicamente, por ejemplo una vez al año. Aunque la redacción del plan inicial supondrá una gran cantidad de trabajo, una vez que se dispone del plan, las actualizaciones son relativamente fáciles.

3.15. Contenido del plan de contingencia

El plan de contingencia debe intentar definir las cinco áreas siguientes:

1. Listas de notificación, números de teléfono, mapas y direcciones
2. Prioridades, responsabilidades, relaciones y procedimientos
3. Información sobre adquisiciones y compras
4. Diagramas de las instalaciones
5. Sistemas, configuraciones y copias de seguridad en cinta

Hay que cerciorarse de que se sabe a quién notificar en primer lugar cuándo ocurre un desastre. Por ejemplo, si hay un incendio, llamar primero a los bomberos y luego al director general. Pueden existir otras personas o organizaciones identificadas con características o conocimientos especiales que puedan ayudar a minimizar el daño. Si no se dispone de números de teléfono o direcciones actualizados, se puede pasar muy mal contactando con las personas afectadas.

Cuando en primer lugar se comienza a reflexionar sobre cómo responder a un desastre, hay que centrarse en las prioridades establecidas. El tiempo pasa; el trabajo debe empezar por recuperar inmediatamente las aplicaciones de mayor prioridad. Las personas deberían disponer de instrucciones y responsabilidades precisas. Por último, deberían incluirse, de manera detallada, las operaciones y tareas que muestren las labores de instalación y recuperación necesarias, debiendo

ser fáciles de leer y seguir. También habría que incluir aquí los números de teléfono de las organizaciones de asistencia que pudieran requerirse.

Es posible ahorrarse horas o incluso días en el proceso de recuperación si existe la posibilidad de almacenar algunos sistemas de repuesto con la capacidad de gestionar tareas diferentes. Planifíquese instalar una configuración genérica que, como mínimo, permita ejecutar las aplicaciones de mayor prioridad sin problemas.

Hay que asegurarse la disponibilidad de un sistema de copias de seguridad de cinta en funcionamiento. Si es posible, debe mantenerse un sistema de reserva, incluyendo adaptadores, cables y software de unidades de dispositivo, en un sitio alterno.

3.16. Verificación e implementación del plan

Una vez redactado el plan, hay que probarlo. Hay que estar seguro de que el plan va a funcionar. Para ello, se debe ser escéptico sobre el propio trabajo, de manera que pueda uno probarse a sí mismo que funciona. Psicológicamente, esto no es fácil porque con toda probabilidad se ha invertido una gran cantidad de tiempo y energía personal en este proceso, aunque lo mejor sería, si es posible, situarse de manera imparcial ante la confiabilidad del plan. Por consiguiente, han de realizarse las pruebas para encontrar problemas, no para verificar que el plan funciona.

3.17. Comprobación del plan por partes

No se puede tumbar el sistema algún día para ver si se es capaz de recuperarlo. Existen muchas y mejores formas de verificar un plan de contingencia sin causar mayores interrupciones en el trabajo de la organización. Algunas de las cosas en

las que habitualmente no se piensa a la hora de comprobar pueden ahorrar mucho tiempo posteriormente.

Por supuesto, también es necesario verificar los procedimientos que se emplearán para recuperar los datos. Compruébese el software para la realización de las copias de seguridad para confirmar si pueden recuperarse las aplicaciones de mayor prioridad de la manera esperada. Esto debería hacerse en una red aislada para evitar problemas con el servidor de licencias.

Una vez recuperada la información, verifíquese si el usuario puede acceder a ella. Esto requiere de algunas estaciones de trabajo conectadas a la red para simular auténticos usuarios finales con cuentas en los servidos originales. En este punto, puede ser necesario actualizar el plan para incluir información sobre el establecimiento de cuentas de usuario. Compruébese cada una de las operaciones del plan individualmente y examínese entonces si, como resultado, se tiene un sistema de red en funcionamiento. No está de más verificar el plan con otras personas de la organización que se encuentren tan familiarizadas con los productos o procedimientos empleados.

Revísese cada día la parte del plan relacionada con las operaciones de copias de seguridad verificando la finalización correcta de las mismas. Además, supervise esto asegurándose de que algunas personas de la organización saben realizar copias de seguridad adecuadamente, y comprobar su finalización.

3.18. Distribución y mantenimiento del plan

Por último, cuando se disponga de un plan definitivo ya verificado, es necesario distribuirlo a las personas que necesitan tenerlo. Inténtese controlar las versiones

del plan, de manera que no exista confusión con múltiples versiones. Así mismo, es necesario asegurar la disponibilidad de copias extra del plan para su depósito en la instalación exterior a en cualquier otro lugar además del lugar de trabajo.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación. Sin embargo, esto no debería verse como un problema porque probablemente la sección de procedimientos tenga que actualizarse de todas formas debido a otros cambios.

Este proceso llevará tiempo, pero posee algunos valiosos beneficios que se percibirán aunque nunca tengan que utilizarse. El mantenimiento y verificación de un plan de migración ayudará a que se produzca dicha comunicación dentro de la organización.

Conclusiones

- Podemos concluir que la presenta propuesta de contingencia para el GMCL, será de gran ayuda que permitirá minimizar errores e ir incrementando la contingencia para los procesos que normalmente se desarrolla.

- En la propuesta se concluye con soluciones que se presentan a los problemas para proteger al software, hardware, datos y personas.

- Las instalaciones eléctricas del GMCL no son las apropiadas, al tener un centro de datos es necesario que exista una línea a tierra que le permita descargar los altos y bajos e energía.

- No existe manuales de procedimientos, de funciones que permitan resolver los diferentes imprevistos que se presentan diariamente; solo poseen conocimientos adquiridos en la práctica.

- La seguridad de la información abarca la seguridad física y la seguridad lógica. Entendiéndose por seguridad física la protección del hardware y de los soportes de datos, edificios e instalaciones que los albergan.

- Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, entre otros niveles de riesgos .En cambio la seguridad lógica se refiere a la seguridad del uso del software a la protección de los datos, procesos, programas, niveles de acceso de los usuarios a la información.

Recomendaciones

- Se recomienda redistribuir el equipo informático de acuerdo a un estudio de factibilidad de las necesidades de cada una de las dependencias.

- Para evitar la sobrecarga de UPS, es necesario enmarcar en las especificaciones técnicas o instalar un software de monitoreo del UPS.

- Se recomienda establecer programas de capacitación tecnológica para el personal técnico y usuarios internos y externos del GMCL. De idéntica forma planificar cronogramas de actualización tecnológica que permita mantener competitiva a las demás entidades educativas.

- Es importante contar con los permisos y licencias del software que se utiliza en el GMCL. El uso de Software no autorizado o adquirido ilegalmente, se considera como PIRATA y una violación a los derechos de autor por las leyes que rige nuestro país.

- Es importante recordar que el talento humano e uno de los principales recursos que cuentan una entidad, ahí la importancia de motivar, capacitar y darle la oportunidad de que exploten las cualidades competitivas y las ponga al beneficio de la comunidad convirtiéndose en un ente productivo.

- Aprovechar el recurso humano, que al aplicar conocimientos adquiridos durante su vida estudiantil permita generar sistemas de información, fomentando de esta manera la competitividad del GMCL frente a las demás instituciones educativas.

GLOSARIO DE TÉRMINOS BÁSICOS

A

Accesibilidad: Permite asegurar quien puede acceder a la información y cuando

Auditoria Informática: es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Administración: Es un proceso que consiste en las actividades de planeación, organización, dirección y control para alcanzar los objetivos establecidos utilizando para ellos recursos económicos, humanos, materiales y técnicos a través de herramientas y técnicas sistematizadas.

Ambiente: Es el conjunto de todas aquellas entidades, que al determinarse un cambio en sus atributos o relaciones pueden modificar el sistema.

C

Componente físico: Es el que constituye el hardware del sistema informático lo conforman básicamente los ordenadores, periféricos y el sistema de comunicación

Componente lógico: es el que constituye al software del sistema informático y lo conforman básicamente los programas, estructuras de datos y la documentación asociada. El software, como programa, consiste en un código en un lenguaje maquina específico para un procesador individual.

Componente humano: está constituido por todas las personas participantes en todas las fases de la vida de un sistema informático (análisis, implantación). Este componente humano es de suma importancia ya que los sistemas informáticos están desarrollados por humanos y para uso de los humanos.

Computadora.- Es un dispositivo electrónico que permite procesar información y datos con programas diseñados para ello. Actualmente este término no se usa demasiado en el mundo de la informática.

D

Desastre: Se puede considerar como un desastre la interrupción prolongada de los recursos informáticos y de comunicación de una organización o empresa

E

Ejecución: es el proceso mediante el cual una computadora lleva a cabo las instrucciones de un programa informático.

Empresa: Es la institución o agente económico que toma las decisiones sobre la utilización de factores de la producción para obtener los bienes y servicios que se ofrecen en el mercado.

I

Implementación: Formas y métodos para llevar a cabo algo.

ITIL: Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado.

M

Metodología.- Se refiere a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia. Aun cuando el término puede ser aplicado a las artes cuando es necesario efectuar una observación o análisis más riguroso o explicar una forma de interpretar la obra de arte. En resumen son el conjunto de métodos que se rigen en una investigación científica o en una exposición doctrinal.

P

Procedimiento: Puede considerarse como la sucesión cronológica y secuencial de operaciones concatenadas entre sí, que se constituyen una unidad, en función de la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación.

Planificación: es un proceso de toma de decisiones para alcanzar un futuro deseado, teniendo en cuenta la situación actual y los factores internos y externos que pueden influir en el logro de los objetivos.

Protección de datos: Conjunto de técnicas utilizadas para preservar la confidencialidad, la integridad y la disponibilidad de la información.

R

Redes: Conjunto de ordenadores conectadas entre sí ya sea alámbricas o inalámbricamente

Recuperación de información: es el conjunto de tareas mediante las cuales el usuario localiza y accede a los recursos de información que son pertinentes para la resolución del problema planteado. En estas tareas desempeñan un papel

fundamental los lenguajes documentales, las técnicas de resumen, la descripción del objeto documental.

S

Seguridad: La seguridad de las instalaciones, los datos y la información generada es parte de una conversión satisfactoria. La seguridad tiene tres aspectos interrelacionados, física, lógica y de comportamiento. Los tres tienen que trabajar juntos si se pretende que la calidad de la seguridad permanezca alta.

Servidor: Computadora central de un sistema de red que prevee servicios y programas a otras computadoras conectadas.

T

Tecnología: es el conjunto de habilidades que permiten construir objetos y máquinas para adaptar el medio y satisfacer nuestras necesidades.

U

Usuario: Son las personas que acceden a los servicios que presta la empresa.

Bibliografía

Consultadas:

FREEDMAN, A, Diccionario de computación, Edición marzo 1996, Bogotá-Colombia.

HALLSAL, Fred, Comunicación de datos, redes de computadoras, cuarta edición, México, 1988.

JAMES, Senn, Análisis y Diseño de Sistemas de información; México, Ediciones

LOPEZCANO, Jorge, Manual Moderno de Informática; Colombia, Ediciones ZAMORA cuarta Edición 2004.

MCGRAW-HALL segunda Edición 1992.

MARAVEN, Plan de Contingencia; Maracaibo, Ediciones PLAN COLM tercera Edición 1991.

MURRIA**, J,** Aspectos Metodológicos de un Plan de Contingencia; Venezuela, 1991.

PERKINS, Charles, Seguridad de información; Madrid, Ediciones MCGRAW-HALL tercera Edición 2003.

RODRIGUEZ Jorge, Introducción a las Redes de Área Local, McGraw Hill, México, 2000. Pag. 23-28.

RUSSELL, Ackoff, Plan de contingencia, México, 1981.

Virtuales

http://www.monografias.com/trabajos24/plan-contingencia/plan-contingencia.shtml

http://www.ocp.com.ar/plan-de-contingencia.php

http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf

http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml:

http://www.latacunga.gov.ec

http://Monografias.com/analisis-de-sistemas-informaticos.html

http://www.enterate.unam.mx/Articulos/2004/Abril/redes.htm,

http://www.wordreference.com/definicion/implementacion.html

http://www.consultaanteproyecto/sinonimos/plan.htm,
http://www.latacunga.gov.ec
http://ar.groups.yahoo.com/group/foro-itil./html
http://www.vcd.cl/tombrad/pcasval/seguridad.html
http://www.ConsultaAnteproyecto\InformationTechnologyInfrastructure Library - Wikipedia, la enciclopedia libre.htm
http://www.monografias.com/sobre_metodologia
http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
http: // es.wikipedia.org/wiki/Plan de contingencia
http: //www. Plan-es.org/sobre_ Plan
http://www.monografias.com/trabajos18/redes-computadoras/redes-computadores.html.
http://es.wikipedia.org/wifi

PLAN DE CONTINGENCIAS

INTRODUCCIÓN

Este documento tiene por objetivo delinear las actividades principales a cumplirse en la eventualidad que dentro de las instalaciones del GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA, se presentara alguna contingencia, respecto de la red de computación y sus componentes, entre los cuales se pueden encontrar diversos componentes como hardware (equipos) y software (programas), los cuales deben estar funcionando de manera íntegra para asegurar el correcto control de la operación.

Para propósitos de presentación se ha dividido el presente documento en los subsiguientes temas de contingencia:

1. A nivel de los servidores de red
2. A nivel de hardware de red
3. A nivel de software (programas y datos)

Para cada punto a evaluar se describirán posibles escenarios y algunas recomendaciones a seguir. En caso de contingencias el responsable de la ejecución del Plan es el Jefe de Sistemas o Ing. de Soporte en oficinas principales y Coordinador de Sistemas o Auxiliar de Sistemas en las bodegas, patronato. El encargado de realizar las tareas respectivas asegurará la correcta aplicación del Plan y contribuir a la continuidad de la operación sin mayores retrasos.

1.- CONTINGENCIAS A NIVEL DE LOS SERVIDORES

La red computacional de cada oficina está soportada por un servidor de Aplicaciones, Impresión, Archivos y Red montado bajo plataforma Windows 2003 en todo el Municipio. Un resumen de la ficha técnica de cada servidor se encuentra en las oficinas del departamento de sistemas.

Podemos encontrar varios escenarios de contingencias que deberían ser analizados en este documento.

1.1 CONTINGENCIAS EN EL SERVIDOR PRINCIPAL.

Al hablar del servidor principal o central se considera al único equipo servidor que proporciona la aplicaciones que trabajan en los distintos departamentos del municipio es servidor de archivos, de usuarios principalmente, adicionalmente de base de datos, genera respaldos diarios entre otras actividades. En este momento los equipos a los que se hace referencia son los que se encuentran en el departamento de sistemas. Tomando en cuenta esta situación, los posibles casos de contingencia a resolverse, serían los siguientes:

1.1.1 Daño a nivel de la memoria.

En el caso de que alguno de los simms de memoria colocados en el servidor respectivo presente problemas, el servidor enviará un mensaje de error a la consola del servidor y será necesario apagar el servidor y volverlo a reiniciar, retirando uno por uno los simms de memoria, hasta detectar el que haya presentado el problema. Detectado el daño debe retirar ese simms y seguir trabajando aunque con menor rendimiento, hasta que pueda reemplazar lo más pronto posible la memoria dañada. Este proceso de apagar el servidor y detectar

el o los simms con daño, tomaría entre 10 y 20 minutos para nuevamente estar trabajando. Debe considerarse la necesidad de que con los servicios actuales que se requiere en el servidor, la mínima cantidad aconsejable de memoria requerida es de 4 GB de RAM.

1.1.2 Daño a nivel del sistema de almacenamiento.

Al momento los servidores cuentan con discos de 320 Gigabytes.

En Oficinas principales se cuenta con un disco adicional similar que está en espejo para asegurar un cierto nivel de contingencia teniendo un disco idéntico en el caso de daño del disco principal, adicionalmente contamos con un tercer disco encargado de almacenar archivos (Haciendo de disco servidor de archivos), y adicionalmente para almacenar los respaldos en disco de bases de datos y usuarios.

La primera situación, es que sufra un daño a nivel de los sectores del disco, si es imposible continuar trabajando con este disco y se cuenta con un sistema de espejo, se debe seguir el siguiente procedimiento para poner al 2do disco de espejo a trabajar temporalmente mientras se arregla el disco dañado, como se detalla a continuación:

1. Apague el equipo en cuestión.

2. Reemplace el disco duro dañado por otro similar.

3. Reinicie el sistema con el disco de recuperación respectivo. Este disco debe ser formateado en Windows 2003 y debe tener como disco de booteo el disco 2 de espejo.

4. Una vez que se encienda el sistema, se debe romper el espejo anterior y establecerlo nuevamente.

5. Posteriormente reinicie el sistema sin el disco para asegurar que el espejo esta restablecido correctamente.

Si el segundo disco de espejo llegara a tener problemas contamos con respaldos de la configuración del sistema Windows 2003, aparte de los respaldos de la base de datos, correo electrónico y Sistemas, instalar en otro equipo Windows 2003 y recupere estos respaldos hasta tenerlo listo para funcionar en la red.

Es aconsejable un buen mantenimiento del servidor y chequeos constantes con respecto a las alertas que el sistema genera para evitar que el disco colapse. Si el daño del disco no es severo, debe procederse a un formateo de BAJO NIVEL, con el utilitario correspondiente al modelo y tipo de disco, previo a la comprobación de contar con respaldos de la información que este disco contiene.

Debe tenerse en cuenta que si la cantidad de sectores defectuosos es muy alta, el riesgo de volver a tener problemas con esa unidad de almacenamiento, aumenta y en ese caso sería lo correcto, proceder a reemplazarla por otra similar. En cualquiera de las dos situaciones - luego de formatear a bajo nivel o usar una nueva unidad -, debe procederse a reinstalar el software requerido. El tiempo necesario para poder cumplir este proceso de comprobación y reinstalación total del software requerido tomará entre 8 y 12 horas de trabajo, por lo que sí es se presenta en un momento **no crítico**, debería procederse a reinstalar totalmente el software.

La segunda situación es que colapse totalmente la unidad de almacenamiento, sea por un daño interno o por un daño a nivel del controlador de disco, pero en un momento crítico. En ese caso el determinar el tipo de daño puede tomar un tiempo relativamente alto que puede oscilar entre 3 y 6 horas, por lo que en una situación similar, debe usarse otro disco de reserva con los respectivos respaldos para solucionar el problema temporalmente mientras se arregla el disco con daño. En caso de pérdida total de disco contaríamos con un respaldo de un día de retraso.

Continuamente es aconsejable reinstalar las aplicaciones que presentan comportamientos anómalos debido a que el uso de las mismas va deformando naturalmente ciertos programas que a la larga pueden causar inconvenientes. Esto permite corregir algún nivel de corrupción dentro del software de aplicación utilizado, sea por algún proceso que terminó anormalmente, por la presencia de algún virus, mal saneado o por alguna actualización de software necesaria o conveniente.

Además de los problemas mencionados respecto de los discos, puede encontrarse un problema en el controlador de los dispositivos SCSI. En el caso del servidor, tanto el disco, la unidad de Cd y las unidades de cinta, son parte del mismo controlador y si el daño se presenta en éste último, una manera de definir es tratando de acceder a los otros dispositivos (unidades de cinta o CD). Si esto no es posible, seguramente se requerirá apagar el servidor, por lo que al proceder a encenderlo nuevamente, parte del proceso de encendido, es verificar los dispositivos instalados, entre los cuales deben constar, el disco, el CD y las unidades de cinta, caso contrario debe chequearse físicamente, que cada uno de ellos se encuentre perfectamente instalado en el bus correspondiente, tenga su

SCSI ID correspondiente y que sea único, además de su alimentación de corriente.

Si luego de todas estas comprobaciones se determina que hay un problema de mayor cuantía, debe determinarse a la brevedad posible los posibles caminos de solución, entre los cuales debe considerarse cambio de equipo temporalmente, sea uno alquilado de similares características o uno que pueda cubrir el trabajo correspondiente al servidor como un PC del personal de sistemas.

1.1.3 Daño a nivel del procesador central.

Existen distintos escenarios en los cuales el procesador del servidor puede llegar a ser inutilizable como por ejemplo incendio, daños en la fuente de poder por sobre-voltaje, descargas eléctricas o simplemente daños en la tarjeta principal por causas aleatorias.

Las acciones a seguir podrían ser tratar de determinar el alcance de los daños presentados y reemplazar todos los componentes defectuosos, sin embargo esta tarea podría tomar demasiado tiempo para los requerimientos de operación a nivel de oficinas en el Municipio. Aunque este tipo de problema es muy raro que se presente, en el caso de darse debe tratar de determinarse correctamente el tipo de problema que se presenta ya que puede ser confundido con alguna situación parecida, diagnóstico que puede ser determinado por un técnico especialista en el área.

Una forma de determinar el problema de procesador es por medio de la quietud total del servidor y por ende la inoperancia de las estaciones de trabajo y las conexiones de red.

En el caso de presentarse el problema, apagar el servidor lo más pronto posible y reiniciarlo para verificar si el problema persiste, posteriormente si se continúa con el problema contactar con el técnico para determinar su solución.

1.3 SITUACIONES ADICIONALES CON LOS SERVIDORES.

Adicionalmente a lo antes mencionado, en cuanto a procesos de recuperación, deben tenerse en cuentas escenarios como el siguiente:

Si el servidor principal no respondiera por algún daño de hardware pero su disco ha permanecido intacto, puede ser una buena solución, poner este en un equipo

servidor alterno, retirando totalmente los discos (arreglo y disco adicional), que este posee, de tal manera que se tendría un tiempo de recuperación total de entre 30 minutos y 60 minutos. Para ello debe tenerse en cuenta el cambio de conexiones internas y la diferencia de drivers sobre todo de la tarjeta de red para un funcionamiento total de los sistemas.

2.- CONTINGENCIAS A NIVEL DE HARDWARE DE LA RED

Las redes locales del Gobierno Municipal del Cantón Latacunga (LAN), están configuradas bajo el esquema de topología Ethernet, por lo cual en todas y cada una de las máquinas se ha colocado una tarjeta de red Ethernet de 10 y 100MB.

Para formar la red se han instalado SWITCH's Ethernet marca CISCO, 3COM, DLINK y Synoptics, apilados para soportar la cantidad de usuarios. Todo el esquema físico de conexiones entre los SWITCH's y las máquinas se lo hace por medio de un cableado estructurado, que se encuentra debidamente etiquetado y que permite hacer una identificación directa de todos y cada uno de los puntos disponibles para la red.

Dentro de esta estructura pueden presentarse algunas anomalías de diferente gravedad, por ello es necesario determinar adecuadamente el tipo de problema que se presenta y en función de ello proveer la solución adecuada.

2.1 Recuperación de Problemas de RED

La recuperación de estos problemas requiere de cierto tiempo para detectar y aislar el equipo o la causa del error.

Una situación es cuando se detecta dificultad de acceso a la red o simplemente no se puede accesar, lo cual podría indicar un problema en el cableado, entonces se debe revisar si las conexiones están correctamente realizadas con las herramientas

necesarias, como testers de red, ponchadoras, etc. Por otro lado si no es problema de cable se debe verificar la configuración de la tarjeta de red, si no existen conflictos en lo que respecta a IRQs o rangos I/O. Finalmente si todo está correcto debemos revisar la tarjeta actual por si está dañada, para lo cual podemos usar una tarjeta adicional previamente probada.

Adicionalmente a estas pruebas puede procederse a una comprobación física de todos y cada uno de los cables y puntos instalados en la red, para lo cual deben usarse algunos equipos especiales como un comprobador de cables o preferiblemente el llamado LAN Tester, que ayudará a determinar con mayor precisión alguna anomalía física dentro de la estructura de la red. Consecuencia de esto puede requerirse, arreglar algún tramo de cable o ajustar algo dentro de esta infraestructura.

3.- CONTINGENCIAS A NIVEL DE SOFTWARE

Debido a la gran importancia de la información almacenada en los servidores es indispensable tener un muy buen sistema de respaldo, que permita poder disponer de dicha información lo más actualizada posible en el caso de contingencias, y también de fechas o períodos anteriores, en casos de así necesitarlo.

Para manejar las contingencias a este nivel, es necesario indicar que se tiene un proceso diario de respaldo el mismo que en términos generales se define de la siguiente manera:

a) El utilitario usado para efectuar el trabajo de backup es el programa **pkzip, winzip, winrar.**

b) Se dispone de unidades de respaldo tipo cintas de Tape Backup, en las cuales se almacenan los respaldos diarios de la base de datos de los sistemas que

son considerados como críticos, bases de datos de ACCESS, FOX y otras aplicaciones, así como los respaldos semanales de usuarios.

c) También se cuenta con discos duros externos con capacidades de 320 GB para almacenar información de usuarios.

d) Los respaldos se realizan por medio de una utilidad propia del Windows 2003 llamada AT que ejecuta una acción a una determinada hora y fecha por el período que sea necesario.

De esta manera los respaldos de bases de datos se ejecutan todos los días a altas horas de la noche para evitar congestión de la red, estos respaldos se realizan en disco y adicionalmente en las cintas del Tape Backup las cuales son verificadas todos los días a primera hora para verificar la existencia del respaldo.

Por otro lado los respaldos de usuarios se realizan una vez por semana al medio día (hora del almuerzo) para asegurar que estén encendidos los equipos y tener respaldos de todos.

INSTALACIÓN DE UN SERVIDOR SECUNDARIO EN CASO DE CONTINGENCIAS.

Esta posibilidad de uso del servidor secundario para solucionar una contingencia, permite utilizar un equipo adicional en el cuál se instalaría un disco de backup con el sistema operativo y configuración suficientes para continuar con el trabajo, después de bajar la información de los respaldos obtenidos en última instancia, sea de un día anterior o la información del disco del servidor actual.

El utilizar el servidor secundario para seguir operando normalmente puede hacerse efectivo mediante dos situaciones bien definidas:

1) Que el servidor principal sufra un desperfecto que no dañe los discos duros y por ende la información allí contenida.

2) Que el desperfecto en el servidor principal implique el no poder accesar o utilizar los discos duros existentes y por ende NO se pueda acceder a la información contenido en los mismos.

Detalle de estas situaciones:

1) Cuando el daño sufrido por el servidor principal NO AFECTA sus discos duros y por ende la información allí contenida, debe hacerse lo siguiente:

1.1 Retire los discos duros del servidor dañado etiquetándolos adecuadamente.

1.2 En el servidor secundario, debe ubicarse físicamente en las bahías disponibles.

1.3 Al colocarlos en el bus SCSI, deben ponerse las identificaciones (ID Numbers), de cada componente de manera que no hayan duplicidades y además respondan a la secuencia de identificación que esta tecnología exige.

1.4 Si la configuración es correcta, el equipo debe inicializar sin ningún problema, reconociendo el disco últimamente instalado.

1.5 Al levantar el servidor debe tenerse en cuenta la tarjeta de red que actualmente se tiene instalada, por lo que se puede considerar dos acciones a realizar:

a) Poner la tarjeta del servidor dañado en el servidor secundario, siempre y cuando esta se encuentre funcionando bien, y pueda ser instalada correctamente en el nuevo equipo; de esta manera no haría falta cambiar la configuración del sistema operativo y los drivers de la misma para poder levantar estos servicios.

b) Utilizar la tarjeta de red ya existente en el servidor secundario, con lo que al levantar el sistema operativo, debe cargarse el driver correspondiente a dicha tarjeta.

1.6 Si esta configuración es adecuada, esta máquina pasará a ser el servidor principal y no se requerirá ningún cambio adicional en las aplicaciones. Es necesario que se tenga en cuenta que todos los discos y configuraciones existentes en el servidor secundario, antes del cambio, NO ESTARAN DISPONIBLES.

2) Cuando el desperfecto en el servidor principal implica el no poder accesar o utilizar los disco duros existentes y por ende NO se pueda acceder a la información contenido en los mismos, puede utilizarse otro mecanismo implementado previamente y que consiste en:

2.1 Activar una copia calendarizada y planificada de la información que se actualiza constantemente en el servidor principal, almacenada en un disco de reserva.

2.2 El uso de este mecanismo implica tener presente lo siguiente:

a) Habilitar un equipo que soporte el disco a ser usado.

b) Revisar la configuración actual, hacer los cambios necesarios como actualización de usuarios de red, impresoras de red, cuentas de mail, entre otros.

4.- CONTINGENCIAS A NIVEL DE COMUNICACIONES

Las comunicaciones son de vital importancia para nuestra organización. Aunque el sistema es muy simple debemos tener una idea de la forma como se maneja este sistema, especialmente en momentos de problemas que pueden detener la transmisión de datos.

El sistema consiste básicamente en la agrupación de un módem, una línea telefónica y un programa de transmisión de datos. Las comunicaciones son utilizadas para transmitir datos diariamente desde el internet con las paginas estatales.

4.1 Problemas con la línea telefónica

Podríamos detectar este problema haciendo una prueba al conectar directamente en la línea afectada un teléfono normal y verificando que la línea este funcionando. Si no funciona la solución es buscar otra línea de backup para lograr la comunicación.

Si no se cuenta con una línea de backup y determinando la urgencia de la transmisión de los datos, debería pensarse en la posibilidad de hacerlo por un medio semejante.

4.2 Problemas con el módem

En el caso de tener problemas con el módem lo ideal es buscar otro módem para lograr la comunicación y en el caso de persistir con el daño comunicar a los técnicos proveedores de los servicios de internet, para la suplantación del equipo que presente los daños.

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA

PROCEDIMIENTOS PARA UN PLAN DE CONTINGENCIAS

NOMBRE : PLAN DE CONTINGENCIAS	
FECHA INICIO: Julio 21 de 2010	**FECHA ACTUALIZACION**:Julio 21 de 2010
CODIGO :	**ELABORADO POR** : Sistemas

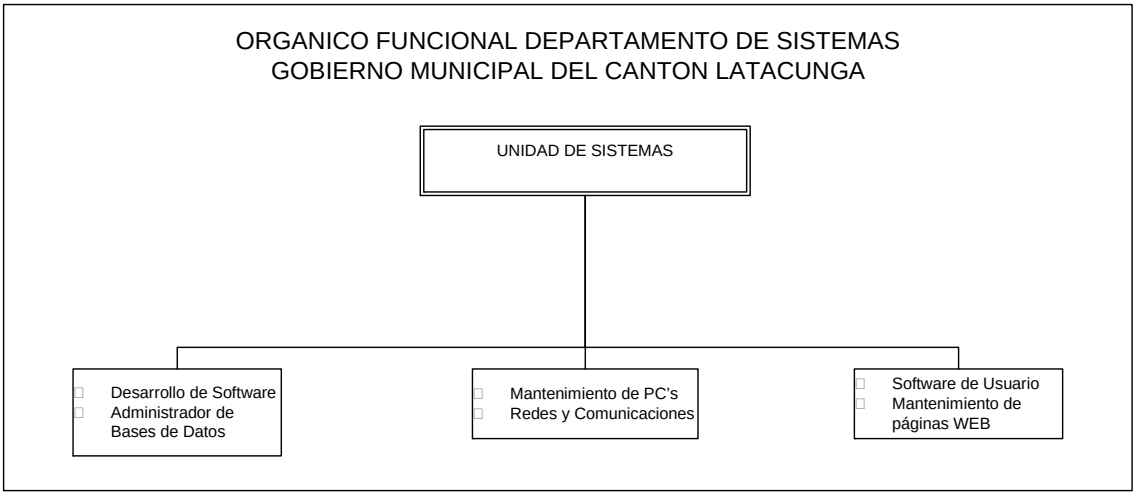
REVISADO POR	**APROBADO POR**
JEFE DE SISTEMAS	**JEFE ADMINISTRATIVO**

Objetivo general

El objetivo de este Plan es encontrar todas las debilidades del Área de Sistemas en esta Institución para poder elaborar un plan que permita prevenir y solucionar problemas futuros del área es cuestión.

Descripción del Área de Informática

El Departamento de Sistemas del Municipio de Latacunga en la actualidad cuenta con las siguientes aéreas para brindar soporte y desarrollo de nuevas aplicaciones que la Institución trabaja.



OFICINAS ADMINISTRATIVAS

1. Dar soporte a los usuarios de la Red en todo el Municipio.
2. Diseño y elaboración de aplicaciones.
3. Investigación de nuevas tecnologías relacionadas a su área de responsabilidad dentro del departamento.
4. Adquisiciones de equipos y demás implementos informáticos.
5. Administrar los respaldos de la información de los usuarios de la red.
6. Realizar transmisiones y centralización de la información de los centros de distribución.
7. Proveer de mecanismos de seguridad de software y datos para cada usuario de la red.

PERSONAL DE SISTEMAS QUE SON SOPORTE EN OTROS DEPARTAMENTOS

1. Dar soporte a los usuarios de la red local y si requieren consultar a personal de sistemas para ayuda o asesoramiento.

2. Identificar necesidades de los usuarios locales para ser transmitidas a personal del departamento de sistemas.

3. En el caso de requerir mantenimiento deben contactarse con la empresa asignada para esta tarea previa autorización de Jefatura de sistemas o persona responsable del área de soporte.

4. No pueden dar solución a problemas de mediana magnitud sin previa consulta a oficinas del departamento de sistemas, solamente a soluciones locales simples.

INTRODUCCIÓN

El presente Plan pretende dar una guía a los administradores de la red o usuarios autorizados para poder resolver un problema informático cuando este ocurriere.

IDENTIFICACIÓN DE RIESGOS

Existen varias circunstancias que en la red del Municipio pudiesen darse problemas y se va a realizar el estudio detalladamente.

OFICINAS ADMINISTRATIVAS

Riesgos

1. Daño físico de equipos (Computadores, impresoras, hubs,switch, modems, etc)
2. Desconfiguraciones a nivel de software de equipos.
3. Problemas con los sistemas.
4. Pérdida de información o datos en algún equipo.
5. Problemas con el internet.
6. Falta de seguridad que presenta el sistema contable- financiero en el manejo de la información.
7. No poder enviar la información por medio magnético.
8. No poder enviar la información por medio de líneas telefónicas, o medios de comunicaciones.
9. Robos o Incendios.
10. Falta de fluido eléctrico

Problemas

1. Retraso en las actividades normales por el daño de equipos, impresoras, módems, etc.
2. Retraso en las actividades normales por desconfiguración de equipos varios.
3. No poder facturar y generar reportes relacionados.
4. Repetir todo el trabajo que implique recuperar la información desde el último respaldo.
5. No poder contar con e-mails o archivos enviados mediante internet.
6. No poder sacar balances con respecto a meses pasados o consolidados que reflejen la verdadera situación del municipio. Contar con información incompleta en el sistema versus documentos físicos previamente impresos.
7. No poder consolidar la información a tiempo en las oficinas.
8. Pérdida de equipos e información.
9. Posible desconfiguración de equipos y no poder laborar normalmente.

Recuperación

La solución de los problemas que afecten al sistema de oficinas administrativas debe ser dada por el Jefe de Sistemas o el Ingeniero de hardware o aplicaciones.

1. **Para solucionar el problema de daño de equipos el responsable de los otros departamentos deberá coordinar con el Jefe de Sistemas o Ing. de Soporte y realizar las siguientes tareas:**
   - Intentar determinar el real problema del equipo.
   - Verificar el/los números de serie de los equipos.

- Revisar los datos de la persona y empresa donde fue adquirido el/los equipos.
- Chequear si está dentro de la garantía.
- Sea cual sea el caso si no se puede solucionar inmediatamente se debe llamar a la empresa que vendió el equipo y pedir una solución, o a la empresa contratada de mantenimiento si existiera para que trámite la solución.
- Si se requiere enviar el equipo a mantenimiento, se debe sacar un respaldo de los datos en él contenidos, colocarlos una copia en un equipo temporal y la otra en un dispositivo de respaldo, generar un documento de salida del equipo para mantenimiento y enviar el equipo para su arreglo con la firma de recepción de la empresa de soporte.
- Si el equipo cuenta con garantía solicitar a la empresa otro similar en calidad de préstamo.

2. **En el caso de desconfiguración de equipos, el encargado de la solución debe realizar el siguiente proceso:**

- Conocer específicamente el problema que tiene el equipo, ¿Qué no funciona?
- Tratar de resolverlo volviendo a configurarlo.
- Si no puede solucionarlo llamar al Ingeniero de Soporte del municipio y en última instancia a la empresa que realiza el mantenimiento de equipos y buscar una solución.

3. **Si se diera el caso de tener una pérdida de información de cualquier equipo, lo que el encargado de sistemas debe hacer es :**

- Determinar qué equipo sufrió la pérdida, y si se puede recuperar en el mismo equipo por medio de una restauración de la papelera de reciclaje, usando el comando undelete o algún utilitario para el caso, como Norton Disk Doctor.
- Si fuese el servidor el del problema, solicitar a los usuarios salgan del sistema para evitar posibles problemas y pérdida de información en otros equipos.
- Averiguar cuál es el último respaldo de la información y determinar el tiempo de pérdida aproximado.
- Revisar los respaldos que deben existir ya sea en el disco del servidor en el directorio **usuarios** destinado para este propósito, o en el medio de respaldo que debe tener guardado el área de sistemas.
- Determinar la cantidad de información perdida, y la fecha desde cuando se perdió.
- Recuperar la información borrada, mediante la digitación en base a los documentos físicos.

4. Si hubiese problemas con Internet.

- Consultar con el Ingeniero de Soporte su posible solución.
- Si no se puede solucionar llamar al proveedor de internet y comunicar el problema para su solución.

5. Robos o incendios.

- En el caso de sufrir el robo de un equipo de la empresa se debería diferencia entre un equipo que almacena información y uno de solamente soporte a usuario. Si se trata de un equipo de soporte a usuarios como impresoras, mouse, teclado, modems, ups, reguladores,

etc. Los cuales no implican almacenamiento de datos el procedimiento a seguir es :

- La persona responsable el equipo debe emitir un informe que indique la situación en que se extravió el equipo ya sea por robo o pérdida.
- Segundo se debe verificar por parte del administrador de los activos de computación si el equipo está bajo garantía.
- Si está bajo garantía se debe emitir un informe a la empresa de seguros indicando las características del equipo perdido y la situación en la que se extravió.
- Determinar la urgencia de reemplazar dicho equipo, y dependiendo de eso adquirir otro mientras el seguro responde por el extraviado.
- Si se trata de un equipo nuevo, ingresarlo al inventario y anotar las novedades con respecto al perdido.

- Si fuera el caso de tener un equipo similar a un PC, servidor, discos duros, etc el procedimiento a seguir es:
    - La persona responsable el equipo debe emitir un informe que indique la situación en que se extravió el equipo ya sea por robo o pérdida.
    - Segundo se debe verificar por parte del administrador de los activos de computación si el equipo está bajo garantía.
    - Si está bajo garantía se debe emitir un informe a la empresa de seguros indicando las características del equipo perdido y la situación en la que se extravió.
    - Determinar la urgencia de reemplazar dicho equipo, y dependiendo de eso adquirir otro mientras el seguro responde por el extraviado.

- Revisar los respaldos de información para determinar cual es el último respaldo que puede ser recuperado en el equipo provisional o nuevo adquirido.
- Restaurar el respaldo en el nuevo equipo y verificar que contenga toda la información requerida.
- Si se trata de un equipo nuevo, ingresarlo al inventario y anotar las novedades con respecto al perdido.

- Si se tratase de un incendio o alguna causa de fuerza mayor que destruye los equipos especialmente que contienen datos tendríamos el siguiente procedimiento a seguir:
    - La persona responsable del inventario de equipos de computación debe emitir un informe que indique la situación en que se dañaron o destruyeron los equipos ya sea por incendio, derrumbes, inundaciones, terremotos, deslaves, etc.
    - Segundo se debe verificar por parte del administrador de los activos de computación si los equipos están bajo garantía.
    - Si están bajo garantía se debe emitir un informe a la empresa de seguros indicando las características de los equipos perdidos y la situación en la que se destruyeron.
    - Determinar que equipos requieren ser recuperados inmediatamente, si no son todos.
    - Una vez que se cuente con los nuevos equipos, se debe restaurar el último respaldo de la información que dicho o dichos equipos hubieren tenido.
    - Si se trata de equipos nuevos, ingresarlos al inventario y anotar las novedades con respecto a los destruidos.

6. Falta de fluido eléctrico.

- El fluido eléctrico normal puede ser un problema el momento de suspenderse especialmente si se trata de un área crítica, como contabilidad, financiero, agua potable, catastro. En la red del municipio existen varios equipos que cuentan con UPS de aproximadamente 10 a 15 minutos de duración, con lo cual se puede solucionar temporalmente el problema de energía eléctrica. Existen casos en los que dichos UPS soportan mientras los generadores del municipio reactivan el fluido eléctrico, o el fluido de la empresa eléctrica se reactive, pero si el fluido no ha regresado en máximo 10 minutos, deben ser apagados los equipos normalmente y posteriormente apagar el UPS para evitar una descarga total de la energía almacenada.

Comité de Apoyo

En caso de problemas extremos que requieran de un mayor nivel de aprobación de toma de decisiones solamente para oficinas de sistemas, se requiere de la decisión y supervisión del Jefe Administrativo o directamente del Señor Alcalde.

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA

PROCEDIMIENTOS

NOMBRE : SOLUCIÓN A PROBLEMAS TÉCNICOS

FECHA INICIO: Julio 21 de 2010 **FECHA ACTUALIZACIÓN**: Julio 21 de 2010

CÓDIGO : TEC001 **ELABORADO POR** : Sistemas

REVISADO POR	APROBADO POR
JEFE DE SISTEMAS	**JEFE ADMINISTRATIVO**

OBJETIVO

Conocer la manera de solucionar los problemas que afecten a equipos de computación y/o programas existentes en el Municipio de Latacunga.

POLITICAS

1. No tomar las decisiones localmente, consultar con Sistemas para decidir la solución.

PROCEDIMIENTO GENERAL

1. El momento de darse algún problema de hardware, debe generarse un documento (memo – Problema técnico) en el cuál se detalle el equipo afectado con la respectiva clasificación (Servidor, Computador, Impresora, switch, UPS, etc), por otro lado la persona asignada, el o los respectivos números de serie, el motivo aparente de la falla y el estado actual, las fallas que tiene.

2. Este documento debe ser enviado a oficinas principales al Jefe de Sistemas para su evaluación y comunicado verbalmente para agilitar el trámite de arreglo.

3. Una vez que Sistemas se ha enterado del desperfecto, se determina la solución sea arreglo por parte de Sistemas, envío al distribuidor más cercano o en el último de los casos reclamo de garantías al proveedor de los equipos.

PROCEDIMIENTO DE ENVIÓ DE EQUIPO A SERVICIO TÉCNICO

1. Si se trata de un equipo que contenga información como computadores, asegurarse de contar con un respaldo final actualizado de la información ya sea en otro computador o cintas de respaldo, para poder grabar esta información en otro equipo mientras se soluciona el desperfecto.

2. Posteriormente colocar toda la información en un equipo provisional asignado para suplantar temporalmente al dañado.

3. Antes de entregar el equipo a la empresa, si es posible borrar la información o retener el disco duro evitando que información de la empresa vaya a parar a manos de extraños.

4. Si se requiere enviar el equipo a la empresa de Servicio autorizado, previa identificación del personal de dicha empresa, generar una nota de entrega numerada y debidamente documentada que confirme la salida del equipo con datos como :

- Oficina que reporta el problema.
- Fecha y lugar de la entrega del equipo
- Persona que entrega el equipo por parte del Municipio
- Persona y empresa que recepta el equipo para darle servicio técnico.
- Tipo de equipo (Computador, impresora, cinta de respaldo, regulador, UPS, etc.)
- Marca del equipo.
- Serie/s del o los equipos enviados.
- Problema exacto del equipo, confirmado por el técnico de la empresa externa.

5. Entregar el equipo previa firma del técnico responsable.

6. Archivar la nota de entrega y enviar una copia al Jefe de Sistemas con copia al señor jefe administrativo.

7. Dependiendo de la decisión tomada en Sistemas en coordinación con el señor Jefe Administrativo, si es el caso colocar un equipo proporcionado en calidad de préstamo por el departamento de sistemas del municipio que pueda solucionar el problema.

PROCEDIMIENTO DE REEMPLAZO TEMPORAL DE EQUIPO CON DESPERFECTO

En el caso de tener un equipo que ha sido enviado a Servicio técnico, debe ser reemplazarlo de la de siguiente forma:

IMPRESORAS

- Comunicar a Sistemas el posible cambio.
- Si se cuenta con un equipo temporal asignado por la compañía de servicio técnico, colocarlo en reemplazo del equipo original.
- Si no se cuenta con un reemplazo de la empresa de servicio técnico colocar temporalmente o imprimir temporalmente en una impresora de similares características.

COMPUTADORES

- Comunicar a Sistemas el posible cambio.
- Si se cuenta con un computador temporal asignado por la compañía de servicio técnico, colocarlo en reemplazo del equipo original, previa instalación de los programas necesarios y copia de los respaldos en dicho equipo para continuar con el trabajo normalmente.
- Si no se cuenta con un respaldo externo, asignar un equipo de similares características cuyo trabajo no sea de mucha importancia, si es que el reemplazo se hace urgente.

OTROS EQUIPOS

- El departamento de Sistemas del municipio asignará la solución más acertada al problema.

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA

DEPARTAMENTO DE SISTEMAS

PROCEDIMIENTO DE SOLUCIÓN DE PROBLEMAS DE SOFTWARE

En el caso de tener problemas a nivel de software, primero consultar con Sistemas Oficinas Principales, para buscar la solución. En el caso de contar con los paquetes originales de instalación de una aplicación con problemas, se puede optar por sacar respaldos de la información necesaria, desinstalar el software y reinstalarlo con las debidas seguridades.

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA
PROCEDIMIENTOS

NOMBRE: SOLICITUD DE PRÉSTAMO DE RECURSOS INFORMÁTICOS	
FECHA INICIO: Julio 21 de 2010	**FECHA ACTUALIZACIÓN**: Julio 21 de 2010
CÓDIGO : PRE001	**ELABORADO POR** : Sistemas

REVISADO POR	APROBADO POR
JEFE DE SISTEMAS	**JEFE ADMINISTRATIVO**

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA

DEPARTAMENTO DE SISTEMAS

OBJETIVO

Conocer cuál es el procedimiento para solicitar el préstamo de un determinado recurso informático (Equipos, Infocus, Documentación, Software, etc), cuyo uso debería ser por motivos de trabajo.

POLITICAS

1. En este procedimiento se conocerá a PERSONA AUTORIZADA como Jefe de Sistemas, o en su ausencia Ingeniero de Soporte o Ingeniero de Desarrollo.
2. La PERSONA AUTORIZADA es el único que puede autorizar el préstamo de recursos informáticos y/o cambio de lugar de dichos recursos en la misma oficina o hacia otras oficinas.
3. Los equipos encontrados en las diferentes oficinas del Gobierno Municipal del Cantón Latacunga se encuentran bajo la responsabilidad del Coordinador de Sistemas local, lo cual no implica que esta persona está autorizada a entregarlos en calidad de préstamo temporal a ninguna persona sin previa autorización.

PROCEDIMIENTO GENERAL

1. En el caso de ser requerido un recurso en calidad de préstamo, la persona interesada debe solicitarlo a la PERSONA AUTORIZADA en Oficinas del Departamento, y a los Coordinadores de Sistemas en las respectivas oficinas del municipio, previa autorización de la PERSONA A CARGO.
2. El momento de requerir el recurso, el responsable debe llenar una Planilla de Préstamos donde constan datos divididos en Información de Préstamo. Estos datos van de acuerdo a la Planilla anexa.

3. El equipo debe ser entregado en la fecha y hora señalada debido a que puede ser requerido por otra persona.
4. El momento de recibir un recurso informático debe ser revisado íntegramente y anotar en novedades la situación actual del equipo para controlar el estado en que se lo recibe.

GOBIERNO MUNICIPAL DEL CANTÓN LATACUNGA **PROCEDIMIENTOS**

NOMBRE : RESPALDOS DE LA INFORMACIÓN	
FECHA INICIO: Julio 21 de 2010	**FECHA ACTUALIZACIÓN**: Julio 21 de 2010
CÓDIGO : PRE001	**ELABORADO POR**: Sistemas

REVISADO POR	APROBADO POR
JEFE DE SISTEMAS	**JEFE ADMINISTRATIVO**

1. DESCRIPCIÓN

1.1. OBJETIVO

El siguiente documento define las políticas y procedimiento a seguir en cuanto a respaldos de información en Oficinas y departamento de sistemas del Municipio de Latacunga. De esta manera el personal de sistemas contará con un documento formal que le especifique cómo y cuándo generar dichos respaldos.

1.2. POLITICAS

1. El listado de toda la información a ser respaldada consta en el cuadro "Información a Respaldar" y las aplicaciones en "Programas a respaldar".
2. Se deben generar los respaldos de acuerdo al horario establecido en la tabla de "Horario de Respaldos" y "Fecha de Respaldos", sin excepciones, ni retrasos, pues van a ser supervisados por Oficinas centrales continuamente.
3. Los respaldos serán realizados por la persona responsable, o por quien esta designe como se ve en el cuadro "Responsables de los respaldos".
4. Las copias de los respaldos deben ser enviadas a oficinas centrales donde se almacenará una copia de toda la información de las oficinas como Avalúos, Comisaria, Planificación y catastro excepto información de usuarios.

5. Los respaldos deberán ser programados para ser realizados en horarios de poca congestión, como es la hora del almuerzo o al final de la jornada diaria. Para el caso de respaldos de información crítica como es cierres de mes del departamento financiero, contabilidad y donde se requiera de manejo de dineros, se debe coordinar primeramente con el responsable del manejo de dicha aplicación para asegurar respaldar a la fecha exacta de cierre.
6. Los directorios o archivos deben respaldarse por medio de un empaquetador como **pkzip.exe, winzip.exe, winrar.exe.** Para el caso del servidor Linux se debe ejecutar el comando **TAR** y luego el comando **GZIP.**
   - El comando para empaquetar en ambiente Windows es :

     Pkzip NombreAplicaciónDiaMesAño.zip Directorios/Archivos a empaquetar

   - El comando para empaquetar en ambiente Unix es :

     Tar -cvf NombreAplicaciónDiaMesAño.tar
     Dir/Arch. a empaquetar

     Gzip NombreAplicaciónDiaMesAño.tar

7. La información debe ser respaldada de acuerdo a la tabla de "Medios de almacenamiento".
   - El formato de los archivos a respaldar debe ser :

     Nombre**A**plicación**D**ia**M**es**A**ño.zip (Windows)

     Nombre**A**plicación**D**ia**M**es**A**ño.tar.zip (Linux)

8. Las cintas a ser usadas para el respaldo pueden ser reutilizadas siempre y cuando se mantenga la cantidad de cintas apropiada para los respaldos establecidos de acuerdo a la tabla "Medios de almacenamiento".
9. Para el caso de los distintos departamentos del municipio habrá una persona que se encargue de Coordinar las actividades de Sistemas y estos deben enviar una copia de sus respaldos a las oficinas centrales asegurando de esta manera contar con una medida de contingencia en el caso de daño o pérdida de los respaldos locales.

1.3. PROCEDIMIENTO

Existen dos tipos de respaldos que pueden ser elaborados, Uno es el tipo de respaldo que continuamente se mantiene en disco y solamente al final del mes o en la fecha planificada se copia a discos de respaldo que para el efecto es un Disco Externo o alguna unidad de almacenamiento USB. El segundo es un respaldo que se genera en disco duro y cinta, diariamente, debido a la importancia de la información involucrada.

1. Asegurarse de contar con los programas batch que generan los respaldos cuyos nombres deberían ser :
    - Para respaldos de financiero: finan.bat
    - Para respaldos de catastro : catastro.bat
    - Para respaldos de agua potable : agua.bat
    - Para respaldos de comisaria : comisa.bat
    - Para respaldos de el almacenamiento general : mensual.bat
2. Asegurarse de tener correctamente programada la ejecución automática de estos programas mediante los comandos AT para Linux y Windows, tomando en cuenta la ejecución de los archivos de acuerdo a las tablas “Información a respaldar y Horario de Respaldos de Información”.
3. Cuando se trate de respaldos de aplicaciones que no se encuentran en los servidores, así como archivos de usuarios, se debe tener cuidado de encender previamente los equipos requeridos.
4. De acuerdo al tipo de información a respaldar, los respaldos se realizarán simultáneamente en un espacio reservado del servidor y adicionalmente en cintas de respaldo, para otros casos los respaldos solamente permanecerán temporalmente en el servidor.
5. Una vez realizados los respaldos se debe guardar las cintas en un lugar seguro y su copia para el caso de los distintos departamentos, debe ser enviada a oficinas centrales al Ingeniero de Soporte para su almacenamiento y control.
6. Mensualmente se va a realizar una correcta revisión de los respaldos generados por cada oficina.
7. En forma general la manera de generar respaldos es :
    - App. de Bases de datos : Diario al servidor y a cinta

- Usuarios: mensual, al cierre de mes al servidor y si se puede a cinta también.

GOBIERNO MUNICIPAL DEL CANTON LATACUNGA **PROCEDIMIENTOS**

NOMBRE	: RESPALDOS DE LA INFORMACIÓN		
FECHA INICIO: Julio 21 de 2010		**FECHA ACTUALIZACIÓN**: Julio 21 de 2010	
CÓDIGO	: PRE001	**ELABORADO POR**	: Sistemas

REVISADO POR	APROBADO POR
JEFE DE SISTEMAS	**JEFE ADMINISTRATIVO**

2. DESCRIPCIÓN

Define la manera cómo se deben administrar las claves de usuarios en los sistemas que trabajan en el Gobierno Municipal del Cantón Latacunga, Windows 2003 (Clave de Red), Correo Electrónico en general.

2.1. OBJETIVO

Este proceso pretende optimizar la seguridad del acceso a la información de cada usuario y de la institución.

2.2. PROCEDIMIENTO

CLAVES DE SISTEMAS

1. La administración de claves de todos los usuarios de los sistemas del municipio será realizada en el Departamento de Sistemas por el jefe del departamento o la persona que éste delegue o considere que es la persona más adecuada, siendo en la mayoría de casos en el Ingeniero de soporte.

2. El Administrador de los Sistemas que trabajan en el Municipio se deberá cambiar su clave de usuario una vez al mes.
3. Las claves de usuarios deben ser cambiadas cada 6 meses por lo menos.
4. Debe tenerse en cuenta que nunca deben eliminarse las claves de los Sistemas, para deshabilitar el acceso solamente se debe poner N en todas las opciones de los sistemas.

   NOTA: Las claves de usuarios de los sistemas no pueden ser cambiadas en una forma más continua debido a que ellas mantienen el histórico de las transacciones realizadas por los usuarios.

CLAVES DE RED

1. La administración de claves de todos los usuarios de la Red (Windows 2003) será realizada en los servidores centrales por el encargado de las redes y los servidores cuando el jefe del departamento lo autorice, si la administración se lo hace fuera de la institución el jefe deberá disponer a la persona que realice este trabajo.
2. Todas las claves de Red de usuarios deben ser cambiadas una vez al mes, lo cual debe estar configurado en Windows 2003 para la solicitud de cambio de password automática.

CLAVES DE CORREO ELECTRÓNICO

1. La administración de claves de correo electrónico de todos los usuarios será realizada en la institución por el Ingeniero de Soporte.
2. Todas las claves de correo electrónico de los usuarios deben ser cambiadas una vez al mes por el mismo usuario, este proceso debe ser realizado por cada usuario para lo cual deben ser instruidos sobre la manera de cambiar dichas claves.

CLAVES DE OTRAS APLICACIONES

1. El proceso de cambio de claves debe ser realizado por el departamento de sistemas en coordinación con los usuarios, por lo menos una vez al mes.