CAPITULO II

INTRODUCCION AL PLAN DE CONTINGENCIA

2.1. Conceptos básicos de Plan de Contingencia

Hoy en día tanto las personas como las organizaciones son muy dependientes de las computadoras, las redes que manejan nuestras actividades diarias y la disponibilidad de los sistemas informáticos, ya que sin estos recursos para las empresas sería difícil laborar. Todas las empresas deberían estar preparadas ante un desastre, es decir a la interrupción prolongada de los servicios informáticos, hay que tener en cuenta que si un desastre llegase a suceder, se podrían tener pérdidas tanto materiales como de información de clientes, empleados, proveedores y productos, dependiendo de la actividad a la que se dedique una determinada organización.

2.1.1 Plan de Contingencia

Es el proceso de determinar qué hacer si una catástrofe sucede en una empresa. La Institución debe estar lista a la reanudación de las actividades ante una calamidad, misma que podría ser una de las situaciones más difíciles con las que una organización deba enfrentarse. Luego de un desastre, existe la posibilidad de que las edificaciones queden totalmente destruidas, o que no se disponga de ninguno de los recursos, es posible que no se pueda contar con todo el personal, es por esto que tanto la Ilustre Municipalidad como el personal que labora en la Institución deben estar preparados para salir de dicho problema, por mas pequeño que este sea.

Un plan de contingencia esta sujeta a tres tipos de acciones que se mencionan a continuación:[4]

- **Prevención**

Es un conjunto de acciones que se deben realizar para prevenir cualquier contingencia que afecte la continuidad operativa de la Institución, tanto de forma

[4] Bradanovic "Contingencia" 2007
http://www.bradanovic.cl/pcasual/seguridad2.html

parcial o total. Hay que ser siempre precavidos por que esto puede reducir el impacto y ayudar a su pronta recuperación.

- **Detección**

Para la detección de un desastre se deben examinar todos los daños tanto naturales como eventuales que todavía no están considerados, tales como cortes de energía, robos, entre otros, para que a futuro se pueda prevenirlos y llegar a una pronta solución en el caso de que llegasen a suceder.

- **Recuperación**

Se considera el mantenimiento de los recursos afectados por un desastre que posee la Institución ya sea física o lógica.

2.1.2. Estadísticas Recientes

Entre los desastres que ocurren con más regularidad en los países de Latinoamérica son los siguientes:[5]

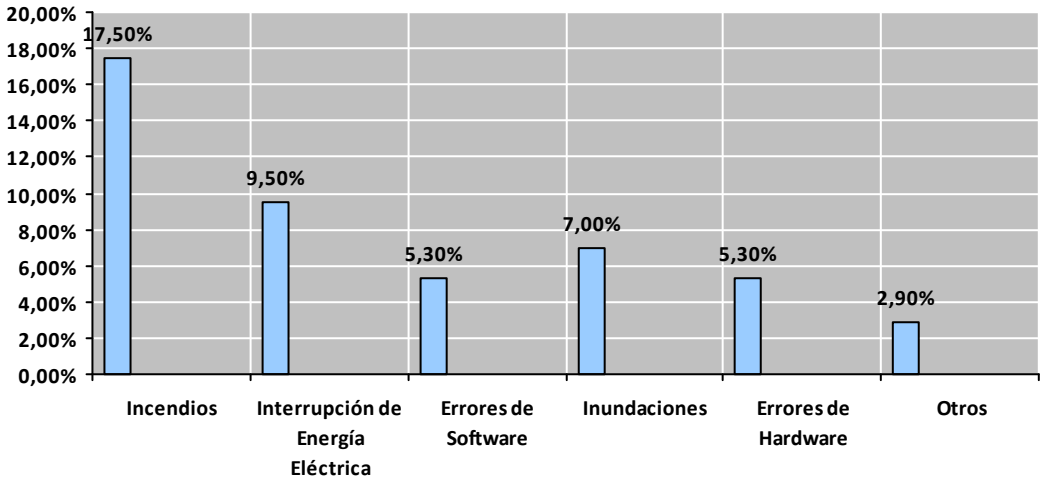

Diagrama 3: Principales Causas de Desastres en las Empresas

De acuerdo a la ubicación y la estructura del edificio que dispone La Ilustre Municipalidad de Paute, los valores estadísticos mencionados en el diagrama Nº 1

[5]Monografías "Plan de Contingencia" 2007-12-15
www.monografias.com/trabajos11/plconting/plconting.shtml

pueden ser tomados en cuenta, debido a que la probabilidad de sufrir dichos desastres es importante, excepto la inundación cuyo riesgo es bajo. (Ver análisis de riesgos Capítulo I).

2.1.3. Metodología para elaborar un Plan De Contingencia Informático

El diseño e implementación de un plan de contingencia informático para la recuperación de desastres implica esfuerzos y gastos considerables.

Una solución comprende las siguientes actividades:

- Debe ser diseñada y elaborada de acuerdo con las necesidades de la Institución.
- Se deberá analizar cada uno de los riesgos, de acuerdo a su probabilidad de ocurrencia.
- El personal de diferentes departamentos debe trabajar en equipo cuando se desarrolle y aplique la solución.
- Implicará un compromiso entre costo, velocidad de recuperación, medida de la recuperación y alcance de los desastres.

2.2. Reconocimiento de la Institución para la elaboración del Plan de Contingencia

Teniendo en cuenta que La Ilustre Municipalidad de Paute, no cuenta con un plan de contingencia vigente, se procedió al análisis de los riesgos encontrados en el capitulo I, para la elaboración de un plan de contingencia que ayude a la recuperación inmediata frente a cualquier tipo de desastre.

2.2.1. Evaluación de Riesgos

Es un proceso mediante el cual se obtiene la información necesaria, para que la organización esté en condiciones de tomar decisiones apropiadas sobre la oportunidad de adoptar acciones preventivas y en tal caso, sobre el tipo de acciones que deben adoptarse, es decir es un proceso dirigido a estimar la magnitud de

aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que La Institución esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas.[6]

2.2.2. Amenazas

Es un es un factor externo del riesgo, teniendo en cuenta la posibilidad de que ocurra un fenómeno o un evento desfavorable, que podría generar daño en las personas o su entorno, y que puede manifestarse en un momento y un lugar específico con una magnitud determinada.[7]

2.2.3. Ataques Internos

La Institución se encuentra sujeta a varios ataques ya sean estos internos o externos, afectando de esta manera tanto la integridad de los datos como el desempeño de la misma.

Algunos ataques internos que suelen suceder con mayor frecuencia en la Municipalidad son los siguientes:

- **Suplantación de IP**

La suplantación de IP se produce cuando se cambia la dirección de origen de un paquete IP para ocultar la identidad del remitente. La función de enrutamiento de Internet sólo utiliza la dirección de destino para enviar un paquete por su camino e ignora la dirección de origen. Por lo tanto, un intruso puede enviar un paquete destructivo al sistema y disfrazar su origen para que no se sepa de dónde procede.

- **Reconocimiento de redes**

El reconocimiento de redes consiste en explorar las redes para descubrir las direcciones IP válidas, los nombres del sistema de nombres de dominio (DNS) y los puertos IP antes de iniciar un ataque.

[6] Wikipedia "Evaluación de Riesgos" 1997-01
http://www.segulab.com/evaluacion_riesgos.htm
[7] Gobierno de Buenos Aires "Amenaza" 2008-02-09
http://www.buenosaires.gov.ar/areas/seguridad_justicia/emergencias/glosario.php

El reconocimiento de redes no es dañino, el descubrimiento de las direcciones que se utilizan puede ayudar a que alguien pueda iniciar un ataque.

- **Modificación/Alteración de Información**

La modificación de la información es un ataque interno al que se expone La Institución a diario, puede darse el caso de empleados que de forma accidental o involuntaria alteren la información.

- **Acceso a información restringida**

El acceso a la información restringida, es un riesgo interno al que se expone la Municipalidad por no administrar un solo sistema de información, cualquier empleado puede ingresar y provocar una duplicidad de los datos.

Existen también ataques externos que pueden llegar a afectar a La Institución, siendo estos originados con frecuencia desde Internet, los mismos que son emitidos como virus, o programas de Trojan o troyanos, aunque en estos casos el invasor primero realiza un reconocimiento de los servicios, sistemas, y redes accesibles; la protección contra ataques externos incluye el uso de cortafuegos, la red que supervisa los dispositivos, la distribución de servicios a través de redes múltiples, y el establecimiento de las restricciones de la anchura de banda por protocolo y servicio.

Para protegerse contra estos ataques externos, se debe habilitar los servidores del Domain Name, servidores del Web y servidores del correo en sistemas separados y restringir el acceso a la red a través de un firewall. Es también beneficioso deshabilitar los servicios innecesarios para que el atacante no pueda tener acceso a ningún sistema.

2.3. Plan de Contingencia para La Ilustre Municipalidad de Paute

De acuerdo a las debilidades y análisis de riesgos realizados en el Capitulo I, se procede a la elaboración de este plan de contingencia, de tal manera que recopile los procedimientos tomados en circunstancias de crisis tales como:

- Incendio
- Corto Circuito o sobrecarga
- Ataques Internos
- Robo
- Filtraciones de Agua
- Errores de Hardware
- Virus Informáticos

A continuación presentamos una lista de responsables de cada departamento, con el fin de que cuando se ponga en marcha el plan contingencia, se pueda contar con el apoyo directo de cada uno de ellos, logrando de esta manera un mejor desempeño del personal en el desarrollo de la contingencia en el caso de que un desastre llegase a suceder.

Nombre de Departamento	**Responsable**
Recaudaciones	Ing. Silvia Carnica
Agua Potable	Ing. Diego Vásquez
Planificación	Arq. Danny Jiménez
Difusión y Cultura	Lic. Patricio Ramía
Jefatura de Avalúos y Catastros	Arq. Mª Esther Chacón
Comisaría Municipal	Dr. Omar Flores
Sistemas	Ing. Alejandro Chuquiralao

Tabla 8: Responsables de cada departamento en
La Ilustre Municipalidad de Paute

2.3.1. Incendio

Para que la Ilustre Municipalidad de Paute este prevenida ante un incendio debe cumplir con los siguientes requerimientos:

Precauciones

- Tener equipos de emergencia como extinguidores, mangueras contra incendios, reservorios de agua, en los siguientes departamentos:

    - Recaudaciones
    - Agua Potable
    - Jefatura de Avalúos y Catastros
    - Financiero
    - Alcaldía
    - Y en la entrada principal.

- Realizar simulacros de incendio con los empleados, para que estos estén prevenidos en caso de que suceda dicha emergencia.
- El edificio debe tener dos salidas alternas, que servirán para evacuar de emergencia al personal.
- La Municipalidad debe tener un sistema de monitoreo contra incendios, el mismo que brinda la señal de alerta al cuerpo de bomberos más cercano.
- Se debe tener los equipos informáticos del Municipio, asegurados de tal manera que dicha empresa cubra los equipos afectados.
- Para evitar el ingreso del fuego al cuarto de servidores, las paredes del mismo deben ser cubiertas con pintura retardante contra incendios.

Que hacer si ocurre un Incendio:

- La operadora de la Ilustre Municipalidad alertará al cuerpo de bomberos de la situación.
- El personal que conforma el cuerpo de bomberos tratará de salvaguardar la integridad tanto del personal que labora en la Ilustre Municipalidad como a la Institución físicamente

- Si es posible, el responsable de cada departamento matará las sesiones iniciadas de los usuarios que hayan estado utilizando el sistema en ese momento y apagará los servidores.
- Los empleados designados con anterioridad para la utilización de extinguidores pondrán en marcha su responsabilidad en ese momento.

Que hacer luego de haber ocurrido un Incendio:

- La persona encargada de sistemas realizará un análisis de los daños ocasionados en los equipos de computación y solicitará al cuerpo de bomberos un informe del estado de las instalaciones.
- Los responsables de cada departamento realizarán una auditoría de las pérdidas físicas y lógicas, fijándose siempre si es que existe la posibilidad de rescatar parte de los materiales o la totalidad de la información.
- El ingeniero responsable de sistemas para volver a instalar los equipos nuevamente ya sean estos propiedad de la Municipalidad o nuevos, se debe asegurar que la infraestructura sea segura y esté en buenas condiciones.

En cuanto al respaldo y recuperación de la información de La Ilustre Municipalidad, el personal asignado realizará lo siguiente:

- La persona responsable de sistemas, debe almacenar la información en un lugar diferente que no sea el edificio, el Ingeniero deberá almacenar la información en dispositivos extraíbles como cintas, Dvd, Cd, y guardarlos en una caja de seguridad de un banco si el caso lo amerita.
- Se debe tener una inmediata respuesta de restauración, para que la Municipalidad siga funcionando sin problemas, dichos respaldos deberán estar a cargo del responsable de sistemas.
- El responsable de sistemas debe restaurar la base de datos, junto con la información recuperada y debe notificar a los diferentes empleados que pueden volver a utilizar cada uno de los sistemas.
- Los responsables de cada departamento analizarán cómo se originó y las causas del accidente, para actualizar las políticas de seguridad y los controles.

2.3.2. Corto Circuito o Sobrecarga de Energía.

Tomando en cuenta que las instalaciones eléctricas de La Ilustre Municipalidad no cuentan con los estándares establecidos, es decir; La Institución carece de una conexión a tierra, los equipos se conectan directamente al tomacorriente sin antes una conexión a un regulador de voltaje, existen demasiados empalmes en los cables y al mismo tiempo estos se encuentran totalmente sueltos y dispersos por cada uno de los departamentos.

Por todo esto la ocurrencia de dicho desastre es muy probable, y se mencionará a continuación algunas precauciones que se debe tener en cuenta.

Precauciones

- El responsable de sistemas mantendrá la documentación necesaria de todo el cableado de red y eléctrico de La Municipalidad.
- Todos los equipos informáticos que se encuentren en cada uno de los departamentos y los servidores ubicados en el cuarto de telecomunicaciones, deben estar conectados a UPS para evitar que se apaguen por causa de un corte de energía eléctrica.
- La institución verificará el correcto funcionamiento y estado de cada uno de los puntos eléctricos y su conexión a tierra.
- Para evitar que se detengan las actividades cuando haya pérdidas de energía eléctrica en la Municipalidad, la institución poseerá una planta generadora de energía propia.

Que hacer si ocurre el Corto Circuito o Corte del Suministro de Energía

- El Ingeniero encargado de sistemas deberá informar de dicha anomalía a un técnico para que corrija el problema y así poder tomar las medidas correctivas, para evitar que vuelva a ocurrir.
- Verificar que el fallo no provoque daños a los equipos informáticos, revisar las tarjetas de red, las fuentes de poder, etc.

En el caso de ser internas:

- El Técnico realizará el cambio y/o reparación de las instalaciones afectadas y verificará cada uno de los puntos eléctricos y sus conexiones.

En el caso de ser externas:

- El encargado de mantenimiento será la persona autorizada, de encender inmediatamente el generador de energía que La Ilustre Municipalidad posee.
- El responsable de sistemas deberá comprobar el correcto funcionamiento de los servidores, de los computadores de cada departamento y de la conexión de la red.

2.3.3. Ataques internos en La Ilustre Municipalidad de Paute

La Institución dispone de información muy importante, es por esto que se trata de protegerla de ciertos usuarios de la red interna, como empleados y clientes. El responsable de sistemas debe estar al tanto de los tipos de ataques internos para que pueda contrarrestarlos.

- **Suplantación de IP**

En algunos departamentos de La Municipalidad existen puntos de red inutilizables, el Ingeniero de sistemas tiene que deshabilitar dichos puntos o en otro caso mantener desconectados del switch, para que cualquier persona mal intencionada o los propios empleados no puedan acceder a la red. Esta infiltración puede ser también realizada mediante internet pero como la Municipalidad no posee una buena conectividad, es poco probable que dicha suplantación se dé.

- **Reconocimiento de redes**

El ingeniero de sistemas debe conocer que un reconocimiento de datos se puede dar mediante los siguientes servicios:

- Protocolo simple de transferencia de correo (SMTP).
- Protocolo de control de transmisión (TCP).
- Protocolo de transferencia de hipertexto (HTTP).
- Salida de red (NetBIOS).

Por lo tanto, se debe desactivar dichos servicios teniendo en cuenta que la desactivación de los mismos podría restringir la capacidad de diagnóstico de la red.

- El responsable de sistemas deberá poseer un diseño de la red tanto físico como lógico, las direcciones IP de cada uno de los equipos informáticos y los que lo utilizan.
- El responsable de sistemas realizará monitoreos constantes en busca de conexiones mal intencionadas.

Que hacer si ocurren Ataques Internos

El responsable del departamento de sistemas realizará cada 8 días una auditoría con el fin de encontrar posibles ataques internos, siguiendo el siguiente procedimiento:

- Analizar los archivos log
- Bloquear el equipo en donde se ha realizado una transacción no autorizada.
- Bloquear la cuenta del usuario utilizada en el ataque.
- El ingeniero responsable verificará nuevamente cada uno de los puntos de red.
- Realizar un informe de los eventos sucedidos, de los correctivos y las acciones realizadas y lograr un seguimiento de estos incidentes para observar su evolución y determinar de manera más fácil si vuelve a ocurrir.
- Si hubiere el caso de que vuelva a ocurrir dicha acción, el responsable de sistemas podrá determinar con exactitud quien es el responsable o el causante y tomar las medidas pertinentes al caso, tales como informar al Departamento de Jefatura de personal y ellos previo análisis notificarán a las autoridades competentes de ser necesario.

2.3.4. Robo

Para prevenir robos de equipos informáticos y de Información en La Municipalidades es necesario que:

- El personal que tenga acceso a determinados lugares debe tener su respectiva identificación.
- El lugar físico donde se encuentra resguardada la información debe ser un lugar aislado del edificio propio y seguro.
- Se debe mantener toda la información, especialmente la sensible, en servidores centralizados y no en el disco duro de los computadores personales. Esta práctica ayuda a que cualquier intruso que trate de acceder a la información tiene que superar dos niveles de seguridad: el del computador local y el del servidor de la red y normalmente es más difícil tener acceso a la información de un servidor que al de un computador personal.
- La Ilustre Municipalidad contará con cámaras de vigilancia las 24 horas del día, hemos visto conveniente colocar una cámara en los departamento de:

  - Recaudaciones
  - Agua Potable
  - Jefatura de Avalúos y Catastros
  - Financiero
  - Alcaldía
  - En las 2 puertas de Ingreso al edificio

Qué hacer si ocurre un robo

- Los responsables de cada departamento realizarán un inventario de lo sustraído.
- La persona que labora como operadora informará a las autoridades pertinentes sobre dicho acontecimiento.
- Los responsables de cada departamento y el responsable de la seguridad física del edificio revisarán las políticas.

2.3.5. Filtraciones de Agua

Aunque las filtraciones de agua en La Ilustre Municipalidad es poco probable que suceda, no hay que descartar la posibilidad de ocurrencia, es por esto que a continuación se presentan algunas precauciones que deben tomarse.

Precauciones

- El personal de limpieza mantendrá limpios los sistemas de drenaje y verificará que estos funcionen correctamente.
- La operadora de la Ilustre Municipalidad debe dar la señal de alerta a los organismos pertinentes, en caso de ser necesario.
- Se debe tener los equipos de la Municipalidad asegurados de tal manera que dicha empresa cubra los equipos estropeados**.**

Que hacer si ocurre la filtración de Agua

- Los responsables de cada departamento deben realizar una auditoría de las pérdidas de equipos fijándose siempre sobre la posibilidad de rescatar parte o la totalidad de los mismos.
- El responsable de sistemas para volver a instalar los equipos nuevamente ya sean estos propiedad de la Ilustre Municipalidad o nuevos, debe asegurar que la infraestructura sea segura y esté en buenas condiciones.
- La persona responsable de sistemas realizará un análisis de los daños ocasionados en los equipos de computación como: servidores, computadores y equipos de la red.
- El responsable de sistemas debe restaurar las aplicaciones que son proporcionadas por la AME (Asociación de Municipalidades Ecuatorianas) y demás aplicaciones adquiridas por La Ilustre Municipalidad como PROFIM y BRAIN que son sistemas para la gestión financiera Municipal, estos sistemas serán restaurados al igual que las base de datos junto con la información recuperada y el responsable de sistemas notificará a los diferentes usuarios que pueden volver a utilizar cada uno de los sistemas.
- Los empleados podrán encender el computador, posterior a la revisión interna del equipo, que estará a cargo del Ingeniero responsable del departamento de sistemas.
- Los responsables de cada departamento junto a las autoridades superiores de La Municipalidad, analizarán la infraestructura del edificio para evitar que vuelva a ocurrir una nueva filtración de agua.

2.3.6. Errores de Hardware

En La Ilustre Municipalidad de Paute los computadores pueden fallar por varias razones mencionadas a continuación:

- Ningún computador puede estar sujeto a cambios bruscos de energía, si es así la fuente de alimentación puede fallar, se recomienda verificar las instalaciones eléctricas.
- La memoria RAM también puede fallar repentinamente, en particular si se sobrecalienta, o simplemente los pines de la memoria no están haciendo contacto con los pines del slot respectivo, esto suele suceder por exceso de polvo en dicha unidad, el responsable de sistemas tendrá que realizar mantenimientos frecuentes, recomendable cada 6 meses.
- Verificar si los ventiladores del computador funcionan correctamente.
- Cuando el computador empieza a emitir sonidos raros parecidos a la de un reloj, es muy probable que el disco duro este empezando a fallar, el responsable de sistemas tendrá que almacenar la información en discos extraíbles para salvaguardar la información, antes de que el disco duro falle completamente.
- Si el sistema se vuelve inestable es porque algunos sectores del disco duro pueden estar defectuosos, para ello se sugiere un cambio de disco duro, se puede realizar una reinstalando el sistema operativo o simplemente realizando un Scandisk.

2.3.7. Virus Informáticos

Los virus informáticos suponen una fuente constante de riesgos para la Institución, la amenaza de estos agentes se cierne sobre los sistemas informáticos de forma continua y las consecuencias económicas de una infección son muy graves.

Precauciones

- Todos los computadores deben estar protegidos con un buen antivirus y realizar cada dos días su respectiva actualización.

- En el caso de los servidores, se deben proteger con firewall y con un antivirus actualizado.
- No abrir mensajes de correo desconocidos.
- No activar ejecutables (archivos con extensión .exe).
- Utilizar software legal.
- Realizar copias de seguridad de la información periódicamente.

Qué hacer si ocurre una infección de virus informático

Las acciones más inmediatas serán la contención del virus para que no se extienda y a continuación su erradicación, se describen a continuación algunas actividades para aplicar en caso de una infección.

- Comunicar al responsable del departamento de sistemas sobre lo ocurrido, antes de que el virus infecte a más máquinas del área de trabajo.
- Una vez contenido el virus, deberá desinfectar el sistema y luego examinar cada uno de los equipos de cada departamento junto a los servidores.
- El responsable de sistemas debe realizar un escaneo minucioso de todos los archivos existentes, puesto que los virus están pensados para que se extiendan, entonces no se debe detener cuando haya encontrado el primero se debe seguir buscando hasta estar seguro de que ha comprobado todas las fuentes posibles, es probable que encuentre varios centenares de copias del virus en el sistema.
- Todos los usuarios antes de acceder a información almacenada en dispositivos extraíbles, analizarán dicho dispositivo con el antivirus previamente instalado en su computador.

2.4. Problemas de Conectividad de red

Los problemas de conectividad de red tienen distintas causas pero normalmente se deben a adaptadores de red incorrectos, a un hardware defectuoso o a problemas del controlador. Algunos síntomas de los problemas de conectividad son intermitentes, por lo tanto se detallan algunas pautas para evitar estos problemas.

- Verificar si las tarjetas de red de cada una de los computadores de la Institución funcionan correctamente, es decir:

  - Verificar si el dispositivo esta correctamente instalado físicamente.
  - Verificar si el driver o controlador del dispositivo esta correctamente instalado.

- Si un computador no se conecta correctamente a la red, se debe realizar las siguientes actividades.

  - Comprobar que el conector RJ-45 este correctamente conectado a la tarjeta de red.
  - Comprobar si el patch cord no tiene defectos, es decir que no esté deteriorado.
  - Comprobar si el patch cord está bien conectado tanto en el punto de red, como en la tarjeta de red del computador.
  - Verificar el cable de red desde el punto hasta la conexión al switch.
  - Verificar en el cuarto de telecomunicaciones el estado y funcionamiento del switch

2.5. Plan de Contingencia para cuidar la Integridad del Personal

2.5.1. Acciones antes de la contingencia

- El departamento de sistemas realizará capacitaciones permanentes a todos los empleados que laboran en La Institución, acerca de los riesgos con mayor probabilidad de ocurrencia.
- La Ilustre Municipalidad estará en la obligación de capacitar al personal en temas como primeros auxilios, la misma que solicitará al cuerpo de bomberos dicte dicha capacitación.
- La Municipalidad debe contratar un ingeniero eléctrico para implementar alarmas de emergencia en cada departamento.
- Establecer procedimientos de evacuación en caso de cualquier desastre.

2.5.2. Acciones durante la contingencia

- Cualquier empleado que labora en La Institución es responsable de activar las alarmas lo más pronto posible.
- Priorizar la evacuación del personal.

2.5.3. Acciones después de la contingencia

- Brindar los primeros auxilios a las personas que lo requieran.
- Realizar un recuento de los daños causados.
- Retroalimentar los planes de contingencia con lo aprendido en la última contingencia, para remediarlos en caso de que vuelva a ocurrir.

2.5.4. Documentos necesarios previos a las contingencias

- Contar con una copia del inventario del mobiliario y equipo existente en La Institución.
- Contar con el diseño de la red con sus respectivas configuraciones y las características de los computadores de cada uno de los departamentos que conforman La Ilustre Municipalidad.
- Contar con documentación al día de contratos de mantenimiento de computadores de La Ilustre Municipalidad.

2.6. Pruebas y Mantenimientos

El responsable de la contingencia de La Ilustre Municipalidad de Paute, reunirá a todo el personal o al menos un representante de cada departamento para el cumplimiento de este plan de contingencia, se tendrá que realizar una capacitación acerca de lo que deben hacer, como hacer y quien debe hacer; en cada uno de los casos, de la siguiente manera:

- Al momento de realizar las pruebas pertinentes se deben tener en cuenta que ante todo está la seguridad de las personas y luego de la información.

- El responsable de sistemas explicará a todo el personal de La Institución a cerca de la recuperación ante cualquiera de los casos, comunicándoles a cada uno sus funciones y responsabilidades.
- Este documento lo deben conocer todas aquellas personas responsables del cumplimiento del plan y en el caso de que el documento cambie debe ser comunicado a todo el personal de dicho cambio.
- Si es que fallara una contingencia se comunicaría al personal responsable para que solucione dicha anomalía y los cambios realizados se comunicarán inmediatamente al personal.
- Las pruebas junto a la revisión de esta documentación se realizará semestralmente y se probará la factibilidad de las respuestas propuestas para cada una de las contingencias.

No hay que olvidarse que para la realización de las pruebas se tomaran los días laborables, coordinando con las personas, la fecha, hora y área para realización de dicha prueba.

Una vez concluida cada prueba se reunirá todo el personal que participó, el observador y el responsable para analizar y discutir los sucesos acontecidos durante la misma.

El personal involucrado sacará sus propias conclusiones ya que eso ayudará a detectar posibles deficiencias en el plan de contingencia planteado.