MUNICIPALIDAD PROVINCIAL DE HUANCAYO
Incontrastable y moderna

PLAN DE CONTINGENCIA DE LA SUB GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
V. 1.0

SGTIC

MPH

Contenido

INTRODUCCION

El plan de contingencia de la Sub Gerencia de Tecnologías de la información y Comunicación de la Municipalidad Provincial de Huancayo, es un documento que establece estrategias de respuestas para atender en forma oportuna, eficiente y eficaz, ante un desastre en la Plataforma Tecnológica producto de eventos naturales o incidentes tanto internos como externos en la sede del palacio municipal con respecto a las tecnologías de la Información y Comunicación (TIC).

En la primera parte del presente documento se considera aspectos conceptuales que permitan entendimiento de las contingencias y que servirán como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencias. Las causas para aplicar el Plan de Contingencias pueden ser variadas, desde la falta de energía eléctrica y telecomunicaciones hasta una incorrecta circulación de la información.

El Plan de Contingencia implica un importante avance a la hora de superar situaciones de perdidas, tanto materiales y aquellas relacionadas con las actividades y servicios de la municipalidad durante un periodo de tiempo más o menos largo.

Actualmente, los profesionales y técnicos de la Sub gerencia de tecnologías de información y comunicación tienen como una de sus principales actividades y preocupaciones la seguridad de la información, que constituyen un respaldo a las funciones institucionales realizadas a través de los años, así como en la actualidad facilitan a sobre manera las tareas que se desarrollan en la ejecución de los diferentes procesos administrativos, logísticos, ejecutivos, informativos, sociales de planeamiento y de servicios.

CAPITULO I: DEFINICIONES Y ALCANCES

1.1. OBJETIVOS

1.1.1. GENERAL

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la Sub Gerencia de Tecnologías de información y Comunicación, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la Sub Gerencia de Tecnologías de información y Comunicación.

1.1.2. ESPECIFICOS

- Contar con documentación práctica y actualizada que garantice a la **SGTIC** la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
- Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse en las actividades de la **SGTIC**.

1.2. BASE LEGAL

1.1.3. CONSTITUCIÓN POLÍTICA DEL PERÚ

- Inciso 3 del artículo 200
- Incisos 5 del artículo 2
- Incisos 6 del artículo 2
- Ley referida a la aplicación de la Acción Constitucional de Hábeas Data LEY Nº 26301
- Modifican la Constitución Política de Estado, en lo referido a las Garantías Constitucionales LEY Nº 26470

1.1.4. MANIFESTACIÓN DE VOLUNTAD POR MEDIOS ELECTRÓNICOS

- Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica. LEY Nº 27291

1.1.5. FIRMAS Y CERTIFICADOS DIGITALES

- Ley de Firmas y Certificados Digitales LEY Nº 27269
- Ley que modifica la Ley de Firmas y Certificados Digitales, en relación con Certificados emitidos por Entidades Extranjeras LEY Nº 27310
- Comisión multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales, RESOLUCIÓN SUPREMA 098-2000-JUS
- Disposiciones complementarias al Reglamento de la Ley de Firmas y Certificados Digitales RESOLUCIÓN COMISIÓN DE REGLAMENTOS TÉCNICOS Y COMERCIALES Nº 0103-2003-CRT-INDECOPI
- Reglamento de la Ley de Firmas y Certificados Digitales, 019-2002-JUS
- Reglamento de la Ley de Firmas y Certificados Digitales, DECRETO SUPREMO N° 004-2007-PCM
- Reglamento de la Ley de Firmas y Certificados Digitales, DECRETO SUPREMO Nº 052-2008-PCM

1.1.6. DELITOS INFORMÁTICOS

- Ley que incorpora los delitos informáticos al Código Penal LEY Nº 27309
- Delito de Violación a la Intimidad, CÓDIGO PENAL, Artículo 154
- Uso Indebido de Archivos Computarizados CÓDIGO PENAL, Artículo 157
- Hurto Agravado por Transferencia Electrónica de Fondos CÓDIGO PENAL, Artículo 185
- Delitos contra los Derechos de Autor Difusión, distribución y circulación de la obra sin la autorización del autor, CÓDIGO PENAL, Artículo 217
- Plagio y comercialización de obra, CÓDIGO PENAL, Artículo 218

1.1.7. MICROFORMAS NORMAS GENERALES

- Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras. DECRETO LEGISLATIVO Nº 681
- Reglamento del Decreto Legislativo Nº 681, sobre el uso de tecnologías de avanzada en materia de archivos de las empresas DECRETO SUPREMO Nº 009-92-JUS
- Modifican el D. Leg. N° 681, mediante el cual se regula el uso de tecnologías avanzadas en materia de archivo de documentos e información LEY Nº 26612
- Decreto Legislativo Nº 827, Amplían los alcances del D. Leg. Nº 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales

- Reglamento sobre el uso de tecnologías avanzadas en materia de archivo de documentos e información a entidades públicas o privadas, DECRETO SUPREMO Nº 001-2000-JUS

1.1.8. SOFTWARE

- Ley que norma el uso, adquisición y adecuación del software en la administración pública, LEY N° 28612
- Reglamento de la Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la Administración Pública, DECRETO SUPREMO N° 024-2006-PCM
- "Guía Técnica sobre Evaluación de Software para la Administración Pública", RESOLUCIÓN MINISTERIAL Nº 139-2004-PCM
- Guía para la Administración Eficiente del Software Legal en la Administración Pública, RESOLUCIÓN MINISTERIAL Nº 073-2004-PCM
- Medidas para garantizar la legalidad de la adquisición de software en entidades y dependencias del sector público, Decreto Supremo Nº 013-2003-PCM y sus modificatorias
- Decreto Supremo 076-2010-PCM, Decreto Supremo que modifica el Decreto Supremo Nº 013-2003-PCM estableciendo disposiciones referidas a las adquisiciones de computadoras personales que convoquen las entidades públicas

1.1.9. INTERNET

- Lineamientos de Políticas Generales para promover la masificación del acceso a Internet en el Perú, DECRETO SUPREMO Nº 066-2001-PCM
- Proyecto Piloto en Telecomunicaciones "Cabinas de Acceso Público a Internet - Banco de la Nación" RESOLUCIÓN MINISTERIAL Nº 347-2001-MTC-15.03
- Crean el Proyecto Huascarán DECRETO SUPREMO Nº 067-2001-ED
- Reglamento del Fondo Nacional para el Uso de Nuevas Tecnologías en la Educación - FONDUNET DECRETO SUPREMO Nº 070-2001-ED

1.1.10. PORTAL DEL ESTADO PERUANO

- Portal del Estado Peruano como sistema interactivo de información a los ciudadanos a través de Internet DECRETO SUPREMO N° 060-2001-PCM
- Portal de Servicios al Ciudadano y Empresas - PSCE DECRETO SUPREMO N° 032-2006-PCM
- Centro de Administración del Portal del Estado Peruano – CAPEP RESOLUCIÓN JEFATURAL N° 229-2001-INEI
- Directiva "Normas y Procedimientos Técnicos sobre Contenidos de las Páginas Web en las Entidades de la Administración Pública RESOLUCIÓN JEFATURAL N° 234-2001-INEI

- Directiva "Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las entidades de la Administración Pública" RESOLUCIÓN JEFATURAL N° 347-2001-INEI
- Directiva N° 006-2002-INEI/DTNP sobre "Normas y Procedimientos Técnicos para la Actualización de Contenidos del Portal del Estado Peruano" RESOLUCIÓN JEFATURAL N° 160-2002-INEI
- Implementación del Portal de Transparencia Estándar en las Entidades de la Administración Pública, DECRETO SUPREMO Nº 063-2010-PCM
- Administración del "Portal del Estado Peruano" DECRETO SUPREMO Nº 059-2004-PCM
- Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas y se crea el Sistema Integrado de Servicios Públicos Virtuales DECRETO SUPREMO N° 019-2007-PCM

1.1.11. NOMBRES DE DOMINIO

- Encargan al INDECOPI la administración del nombre de dominio correspondiente al Perú en Internet RESOLUCIÓN SUPREMA Nº 292-2001-RE
- Directiva "Normas Técnicas para la asignación de nombres de Dominio de las entidades de la Administración Pública" RESOLUCIÓN JEFATURAL N° 207-2002-INEI
- Constituyen Comisión Multisectorial de Políticas del Sistema de Nombres de Dominio, RESOLUCIÓN MINISTERIAL Nº 285-2005-PCM

1.1.12. SOCIEDAD DE LA INFORMACIÓN

- Convenio a suscribirse con el PNUD para ejecutar Proyecto "Desarrollo de la Sociedad de la Información", RESOLUCIÓN SUPREMA Nº 004-2003-MTC
- Comisión Multisectorial para el Desarrollo de la Sociedad de la Información - CODESI RESOLUCIÓN MINISTERIAL Nº 181-2003-PCM
- Adenda al Convenio con el PNUD para administración del Proyecto PER/03/005 "Desarrollo de la Sociedad de la Información en el País" RESOLUCIÓN SUPREMA Nº 014-2003-MTC
- Publicación en la Web de PCM y CODESI, informes relacionados al desarrollo de la sociedad de la información en el Perú RESOLUCIÓN MINISTERIAL Nº 235-2004-PCM
- Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0, DECRETO SUPREMO N° 066-2011-PCM

1.1.13. SIMPLIFICACIÓN ADMINISTRATIVA

- Ley que modifica el párrafo 38.3 del artículo 38º de la Ley Nº 27444, Ley Del Procedimiento Administrativo General, y establece la publicación de diversos dispositivos legales en el Portal del Estado Peruano y en Portales Institucionales, LEY 29091

- Reglamento de la Ley Nº 29091 - Ley que modifica el párrafo 38.3 del artículo 38º de la Ley Nº 27444, Ley del Procedimiento Administrativo General, y establece la publicación de diversos dispositivos legales en el Portal del Estado Peruano y en Portales Institucionales, DECRETO SUPREMO 004-2008-PCM
- Decreto Legislativo que Modifica la Ley del Procedimiento Administrativo General - Ley 27444 y la Ley del Silencio Administrativo - Ley 29060, DECRETO LEGISLATIVO 1029
- Plan Nacional de Simplificación Administrativa, RESOLUCIÓN MINISTERIAL Nº 228-2010-PCM,
- Establecen el uso del Sistema de Programación y Gestión por Metas y Resultados denominado Sistema de Metas SIGOB/Perú, DECRETO SUPREMO Nº 038-2010-PCM
- Centro de Atención Telefónica "Aló MAC" como servicio integrado de atención dirigido a la ciudadanía, DECRETO SUPREMO Nº 027-2010-PCM

1.1.14. GOBIERNO ELECTRÓNICO

- Estrategia Nacional de Gobierno, RESOLUCIÓN MINISTERIAL Nº 274-2006-PCM
- Uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática, RESOLUCIÓN MINISTERIAL Nº 179-2004-PCM
- Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, RESOLUCIÓN MINISTERIAL Nº 247-2006-PCM
- Formulación y evaluación del Plan Operativo Informático de las entidades de la Administración Pública y su Guía de Elaboración, RESOLUCIÓN MINISTERIAL Nº 19-2011-PCM
- Lineamientos que establecen el contenido mínimo de los Planes Estratégicos de Gobierno Electrónico, RESOLUCIÓN MINISTERIAL Nº 61-2011-PCM

1.3. ALCANCE

El presente documento es de observancia y estricto cumplimiento de todo el personal de la Municipalidad Provincial de Huancayo, sea cual fuere su régimen laboral, además de minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

1.4. DEFINICIONES, ACRONIMOS Y ABREVIATURAS

Contingencia.- Posibilidad que suceda, una interrupción; incidencia o hecho que se presente de forma imprevista.

Plan de Contingencia.- Es un instrumento de gestión para una buena administración de las tecnologías de la información y de las Comunicaciones, en el dominio del soporte y desempeño.

Ataque.- Acción o evento que intente inferir con el funcionamiento adecuado de un sistema informático, conectividad de una red de computadoras o intento de obtener modo no autorizado la información confiada a una computadora.

Amenaza.- Evento o acción que pueda inferir con el funcionamiento adecuado de una computadora, red de computadoras o causar la difusión no autorizada de información confiada a una computadora.

Incidente. - Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las faltas de suministro eléctrico o un intento de borrado de un archivo protegido.

CAPITULO II: PLAN DE CONTINGENCIAS

2.1. SITUACIÓN ACTUAL DIAGNOSTICO SITUACIONAL

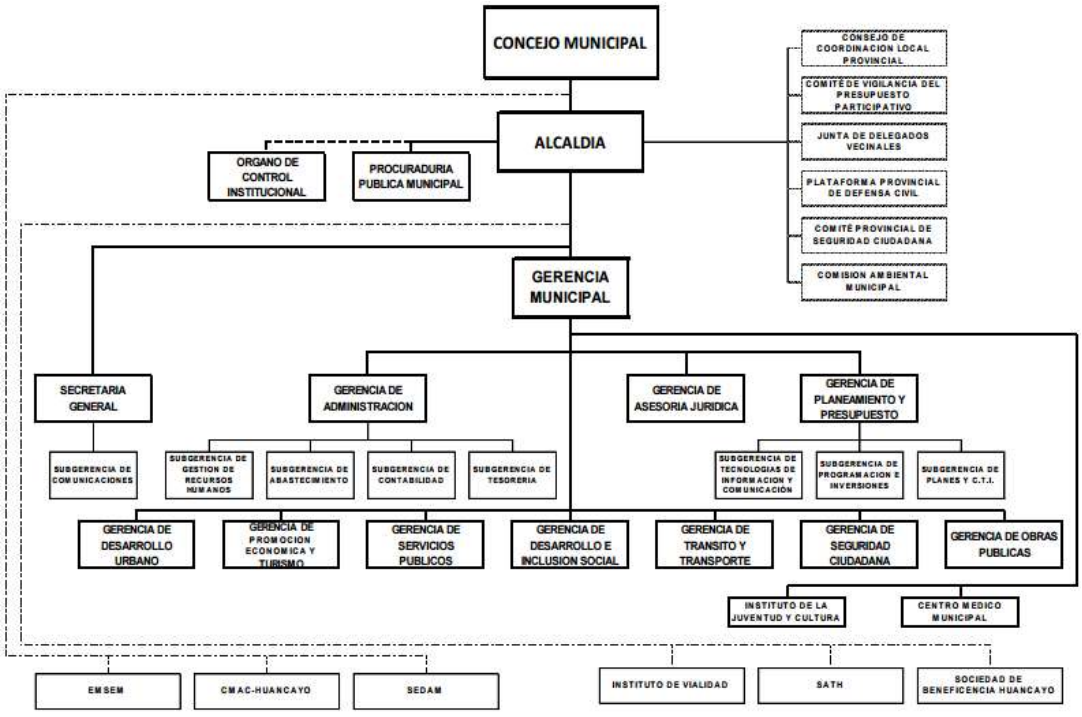
La Sub Gerencia de Tecnologías de Información y Comunicación, responsables del monitoreo del parque informático, cuenta con un proceso de copias de seguridad (BACKUPS) los cuales ayudan a mantener actualizados todos los sistemas de gestión, las mismas que son generadas diariamente, semanalmente, quincenalmente y mensualmente dependiendo el nivel de importancia de la información y/o aplicativo.

La Sub Gerencia de Tecnologías de Información y Comunicación, cuenta con 9 directivas en competencia al uso de equipamiento y servicios informáticos. Aprobada mediante RESOLUCION DE GERENCIA MUNICIPAL N° 150 -2012-MPH/GM.

Así mismo cabe resaltar que el plan de contingencias es una respuesta planificada ante eventos que pudieran interrumpir el normal funcionamiento de la Municipalidad Provincial de Huancayo, tal plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de todo Palacio Municipal.

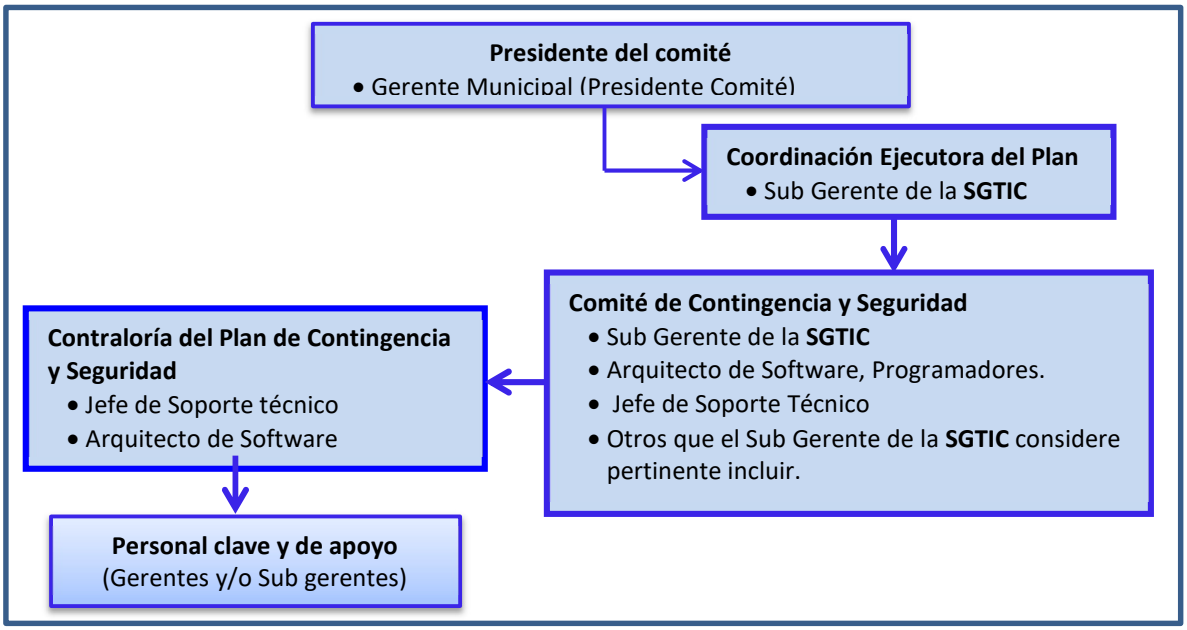
2.2. ORGANIZACIÓN DEL PLAN DE CONTINGENCIA

2.2.1. ORGANIGRAMA



Es necesario entonces que la definición de un Plan de Contingencia informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a todos los trabajadores de la Municipalidad Provincial de Huancayo, que serán personal clave de otras gerencias y/o sub gerencias las cuales serán personas que tienen una trascendencia importante en temas de pro actividad y experiencia en sus respectivas áreas en el Plan de Prevención, Ejecución y Recuperación, es debido principalmente a que las tecnologías de información y comunicación (TIC) se encuentran dispersas e integradas por todo palacio municipal, pero definiendo un grupo responsable para su elaboración, validación y mantenimiento los cuales estará conformado por el personal de la Sub Gerencia de Tecnologías de la Información y Comunicación . Por lo que se propone la siguiente organización según el gráfico Nº 1:

Gráfico 1: Organización Administrativa del plan de Contingencia



A continuación, se describe las funciones y roles de la Organización Administrativa del Plan de Contingencia:

Presidente del comité. –

Es el responsable de aprobar la realización del Plan de Contingencia Informático, dirigir los comunicados de concientización y solicitud de apoyo a los gerentes de las diferentes áreas involucradas y aprobar su terminación. Una vez concluida la realización del Plan de Contingencia, el presidente tendrá una función principal, verificar que se realicen reuniones periódicas, cuando menos cada seis meses, en donde se informe de los posibles

cambios que se deban efectuar al plan original y que se efectúen pruebas de correcto funcionamiento del Plan de Contingencia informático, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten.

Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alterno y autorizará las inversiones a realizar, así como el fondo de efectivo a asignarse paro los gastos necesarios iniciales.

Coordinación Ejecutora del Plan.-

La Coordinación ejecutora del Plan de Contingencia será responsabilidad del Sub Gerente de la **SGTIC**, definiendo todas las políticas y acciones a llevarse a cabo durante un evento de contingencia, también será responsable de que todas las actividades se cumplan de acuerdo a lo planeado. Dicha coordinación será asistida y ejecutada en colaboración de las Direcciones de Líneas de la **SGTIC.**

Funciones y Roles de la Coordinación Ejecutora del Plan:

- Mantener permanentemente actualizado el Plan de Contingencia.
- Responsable de la ejecución del plan de contingencia, cuando se presenten los eventos que lo activan.
- Evaluar el impacto de las contingencias que se presenten.
- Elaborar los informes referidos al Plan de contingencia.
- Proponer al Comité de Contingencia las incorporaciones de eventos al plan de contingencia.
- Proponer la capacitación al personal nuevo del servicio, sobre las actividades que deben ejecutar cuando se presente la contingencia.
- Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el plan de contingencia.
- Proponer reuniones periódicas sobre el plan de contingencia.

Comité de Contingencia

El Comité de Contingencias es el órgano donde se coordinan y aprueban todas las actividades previamente planificadas para ejecutarse en el caso de contingencias del servicio.

Este comité se reunirá por lo menos con una periodicidad trimestral y en él se definirán los lineamientos a través de los cuales se sustentará el Plan de Contingencia.

Dicho comité estará integrado por los siguientes miembros:

- Sub Gerente de la **SGTIC**
- Arquitecto de Software
- Analista Programador
- Maquetador, modelador y programador web
- Programador Junior
- Responsable de Soporte Técnico
- Auxiliares Técnicos

El Sub Gerente de la **SGTIC**, designará a otros integrantes que considere pertinente a participar en el comité.

Funciones y Roles del Comité del Plan de Contingencia:

- Participar en las reuniones periódicas propuestas por el Coordinador del Plan de Contingencia.
- Proponer la incorporación y/o modificaciones del Plan de contingencia.
- Aprobar y/o rechazar las incorporaciones y/o modificaciones del Plan de Contingencia propuesta por el coordinador de contingencia o sus miembros.
- Verificar que el personal a su cargo se encuentre debidamente capacitado en la ejecución del plan de contingencia.
- Coordinar la ejecución de las actividades del plan de pruebas.
- Aprobar los informes presentados por la coordinación del plan respecto a cualquier evento relacionado con el mismo.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.
- Coordinar con los recursos y/o proveedores externos necesarios para soportar y restaurar los servicios afectados por la contingencia.
- Coordinar y ejecutar la capacitación al personal nuevo del servicio sobre las actividades que deben de ejecutar cuando se presenta la contingencia.

Contraloría del Plan de Contingencia

La Oficina de Auditoría Interna sería el órgano que supervise todos los elementos y recursos descritos para intervenir en una situación de contingencia estén disponibles y sean perfectamente viables de modo tal que se garantice que no se presenten carencias y/o fallas en una situación real bajo las Funciones y Roles siguientes:

- Verificar que el plan de contingencia se encuentre actualizado.
- Revisar y verificar que el documento de plan de contingencia se enmarque dentro del alcance establecido.
- Velar por suministrar los recursos necesarios para la viabilidad del plan de Contingencia y Seguridad.
- Corroborar que el plan de contingencia se cumpla correctamente.
- Presentar los informes del Plan de Contingencia al Comité de Contingencia de la SGTIC.
- Certificar que todos los recursos descritos en el Plan de Contingencia (materiales, humanos, externos, etc.) sean viables y se encuentren disponibles para su uso cuando un evento de contingencia lo requiera.
- Auditar los procesos que forman parte del Plan de Contingencia, corroborando que se cumpla correctamente. Participar y visar las pruebas de validación del Plan de Contingencia. Informar al Comité respecto a cualquier evento o anomalía encontrada que ponga en riesgo la ejecución de todo o parte del plan.
- Proponer y recomendar actividades o procesos de mejora que permitan minimizar los riesgos de operación.

2.3. IDENTIFICACIÓN Y PRIORIZACIÓN DE RIESGOS

Denominamos INCIDENCIA al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

Riesgo: Es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.

2.3.1. Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

2.3.2. Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio. Asimismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de

otro modo, es un problema conocido.
La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

2.3.3. Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia. Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto. Para nuestro caso, clasificaremos el impacto con una escala del 1 al 4.

2.3.4. Exposición al Riesgo

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

2.3.5. Definición de eventos controlables y no controlables

Como parte de la identificación de los riesgos, estos deben categorizarse en función a las acciones de prevención que pueden estar en manos de la Sub Gerencia de Tecnologías de la Información y Comunicación, o cuya ocurrencia no puede predecirse con antelación. Así tenemos que los eventos pueden ser:

Eventos Controlables (C), si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.

Eventos No Controlables (NC), cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.
Esta identificación se hará en la matriz de riesgo explicada a continuación.

2.3.6. Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se

presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy objetivos en su análisis. El factor numérico asignado es directamente proporcional y va en ascenso con respecto al impacto o gravedad que su ocurrencia pueda generar sobre los diferentes alcances del servicio y se clasificarán como se indica en el cuadro N° 1.

Cuadro N °1: Cuadro de Impactos

IMPACTO	DESCRIPCION	VALOR
Poco	Pérdida de Información y/o equipamiento no Sensitivo	1
Moderado	Pérdida de información sensible	2
Alto	Pérdida de información sensible, retraso o interrupción	3
Gran	Información crítica, daño serio, patrimonial	4

Cuadro N °2: Cuadro de Probabilidad de Ocurrencia

PROBALIDAD DE OCURRENCIA	DESCRIPCION	VALOR
Frecuente	Incidentes repetidos	4
Probable	Incidentes aislados	3
Ocasional	Sucede alguna vez	2
Remoto	Improbable que suceda	1

2.4. Definición de eventos susceptibles de contingencia

El Plan de Contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos, que serán considerados para su evaluación:

Hardware

- Servidores
- Estaciones de trabajo (laptops y PC´s)
- Impresoras, fotocopiadoras, scanner
- Equipos multimedia

Comunicaciones

- Equipos de comunicaciones switch y conectores RJ-45
- Equipo de comunicaciones Router y LAN.
- Enlaces de cobre y fibra óptica.
- Cableado de Red de Datos.

Software

- Software de Base de Datos (SQL, Mysql)

- Aplicativos utilizados por la Municipalidad provincial de Huancayo.
- Software de Aplicaciones.
- Software Base (Sistemas operativos y Ofimática).
- Antivirus para protección de servidores y estaciones de trabajo.

Información sobre Sistemas Informáticos

- Base de datos utilizados por los Aplicativos.
- Respaldo de información generada con Software y de Ofimática.
- Respaldo de las Aplicaciones utilizadas por la MPH.
- Respaldos de Base de Datos.
- Respaldos de información, configuración de los Servidores, Firewall y Switch.

Equipos diversos

- UPS
- Aire Acondicionado

Servicios Públicos

- Suministro de Energía Eléctrica.
- Servicio de Telefonía Fija analógico/digital.
- Servicio de Conexión a Internet mediante Fibra Óptica.

Recursos Humanos

- Disponibilidad de personal de dirección.
- Disponibilidad de personal operativo.

2.5. Elaboración de los Planes de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento por el personal de la Sub gerencia de Tecnologías de la Información y Comunicación.

Es por ello, que una fase importante de la metodología considera un formato estándar de registro de todos los eventos definidos que forman parte del plan, así se tendrá finalmente un entregable acorde con los requerimientos y políticas definidas para tal fin.

2.5.1. Formato de Registro del Plan de Contingencia

Para una lectura fácil y rápida del Plan de Contingencia, se ha diseñado un formato, Ver Anexo A02: “Formato Registro Plan de Contingencia”, el mismo que describimos a continuación y que se compone de las siguientes partes:

Encabezado

El formato tiene un encabezado, cuyo contenido se presenta como sigue:

Elaborado: En todos los casos se indica “SGTIC”.

Código del Formato: COD – XX .

Nombre del evento: Claro y de fácil entendimiento.

Cuerpo Principal

En el cual se desarrollará cada uno de los eventos que formarán parte del Plan de Contingencia y se describe el contenido que deberá ir en cada campo.

2.6. Identificación de Riesgos Matriz de Contingencia

Para una lectura fácil y rápida se diseña la matriz de Contingencia, usando el conocimiento y la experiencia práctica de la Sub Gerencia de Tecnologías de la Información y Comunicación.

Cuadro N °4: Matriz de Contingencia

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Categoría
Sub: Factor Riesgos relacionadas a Siniestros				
	INFRAESTRUCTURA			
1	Incendio	1	4	NC
2	Sismo	1	4	NC
3	Inundación por desperfecto de los servicios sanitarios	1	2	C
4	Inundación por lluvias	2	2	NC
	SERVICIOS PÚBLICOS			
5	Interrupción de energía eléctrica	3	4	NC
6	Interrupción de servicios de telefonía	3	3	NC
7	Interrupción del servicio de internet mediante Fibra Óptica	2	4	NC
	EQUIPO			
8	Falla de los Ups	1	4	C
Sub Factor. Riesgos relacionadas a Sistemas de Información				
	INFORMACIÓN			
9	Extravío de Información	2	4	C
10	Sustracción o robo de información	1	3	C
	SOFTWARE			

11	Infección de equipos por virus	2	4	C
12	Perdidas de los sistemas centrales servidores Cuadro N °3: Tabla de Servidores	3	4	C
13	Perdida del servicio de correo	1	3	C
14	Falla del Motor de la base de datos Cuadro N° 4: Tabla de base de datos	2	4	C
15	Falla del sistema operativo	1	4	C
	COMUNICACIONES			
16	Fallas en la red de comunicaciones interna Imagen N °1: Diagrama Físico de Red de la institución	1	4	C
	HARDWARE			
18	Fallas de equipos personales	2	3	C
19	**RECURSO OPERATIVOS Y LOGÍSTICOS**			
20	Falla de equipos multimedia, impresoras, scanner y otros	2	3	C
Sub factor: Riesgos relacionadas a recursos humanos				
	RECURSO HUMANO			
21	Ausencia imprevista del personal de soporte técnico	1	4	C
22	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	1	4	C
23	Falta de idoneidad del personal en la reserva de información de la Base de Datos.	1	4	NC
Sub factor: Plan de seguridad Física				
	INFRAESTRUCTURA			
24	Sustracción de equipos y software diversos	1		NC
25	Sabotaje	1		NC

En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (C), y No Controlables (NC).

2.7. Descripción de Planes

SGTIC	Evento: Incendio		COD: 001 Versión: 1.1
Fecha: 05-2017	Responsable: SGTIC	Involucrados: SGTIC	

1. PREVENCIÓN

Descripción: Fuego de grandes proporciones que arde de forma fortuita o provocada y destruye cosas que no están destinadas a quemarse.

Objetivo: Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones.

Condiciones de Prevención de Riesgo

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Acatar las indicaciones del SGTIC, en torno al evento.
- Mantenimiento de los detectores de humo en el "Centro de Datos"
- Realizar el Mantenimiento a los extintores.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

La Contingencia se activará al ocurrir un incendio.

b. Personal que autoriza la contingencia.

Sub Gerente de TIC.

c. Descripción de las actividades después de activar la contingencia.

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable de la SGTIC.
- Evacuar el área.
- En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de extinguido el incendio, se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados al personal, bienes e instalaciones.
- En caso de daños del personal prestar asistencia médica inmediata
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.

d. Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es el personal de la SGTIC.

b. Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

c. Mecanismos de Comprobación

La SGTIC presentará un informe explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

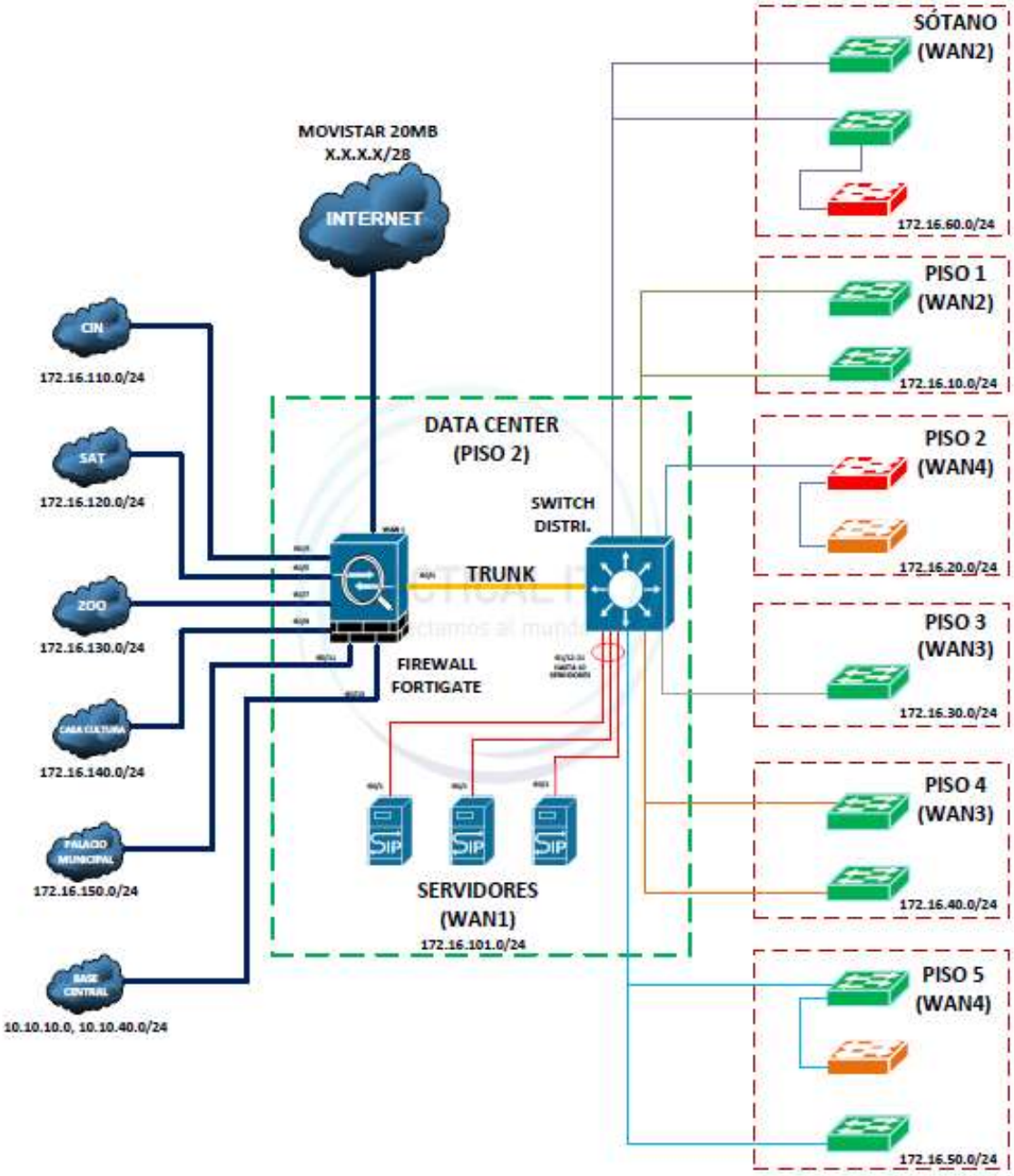
d. Mecanismos de Recuperación

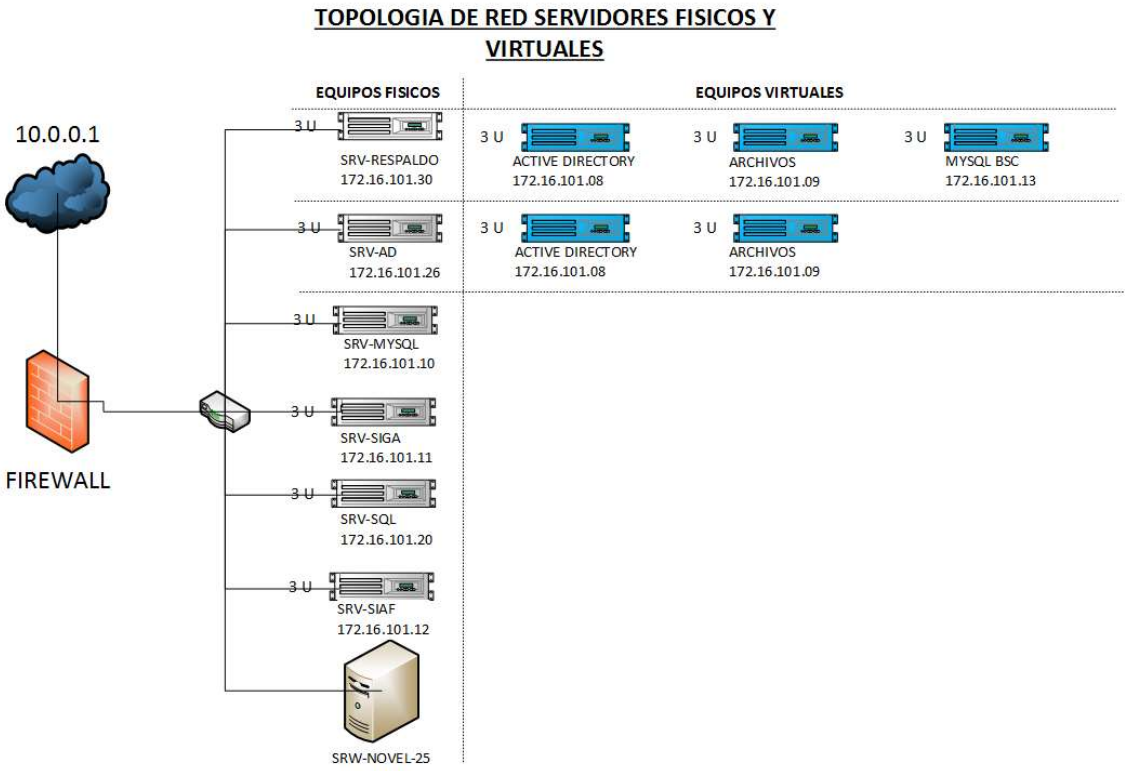
Se efectuara de acuerdo a las instrucciones impartidas que se menciona en el punto a.

e. Desactivación del Plan de Contingencia

El Sub Gerente de TIC desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación.

Diagrama de direccionamiento WAN de la Municipalidad Provincial de Huancayo





2.8. ACTIVIDADES PREVIAS AL DESASTRE

Son aquellas actividades de planeamiento, preparación, entrenamiento, mantenimiento preventivo y correctivo del parque informático y ejecución de las actividades de resguardo de la información e identificación de las propiedades de restauración de los sistemas Informáticos, que nos aseguren un tiempo de respuesta aceptable y optimo y que implique el menor costo posible a la Municipalidad Provincial de Huancayo.

Se han establecido procedimientos referentes al mantenimiento de equipos, impresoras y servidores, copia de respaldo (Backups) e instalación/Actualización de Software Antivirus.

Para poder efectuar en forma óptima y en el menor tiempo posible las actividades descritas anteriormente se debe conocer lo siguiente:

- Reconocer el ambiente donde se encuentran los servidores de la Municipalidad Provincial de Huancayo y saber identificar cada uno de ellos, asimismo la distribución correcta de los equipos informáticos, y los equipos de comunicación. (Ver Anexo 01).
- Gestionar adecuadamente los activos de software para contar con un inventario de software por cada computadora de los usuarios, que facilite una rápida identificación y restauración de los software instalados.

Los Sistemas de Información

Los Sistemas y/o aplicativos desarrollados por Sub Gerencia de Tecnologías de Información y Comunicación se evaluaran con puntaje, que se aplicaran a los niveles de prioridad. (Ver Cuadro Nº1)

Cuadro Nº1: Niveles de prioridad de sistemas de Información

Prioridad	Puntaje
Baja	1
Media	2
Alta	3

A continuación se detalla la lista de los sistemas de información ordenados por prioridad de restauración (desde la máxima prioridad hasta la más baja) Cuadro Nº2

Cuadro Nº2: Sistemas de Información - SGTIC

Sede	IP Servidor	Lenguaje Prog.	Plataforma	Aplicativo	Ruta o URL	Prioridad
PM	10.1.1.10	FOX PRO	Desktop	Sigmamph (Caja)	D:\Caja\	3
PM	Local	FOX PRO	Desktop	Tramite Documentario		3
PM	Local	FOX PRO	Desktop	Sist. GTT		3
PM	Local	JAVA	Desktop	Papeletas GSPL		3
PM	10.0.0.31	FOX PRO	Desktop	SigmaRC (Registro Civil)	D:\SigmaRC	3
PM	10.0.0.31	FOX PRO	Desktop	RCMPH (Registro Civil)	D:\RCMPH	3
PM	Local	.NET VB	Desktop	Control de Personal Biométrico		2
PM	130.0.0.11	Desconocido	Desktop	SIGA		3
PM	130.0.0.12	Desconocido	Desktop	SIAF		3
PM	10.1.1.10	.NET VB	Desktop	Libro de Reclamos Virtual		2
PM	10.1.1.10	FOX PRO	Desktop	Novell (varios)		1
PM	10.1.1.20	.NET VB	Web	Consulta Web GTT	C:\inetpub\wwwroot\	2
PM	10.1.1.20	.NET VB	Web	MMCM	C:\inetpub\wwwroot\	2
PM	10.1.1.20	.NET VB	Web	Biblioteca	C:\inetpub\wwwroot\	2
PM	10.1.1.20	.NET VB	Web	Transportes	C:\inetpub\wwwroot\	2
PM	10.1.1.20	.NET VB	Web	Bromatología	C:\inetpub\wwwroot\	2
PM	10.1.1.10	PHP	Web	Webpebsc	D:\AppServ\www\	2
CIN	192.168.1.100	FOX PRO	Desktop	Sigma (Caja)	D:\Sigma\	3
CIN	192.168.1.100	FOX PRO	Desktop	SisDGC	D:\SisGDEyT\	3
CIN	192.168.1.100	FOX PRO	Desktop	Novell	D:\Novell\smi	3
CIN	192.168.1.100	.NET VB	Desktop	000mphgdet	D:\000mphgdet	2
CIN	192.168.1.100	PHP	Web	Sistema Cobranza Web	D:\MPHcaja	2

Políticas (Normas y Procedimientos de BACKUPS)

La Sub Gerencia de Tecnologías de la Información y Comunicación, responsable del monitoreo informático, tiene establecida una Guía de Procedimientos para obtener copias de seguridad de base de Datos, Aplicativos y Archivos de trabajo de todas las gerencias, sub gerencias y unidades orgánicas de la Municipalidad Provincial de Huancayo.

Entrenamiento

La sub gerencia de tecnologías de Información y Comunicación considera que en el plan de trabajo institucional se debería programar y ejecutar diversas actividades de capacitación teórica y practica contra diferentes tipos de siniestros que afecten el parque informático y la información que se maneja en la Municipalidad Provincial de Huancayo, en ese sentido alta dirección, debería considerar programar eventos para orientar y concientizar a los trabajadores de la Institución respecto a su papel protagónico ante estas amenazas.

Análisis y evaluación de riesgo

Sabemos que los desastres naturales causados por un evento natural o humano, pueden ocurrir y para cada uno de los mismos se presentan distintos tipos de contingencia los riesgos pueden ser: Riesgos naturales, Riesgos Tecnológicos y Riesgos Sociales.

Las causas más representativas que originarían cada uno de los escenarios propuestos en el Plan de Contingencias y Seguridad de la Información se presentan en el siguiente cuadro. **(Cuadro Nº3)**

Cuadro Nº3: Escenarios Propuestos para el Plan de Contingencias

CAUSAS	ESCENARIOS
• Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Swicht. • Fallas Punto puerto desconectado. • Fallas Punto de Red	**I.** **NO HAY COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR EN MPH**
• Fallas de Componentes de Hardware del Servidor. • Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco • Computador de Escritorio funciona como Servidor.	**II.** **FALLA DE UN SERVIDOR.**
• Accidente • Renuncia Intempestiva • Culminación de contrato	**III.** **AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE TECNOLOGÍA DE LA INFORMACIÓN.**
• Corte General del Fluido eléctrico	

	IV. **INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS**
• Falla de equipos de comunicación: SWITCH, Antenas, • Fallas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet.	**V.** **PERDIDA DE SERVICIO DE INTERNET**
• Incendio • Sabotaje • Corto Circuito • Terremoto • Tsunami • Inundaciones	**VI** **INDISPONIBILIDAD DEL CENTRO DE COMPUTO-SGTIC** **(DESTRUCCIÓN DE LA SALA DE SERVIDORES)**

Definición de elementos susceptibles de contingencia

El Plan de Contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos, que serán considerados para su evaluación:

- **Hardware**
  - Servidor de Base de Datos SQL, Aplicaciones Visual Basic (IP. 10.1.1.20)
  - Servidor de Base de Datos MySQL, Aplicaciones PHP (IP. 10.1.1.10)
  - Servidor de Archivos (IP. 10.1.1.15)
  - Servidor de Equipos Virtuales (IP. 10.1.1.30)
  - Estaciones de trabajo(laptops y PC´s)
  - Impresoras, fotocopiadoras, scanner
  - Equipos multimedia
- **Comunicaciones**
  - Equipos de comunicaciones Switch y conectores RJ-45
  - Equipo de comunicaciones Router y LAN.
  - Equipo de Telefonía fija
  - Cableado de Red de Datos.
- **Software**
  - Sistema de Transportes
  - Sistema de Caja

- Sistema de Tramite Documentario
- SIGA
- SIAF
- Sistema de Personal
- Sistema de Registro Civil
- Portal Web
- Sigma
- Sistema de Bromatología
- Sistema de Biblioteca
- Antivirus para protección de servidores y estaciones de trabajo.

- **Información sobre Sistemas Informáticos**
  - Base de datos utilizados por los Aplicativos.
  - Respaldo de información generada con Software Base y de Ofimática.
  - Respaldo de las Aplicaciones utilizadas por **SGTIC**.
  - Respaldos de Base de Datos.
  - Respaldos de información y configuración de los Servidores.
- **Equipos diversos**
  - UPS
- **Infraestructura Física**
  - Oficinas Central de la **SGTIC**.
- **Operativos**
  - Logística operativa (suministros Informáticos).
- **Servicios Públicos**
  - Suministro de Energía Eléctrica.
  - Servicio de Telefonía Fija analógico/digital y móvil.
  - Suministro de Agua.
- **Recursos Humanos**
  - Disponibilidad de personal de dirección.
  - Disponibilidad de personal operativo.

2.9. ACTIVIDADES DURANTE EL DESASTRE

2.3.1 Plan de emergencias

La Sub gerencia de Tecnologías de la Información y Comunicación proporciona una relación de su personal, la misma que será utilizada en caso de producirse algún incidente informático, esta lista debe alcanzarse al personal de seguridad y vigilancia de la

Municipalidad Provincial de Huancayo, paro los casos de horarios de fines de semana y/o feriados si se diera la necesidad.

Procedimiento en caso de emergencia

El siguiente procedimiento de acción, especifica los pasos que se deberán seguir en casos de emergencia. Este procedimiento podrá ser modificado para incorporar información adicional que sea pertinente.

a. Determinar la ubicación del incidente, estimar el tamaño y el tipo de incidente.
b. Llevar a cabo acciones específicas para controlar la anomalía informática
c. Notificar la ocurrencia a los responsables del departamento de sistemas de la Entidad.
d. Modificar las operaciones para evitar la re-ocurrencia potencial del incidente.
e. Documentar el incidente.

Se detalla un cuadro (Cuadro Nº4) de resumen de procedimientos durante la emergencia:

Cuadro Nº4: Procedimiento durante la emergencia

PROCEDIMIENTO DURANTE LA EMERGENCIA		
Horario	**Ocurrencia**	**Acción a seguir**
Laboral	Problemas en funcionamiento de computador personal	Avisar a la SGTIC, vía correo, teléfono, informe, personalmente.
Laboral	Problemas en portal, correo, internet y Comunicaciones.	Avisar a la SGTIC, vía correo, teléfono, informe, personalmente.
No Laboral	Problemas en portal, correo, internet y Comunicaciones.	Avisar al agente de seguridad encargado del piso o puerta, quien notificara al personal de la lista de números telefónicos de emergencia.
Laboral	Siniestro	Avisar a la SGTIC, vía correo, teléfono, informe, personalmente.
Laboral	Siniestro	Avisar al vigilante más cercano, quien notificara al personal de la lista de números telefónicos de emergencia.

2.3.2 Escenarios-Impacto de los Riesgos Informáticos

Escenario I: NO HAY COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR EN MPH

A) Impacto

Impacto	Área afectada
No se puede trabajar con los recursos de la red MPH.(Información).	Área en que labora
Interrupción de sus actividades.	Área en que labora.

- **Tiempos aceptables de caída**

Tiempo aceptable de caída	
Recurso	**Prioridad de Recupero**
Sistemas	Alto
Servidor archivos.	Alto
Servidor WEB	Alto
Internet.	Alto

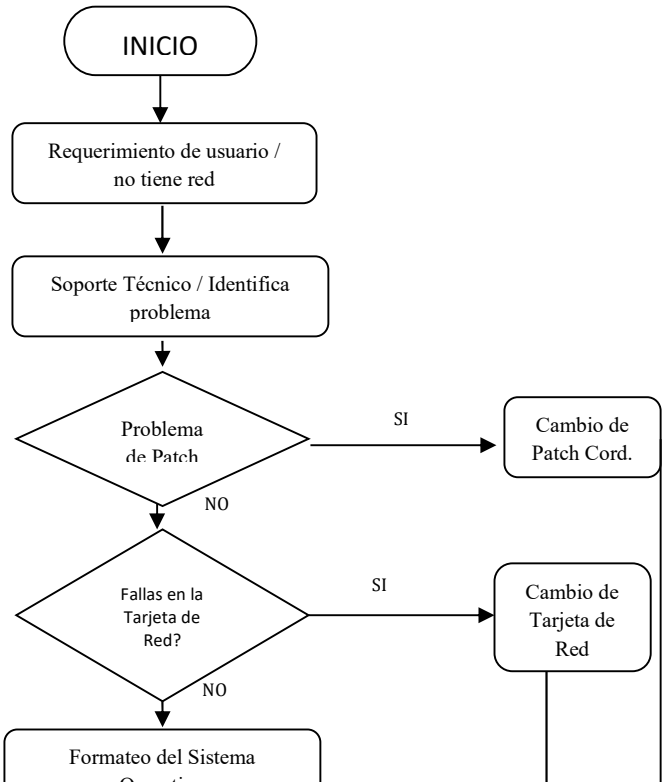
B) Recursos de Contingencia

Componentes de Remplazo:

Tarjeta de Red, Conector RJ-45, Jack RJ-45, Testeador, herramientas de Cableado Estructurado, etc

C) Procedimiento

NO HAY COMUNICACIÓN ENTRE CLIENTE – SERVIDOR EN MPH



Escenario II: FALLA DE UN SERVIDOR

A) Impacto

Impacto	Área afectada
Paralización de los sistemas o aplicaciones que se encuentran en los servidores que presentan fallas	Todas las Áreas
Posible Pérdida de Hardware y Software.	Tecnología de la Información
Perdida del proceso automático de Backup y restore.	Tecnología de la Información
Interrupción de las operaciones.	Tecnología de la Información

- **Tiempos aceptables de caída**

Tiempo aceptable de caída	
Recurso	**Prioridad de Recupero**
Servidor Base de Datos SQL, Aplicaciones Visual Basic (IP. 10.1.1.20)	Alto
Servidor de Base de Datos MySQL, Aplicaciones PHP (IP.10.1.1.10)	Alto
Servidor de Archivos (IP. 10.1.1.15)	Alto
Servidor de Equipos Virtuales (IP. 10.1.1.30)	Alto
Servidor FIREWALL - PROXY	Alto
Servidor SIAF-SIGA	Alto
Servidor Antivirus, Controlador de Dominio Secundario.	Alto
Servidor Backup	Alto

- **Causas de falla de un servidor**

CASO A: ***Error Físico de Disco de un Servidor (Sin RAID).***

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último BACKUP en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios

CASO B: ***Error de Memoria RAM***

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.

- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Institución, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la tarjeta controladora.
4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.

5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de DOS, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO E: Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

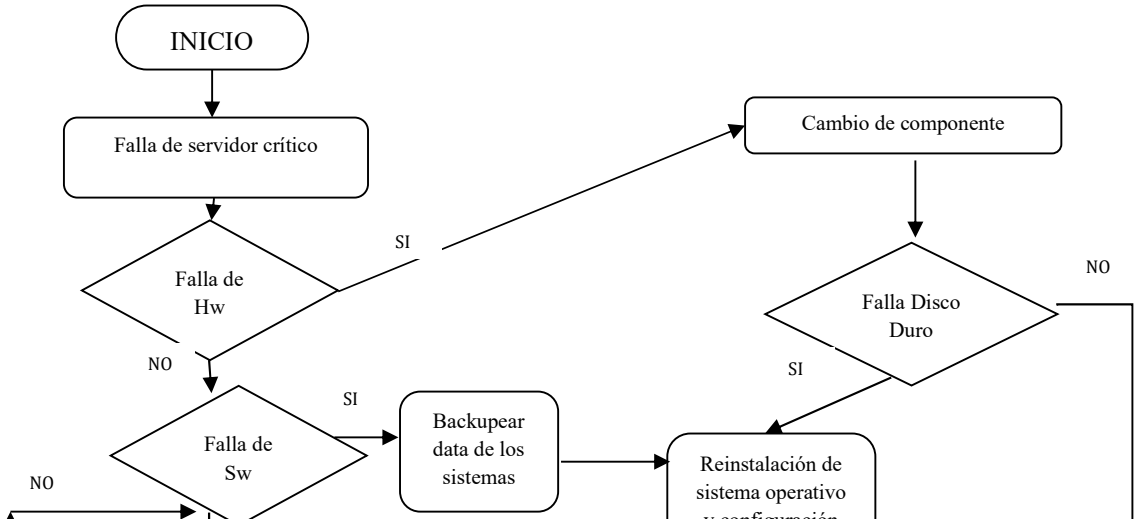
- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del BACKUP.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

B) Recursos de Contingencia

- Componente de Remplazo (Memoria, Disco Duro, Servidor de Contingencia etc.).
- BACKUP diario de Información del servidor

C) Procedimiento:

FALLAS DE UN SERVIDOR CRÍTICO



Escenario III: AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN.

A) Impacto

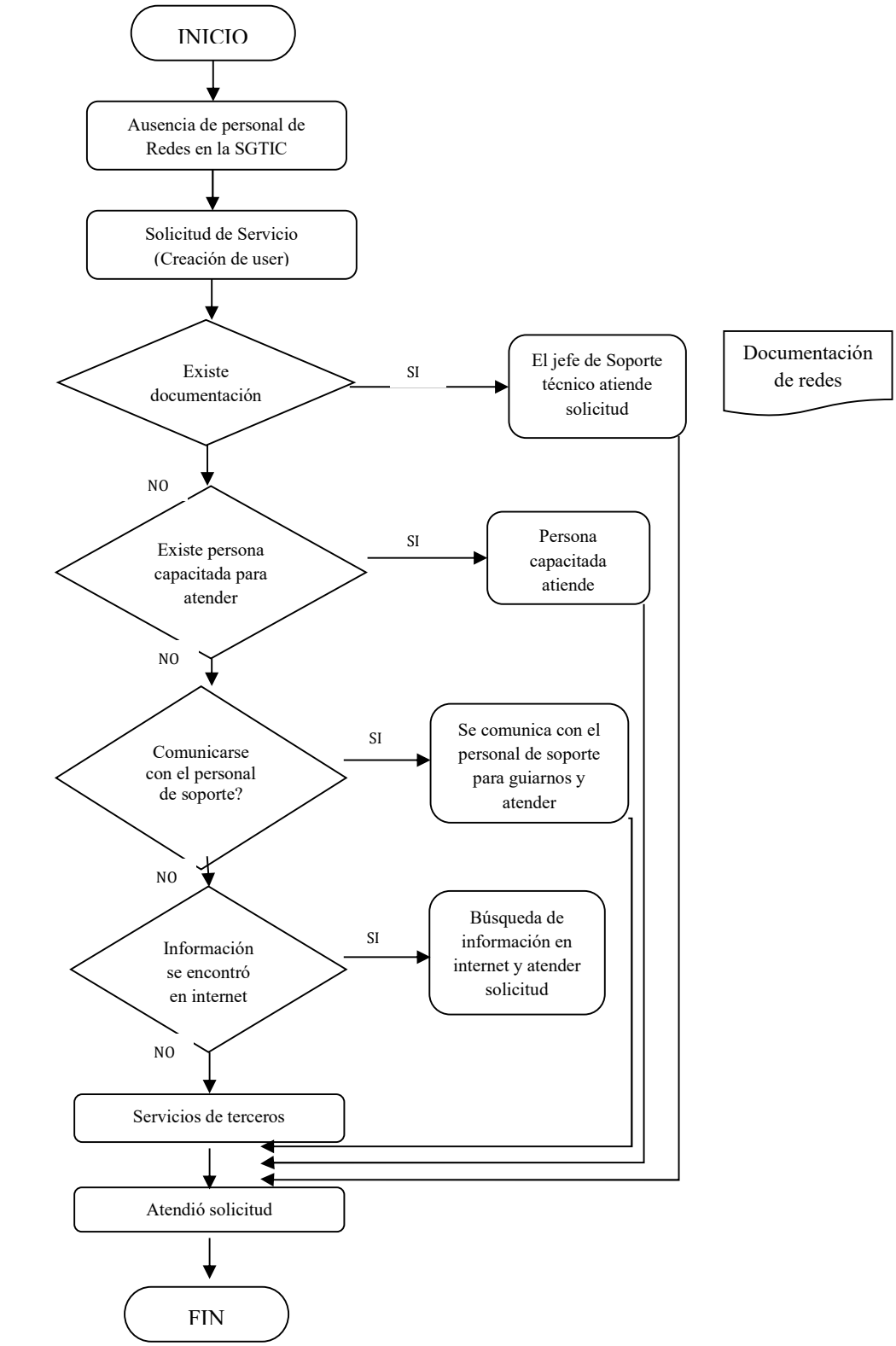
Impacto	**Área afectada**
Interrupción de funciones de la persona ausente	Todas las Áreas
• Administración de bases de datos. • Control y monitoreo de servidores • Soporte a los usuarios. • Ajustes a programas críticos en producción	

B) Recursos de Contingencia

Se presentan las funciones actuales que tienen a su cargo el personal de la Tecnología de la Información.

C) Procedimiento

AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE LA SGTIC



Escenario IV: INTERRUPCIÓN DEL FLUIDO ELÉCTRICO

A) Impacto

Impacto	Área Afectada
Cierre inapropiado de las Bases de Datos	Todas las áreas
Finalización incompleta de los Backup.	Todas las áreas
Falla de un componente de equipo servidor	Todas las áreas
Pérdida total o parcial de la operatividad de los Sistemas.	Todas las áreas

Se puede presentar lo siguiente:

1. Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia (*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón).
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso del UPS.

* Llámese corriente de emergencia a la brindada por UPS.

** Llámese corriente normal a la brindada por la compañía eléctrica.

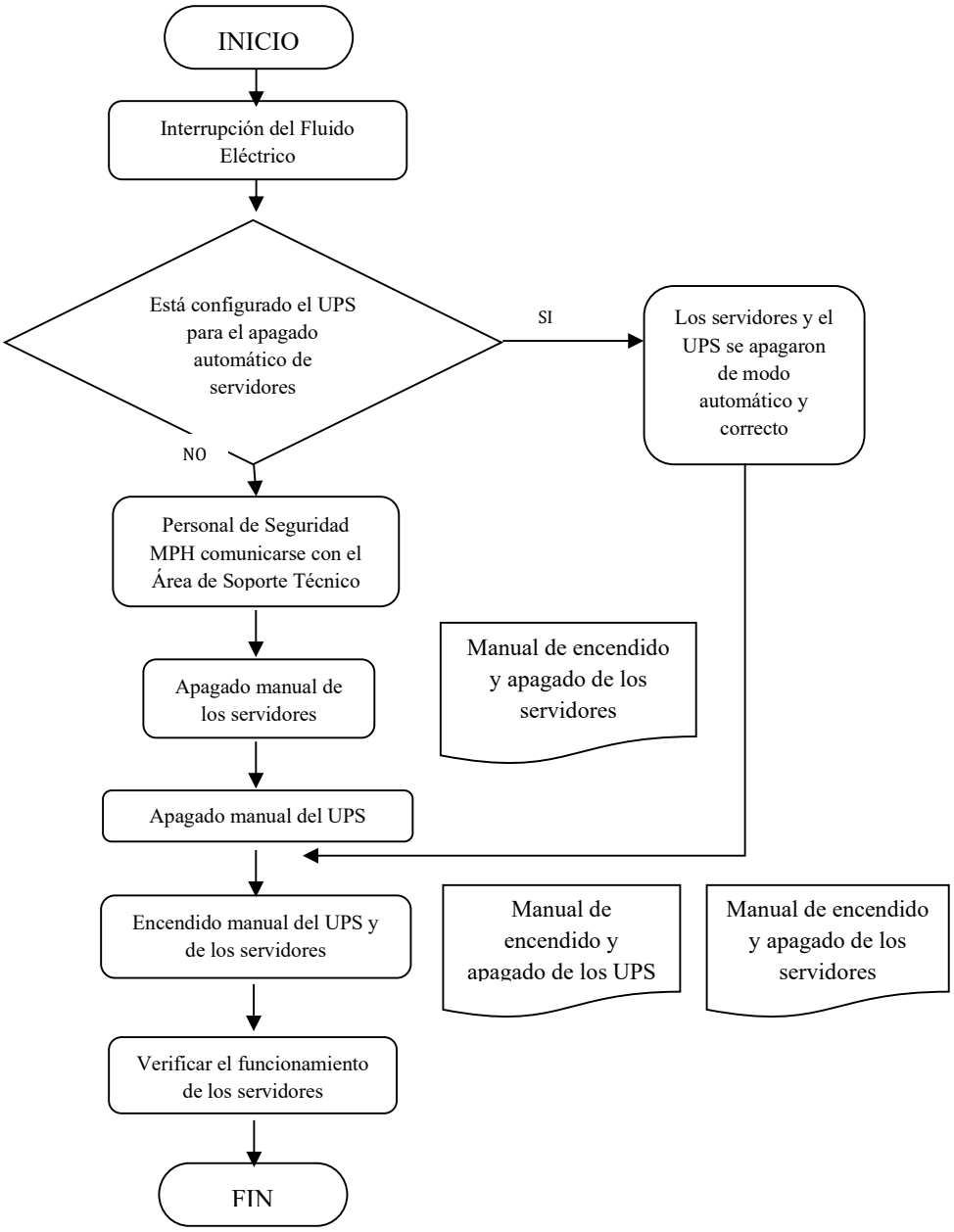
B) Recursos de Contingencia

Si se produjera en horas de la noche una interrupción del fluido eléctrico, se podrían paralizarlos procesos de cierre y backup de los servidores con motores de base de datos.

Por tal motivo es necesario revisar continuamente el estado de las baterías del UPS. Dichas baterías deben garantizar una autonomía de aproximadamente una hora. Es necesario establecer un procedimiento que permita al personal de seguridad de la Municipalidad avisar al personal de Informática de este hecho. El UPS se caracteriza por emitir una alarma fácil de identificar.

C) Procedimiento

INTERRUPCIÓN DEL FLUIDO ELÉCTRICO



Escenario V: CORTE DEL SERVICIO DE INTERNET

A) Impacto

Impacto	Área Afectada
Interrupción de la recepción y envío de información, mensajes y data a nivel nacional e internacional.	Todas las áreas

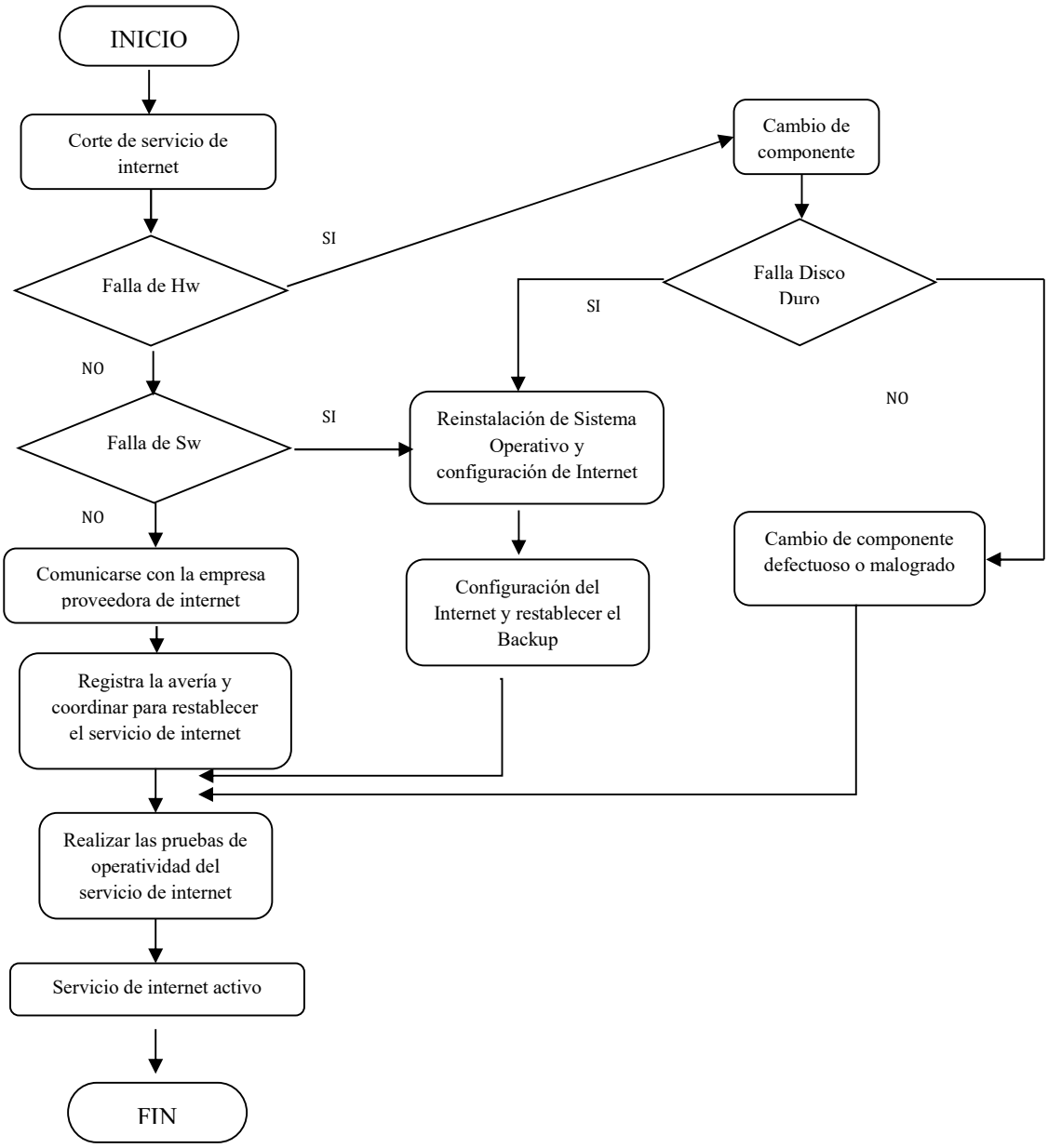
B) Recursos de Contingencia

Hardware

- 1 Router con 1 entrada LAN
- Software
- Herramientas de Internet.
- Backup de las reglas del servidor Firewall.

C) Procedimiento

CORTE DEL SERVICIO DE INTERNET



Escenario IV: INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO

A) Impacto

Impacto	Área Afectada
Caída de la Red LAN: Servidores Windows, equipos de comunicación.	Todas las Áreas
Interrupción de las comunicaciones Internas y Externas.	Todas las Áreas
Paralización de los sistemas que soportan las funciones de la Institución.	Todas las Áreas
Paralización de operaciones de Informática.	Todas las Áreas
Perdida de Hardware y Software.	Tecnología de la Información

IDENTIFICAR IMPACTO DE LA CAIDA Y TIEMPOS ACEPTABLES DE CAIDA		
RECURSO	**IMPACTO**	**TIEMPO DE CAIDA ACEPTABLE**
Servidor Base de Datos,	NO se realiza el control de Asistencia del Personal. No se emiten reportes de Obreros, Planillas, CAS, etc.	
Servidor Web	Dejarían de funcionar aplicativos como: LIBRO DE RECLAMOS, BROMATOLOGIA, BIBLIOTECA, CONSULTA DE TRANSPORTE.	
Servidor de Aplicaciones - SISTEMAS	No se realiza Registro de Comprobantes, Órdenes de Giro, Pagos, Ingresos y Conciliaciones. Dejaría de funcionar el Sistema de Caja, Tramite Documentario	
Servidor de Controlador de Dominio (Active directory)	No existiría seguridad Centralizada en el acceso a la red de la Municipalidad. (No se administra Perfiles, accesos a los sistemas, etc.).	
Servidor SIAF	NO se realiza el Plan Anual de Adquisiciones. No se realizaría el registro de Comprobantes de Pago y Cheques, órdenes de compra, servicio, etc. (Pago al Personal de la Municipalidad provincial de Huancayo).	
Servidor SIGA	No se realizaría notas de pedido, NO se	

	elaboran Requerimientos, NO se realiza la Consolidación de Cuadro de Necesidades.	
Servidor Antivirus	Vulnerabilidad de red de la Municipalidad expuesta a infecciones como Virus, Troyanos, etc y falta de seguridad en el Sistema Operativo, aplicaciones, etc por realizar las actualizaciones.	

B) Recursos de Contingencia

Si es necesario, el hardware y software necesarios deben activarse o adquirirse, así como ser transportados al sitio alterno; las estrategias básicas para disponer de equipo de reemplazo son:

o **Acuerdos con proveedores:** Se establecen acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.

o **Inventario de equipos:** Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa (el sitio alterno).

o **Equipo Compatible Existente:** Equipo existente en sitios alternativos.

– Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación.

– Almacenar un equipo sin usar es costoso, pero permite que la recuperación comience más rápidamente.

– Considerar la posibilidad de un desastre extendido que requiere reemplazos masivos de equipos y retrasos del transporte.

– Mantener listas detalladas de necesidades de equipo y especificaciones dentro del plan de contingencia.

- **Recursos de Contingencia Generales**

  - Router (Proveído por el proveedor de Internet y WAN).
  - Servidores y Equipos de Comunicación (Switchs, Antenas, Fibra, etc.).
  - Gabinete de Comunicaciones y Servidores.
  - Materiales Y herramientas para cableado Estructurado.
  - UPS y Equipos de aire acondicionado.
  - Backup de los Sistemas.
  - Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.

- **Infraestructura del Ambiente Alterno PROPIO.**

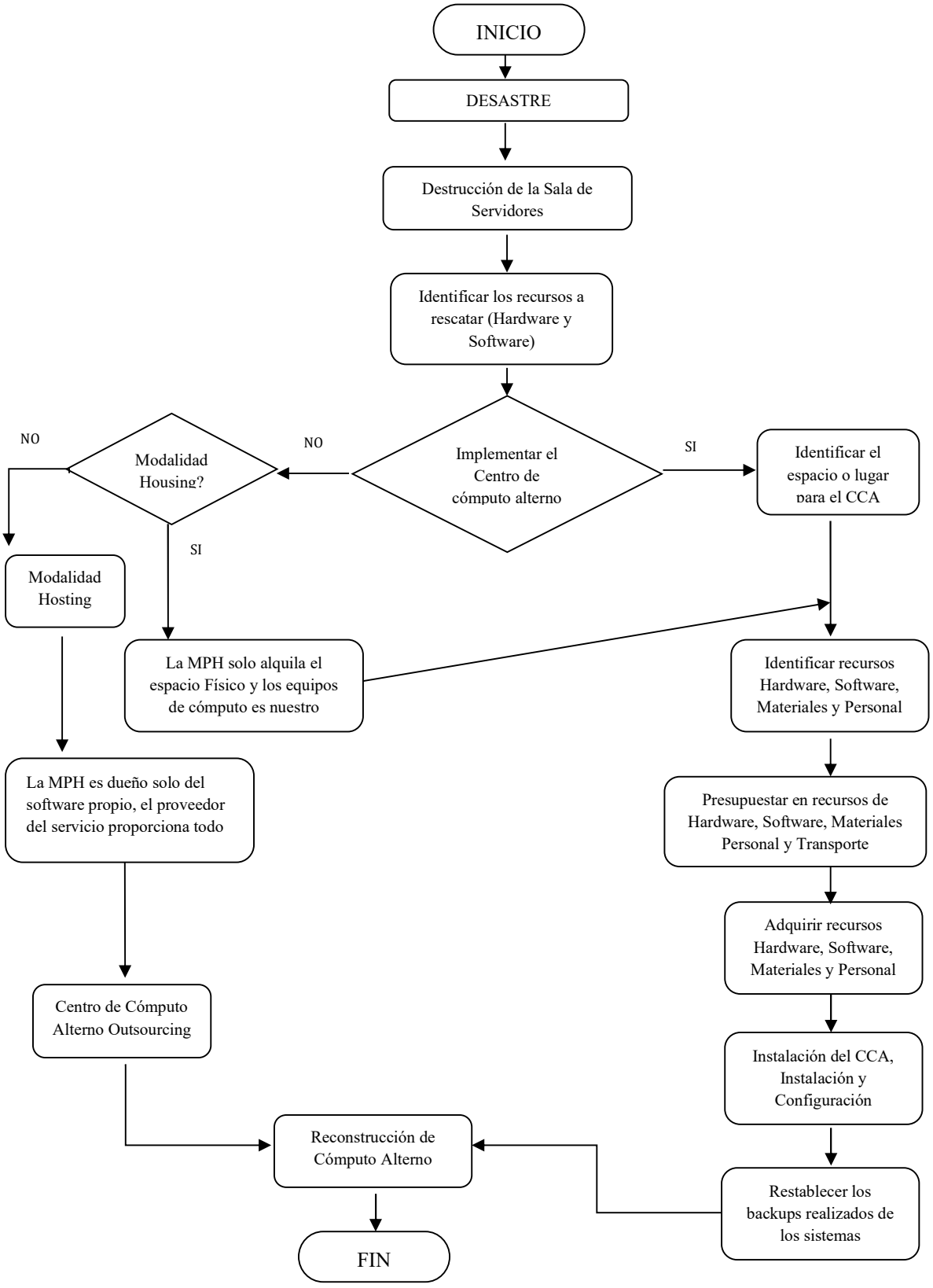
  Para este escenario, se requiere acondicionar un ambiente alterno que pueda ser utilizado como sala de servidores en el momento de la contingencia. Con un espacio de aproximadamente 15 m2 que tiene forma rectangular para facilitar la ubicación de los equipos y mobiliario.

  El ambiente alterno contará con los siguientes recursos:

  · 3 mesas para monitores y teclados de los 8 servidores principales
  · 3 sillas
  · 3 Switches 24 Ports (10/100)
  · 1 Router para la conexión a internet
  · 1 UPS
  · 1 Teléfono
  · 1 Extinguidor Clase A (Gas Carbónico)
  · Útiles de Oficina

C) Procedimientos

RESTAURACIÓN DE LA SALA DE SERVIDORES O CENTRO DE CÓMPUTO ALTERNO (CCA)



2.10. ACTIVIDADES DESPUÉS DEL DESASTRE

2.4.1 Evaluación de daños

Inmediatamente después que el siniestro haya concluido, el personal de la SGTIC realizara una evaluación de los bienes materiales, equipos y Sistemas de Información que se hayan visto afectados por el siniestro, indicando cuales pueden ser recuperados y en cuanto tiempo.

2.4.2 Priorización de actividades del Plan de Acción

Las oficinas involucradas en el Plan de Contingencia de acuerdo al ámbito de su competencia, previa evaluación de los siniestros priorizan las actividades correspondientes, a fin de habilitar los ambientes y poner en funcionamiento en el término perentorio los equipos, sistemas operativos y sistemas de aplicación de la institución. En materia de informática se dará prioridad a las actividades estratégicas y urgentes las cuales pueden ser:

- Habilitación de servidores si fuera el caso que estén dañados.
- Restauración del último BACKUP de datos de los Sistemas en producción.
- Reinstalación de los Sistemas de Información de acuerdo al cuadro de prioridades.
- Reinstalación de Sistemas Operativos y Software Base en los terminales que se encuentren operativos en ese momento, si es que presentasen problemas.
- Puesta en marcha del respaldo alternativo (BACKUP).

A continuación se detalla un cuadro de acciones correctivas a tomar después del desastre:

Acciones Correctivas a tomar después del desastre			
Equipo Informático Afectado	**Acción Correctiva**	**Tiempo estimado**	**Dependencia/Área Responsables**
Equipos de Red: Hub, Switch	Se reemplaza el equipo de red	60 minutos	SGTIC
Impresoras Matriciales, inyección de tinta o laser	Reemplazo de impresora por el mismo tipo o utilizar impresora de Red	20 minutos	SGTIC
Equipos de comunicación: Router	Reemplazo del mismo	20 minutos	SGTIC
Computadoras Personales	Se reemplaza con equipos disponible	40 minutos	SGTIC

	en el stock de equipos Informáticos.		
Servidor Base de Datos, Servidor Web, Servidor de aplicaciones, servicio de Internet	Puesta en marcha de servidor de contingencia Se realizan acciones de reinstalación y configuración. Se reinstala y reconfigura el servidor DNS.	8 horas	SGTIC Empresa Proveedora de Internet

2.4.3 Ejecución de actividades

La ejecución de actividades implica la creación de equipos de trabajo, en el momento de la contingencia, para realizar las actividades previamente planificadas en el Plan de Acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación a la Jefatura a cargo del Plan de Contingencias. El Gerente, Sub Gerente o Jefe a cargo del Plan de Contingencias debe orientar las actividades diferenciando dos etapas: Restauración del Servicio usando los recursos de la MUNICIPALIDAD PROVINCIAL DE HUANCAYO, volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información.

2.4.4 Evaluación de Resultados

La realización de este punto permitirá tener un registro para llevar un archivo histórico de las contingencias. De la evaluación de resultados y del siniestro en sí, deberían de salir dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

2.4.5 Retroalimentación del Plan.

El plan de Contingencias es un documento de gestión de Gerencia de Sistemas de Información y Planeamiento, teniendo la característica de tener contenidos que cambian en el tiempo, vale decir que van acorde con las emergencias que se podrían suscitar y con los cambios tecnológicos de los equipos informáticos, y cuya información tendrá que incorporarse al documento en el marco de una retroalimentación constante, garantizando la vigencia y utilidad de este plan.

2.11. PLAN DE VERIFICACION Y PLAN DE PRUEBAS

Tres medidas de minimizar los riesgos de la tecnología son la:

- Verificación
- Prueba
- Mantenimiento de los sistemas.

Cada componente de un sistema de cómputo equipo, comunicaciones y programas debe ser verificado y probado rigurosamente antes de utilizarlo para un evento.

2.5.1 Plan de Verificación

Para el Plan de Contingencia es muy importante y es conveniente que una autoridad independiente aplique las pruebas de verificación. Para sistemas de menor importancia, la verificación puede realizarse internamente. Las pruebas de verificación (también conocidas como pruebas de calidad) pueden incluir:

- Probar los equipos bajo condiciones que simulen las de operación real.
- Probar los programas para asegurar que se siguen los estándares apropiados y que desempeñan las funciones esperadas.
- Asegurar que la documentación sea la adecuada y esté completa.
- Asegurar que los sistemas de comunicación se ciñan a los estándares establecidos y funcionen de manera efectiva.
- Verificar que los sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.
- Asegurar que se cuente con las debidas medidas de seguridad y que estas se ciñan a las normas establecidas.

2.5.2 Procedimientos para las Pruebas del Plan de Contingencia

Introducción

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la Institución.

Las pruebas se efectúan simultáneamente a través de múltiples unidades, incluyendo entidades externas.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

Objetivos

- El objetivo principal, es determinar si el Plan de contingencia es capaz de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la Municipalidad, probando la efectividad de los procedimientos expuestos en el plan de contingencias.
- Las pruebas permiten efectuar una valoración detallada de los costos de operación en el momento de ocurrencia de una contingencia.

Niveles de Prueba

Se recomiendan dos niveles de prueba:

- Pruebas en pequeñas Unidades Orgánicas.
- Pruebas en a nivel Gerencial.

La premisa es comenzar la prueba en las Unidades Orgánicas más pequeñas, extendiendo el alcance a nivel Gerencial, para finalmente realizar las pruebas entre sedes o con otras instituciones externas.

Métodos para Realizar Pruebas de Planes de Contingencia

a) Prueba Específica

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencia. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

b) Prueba de Escritorio

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios).

Características:

- La discusión se basa en un formato preestablecido.
- Está dirigido al equipo de recuperación de contingencias.
- Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad.

Los ejercicios de escritorio son ejecutados por el encargado de la prueba y el personal responsable de poner el plan de contingencias en ejecución, en una situación hipotética de contingencia. Un conjunto de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a

cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

c) Simulación en Tiempo Real

Las pruebas de simulación real, en una Unidad Orgánica, a nivel de Gerencia en la Municipalidad está dirigida a una situación de contingencia por un período de tiempo definido.

- Las pruebas se hacen en tiempo real.
- Son usadas para probar partes específicas del plan.
- Permiten probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

Preparaciones PRE Prueba

- Repasar el plan de contingencia.
- Verificar si se han asignado las respectivas responsabilidades.
- Verificar que el plan este aprobado por la alta dirección de la institución.
- Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
- Establecer la fecha y hora para la ejecución de la prueba.
- Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
- No dejar de lado los resultados obtenidos, la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.
- La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y restableciendo a la normalidad las actividades realizadas.
- Enfocar los procesos críticos que dependen de sistemas específicos o compañías externas donde se asume que hay problemas.
- Definir el ambiente donde se realizarán las reuniones del equipo de recuperación de contingencias.
- Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

Comprobación de Plan de Contingencias

La prueba final debe ser una prueba integrada que involucre secciones múltiples instituciones externas. La capacidad funcional del plan de contingencia radica en el hecho de que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

El diagrama representa los pasos necesarios, para la ejecución de las pruebas del plan de contingencias.