UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMÁTICOS

“ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA EL CENTRO DE CÓMPUTO DE UN ISP”

AUTOR:

Israel Rubén Bermeo Castillo

TUTOR:

Ing. Mario Mejía

Quito - Ecuador

2013

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Graduación certifico:

Que el Trabajo de Graduación **"ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA EL CENTRO DE CÓMPUTO DE UN ISP",** presentado por Israel Rubén Bermeo Castillo, estudiante de la carrera de Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, Enero 2013

TUTOR

Ing. Mario Mejía

C.C. 170658885-0

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE TESIS

El abajo firmante, en calidad de estudiante de la Carrera de Sistemas Informáticos declaro que los contenidos de este Trabajo de Graduación, requisito previo a la obtención del Grado de Ingeniero en Sistemas Informáticos, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito, Enero del 2013

Israel Rubén Bermeo Castillo

C.C. No. 010450905-4

DEDICATORIA.

Este proyecto está dedicado a mi madre por el esfuerzo realizado para que pueda alcanzar este logro en mi vida, por estar siempre pendiente y brindarme su apoyo incondicional para cumplir cada una de las metas propuestas a lo largo de mi vida; de igual manera se lo dedico a cada uno de mis familiares.

AGRADECIMIENTO.

A Dios por haberme brindado la capacidad de seguir adelante y rodearme de excelentes personas las cuales aprecio demasiado. A mi madre la Sra. Nancy Castillo, la cual con sus enseñanzas, consejos, apoyo, paciencia, y sobre todo ese inmenso amor incondicional que me brinda día tras día, por esa fortaleza y el don de gente con el cual me encamino a ser una persona de bien.

A mi hermana que con sus muestras de afecto e incentivo me ayuda a continuar, a mis familiares que son un pilar fundamental en mi vida, cada uno de ellos con su forma de ser y apoyo a su manera mil gracias. Un agradecimiento muy especial a cada uno de los docentes de la Universidad que me han brindado sus conocimientos y apoyado desde mi ingreso a la institución.

A cada uno de mis compañeros, amigos que de una u otra manera se inmiscuyeron a lo largo de este proceso y por ultimo y no menos importante a ti A. Jota por el apoyo, paciencia, preocupación y constancia.

Israel R. Bermeo Castillo.

Resumen

En la actualidad con el avance de la tecnología y su continuo cambio cada vez va adquiriendo mayor importancia dentro de las organizaciones, así como también es de gran importancia el cuidado de la integridad de os recursos humanos, por tal motivo es de suma importancia contar con un plan de contingencia adecuado que garantice un correcto funcionamiento y de igual manera el restablecimiento de las funcionalidades de los servicios en el menor tiempo posible, ante cualquier eventualidad.

Se considera que los activos de la institución representan un elemento clave para brindar servicios y del mismo modo la información de una organización es el activo mas valioso que posee, por lo tanto es necesario el desarrollo de lineamientos y procedimientos que garanticen la continuidad y disponibilidad del servicio ante cualquier incidente.

Esto implica el incremento de la efectividad, eficiencia y productividad del personal para proveer un servicio continuo y eficaz.

El plan de contingencias implica un análisis exhautivo de los posibles riesgos a los cuales puede estar expuesto un centro de computo y la información contenida en los diversos dispositivos de almacenamiento, por tal motivo es importante que el Plan de Contingencias posea un plan de recuperación, el cual tendrá como objetivo primordial restaurar el servicio de computo de forma rápida, eficiente y con el menor costo y perdidas posibles.

Un daño puede presentarse de distintas maneras por lo tanto es necesario asumir que el daño fue total, esto con la finalidad de poseer un Plan de Contingencias lo mas integro posible. Pese a todas las medidas de seguridad tomadas se pueden presentar desastres que no son evitables.

El presente documento posee un conjunto de recomendaciones generales para el diseño y elaboración de un Plan de Contingencia para un centro de cómputo, el cual puede ser un repositorio centralizado de información, procedimientos y tareas que pueden ayudar en la toma de decisiones al personal administrativo, de igual manera para el desarrollo de procesos y definición de tiempos de respuesta ante cualquier interrupción de las operaciones y servicios de la institución.

Summary

Today with the advancement of technology and changing each time becomes more important within organizations as well as of great importance is the care of the integrity of human will, for this reason it is very important to have adequate contingency plans to ensure proper operation and likewise restore the functionality of the services in the shortest possible time, for any eventuality.

It is considered that the assets of the institution represent a key element in providing services and information just as an organization is the most valuable asset you have, so it is necessary to develop guidelines and procedures to ensure continuity and availability service to any incident.

This involves increasing the effectiveness, efficiency and productivity to provide a continuous and effective.

The contingency plan involves an analysis of the potential exhaustive risks they may be exposed to a computer center and the information contained in the various storage devices, for this reason it is important that the contingency plan has a recovery plan, the which will have as its primary objective of computing restore service quickly, efficiently and at the lowest possible cost and lost.

An injury can occur in different ways so it is necessary to assume that the damage was total, this in order to have a contingency plan as more honest as possible. Despite all the security measures that may occur are avoidable disasters.

This document has a set of recommendations for the design and development of a contingency plan for a computer center, which can be a centralized repository of

information, tasks and procedures that can help in the decision making of administrative staff, similarly for process development and definition of response times to any disruption of operations and services of the institution.

Tabla de Contenido

Tabla de Graficos

Tabla de Anexos

1. INTRODUCCIÓN

Un plan de contingencia informático implica un extenso análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y sistemas de información. De tal manera que corresponde al centro de informática y telecomunicaciones tomar las medidas de seguridad correspondientes para salvaguardar, proteger y estar preparados para afrontar desastres o problemas de diversos tipos.

El plan de contingencia mantiene una estrecha relación con la infraestructura informática, así como los procedimientos relevantes asociada con la plataforma tecnológica. La infraestructura informática está conformada por el hardware, software y todo lo que le complementan a los procedimientos relevantes, soporte y transmisión de datos que permiten la funcionalidad del negocio.

Los procedimientos relevantes a la infraestructura informática, son todas aquellas tareas que realiza el personal con frecuencia al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, entre otros.).

Un plan de contingencia está diseñado para brindar un adecuado sistema de seguridad lógica y física en lo que refiere en previsión de desastres, del mismo modo se establecen medidas orientadas a salvaguardar la información contra los daños que puedan ser ocasionados por el hombre o la naturaleza.

De tal manera que la información siendo uno de los bienes más importantes de la organización, al igual que la continuidad del servicio brindado a los clientes son los fundamentos primordiales a tomar en cuenta en un plan de contingencia.

Al existir un peligro latente de desastres, a pesar de todas las medidas de seguridad, es necesario que el plan de contingencia informático contenga un plan de recuperación de desastres con el objetivo de restaurar el servicio informático en forma rápida, eficiente, con la menor inversión monetaria posible y garantizar la integridad de la información.

La investigación a realizar brindará una amplia recolección de las mejores prácticas para mejorar y proteger el funcionamiento de un centro de cómputo al momento de que se presente una contingencia que pueda afectar al centro de cómputo.

1.1 Antecedentes

Con el tiempo las empresas se han vuelto más dependiente de los computadores y redes para el manejo de sus actividades, la alta disponibilidad de los sistemas informáticos se han vuelto de vital importancia en las empresas.

Actualmente, gran mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

En un estudio realizado por la Universidad de Minnesota, quedo comprobado que más del 60% de las empresas que sufren un desastre y que no poseen un plan de recuperación ya implementado, saldrían del negocio en un plazo no mayor a 3 años. A medida que vaya aumentando la dependencia de la disponibilidad de los recursos informáticos, este porcentaje seguramente crecerá.

Por lo tanto, la capacidad para recuperarse exitosamente de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan estratégico de seguridad para una organización.

1.2 Formulación del Problema

¿Cuándo se instala o mejora un centro de cómputo del ISP se salvaguarda la información y mantiene el servicio a los usuarios?

1.3 Sistematización

1.3.1 Diagnostico

	DIAGRAMA DE PARETO			
Causa	**Frecuencia**	**% Acumulado**		**80-20**
Servicios prestados	23	45%	23	80%
Instalación eléctrica	8	61%	31	80%
Seguridades	7	75%	38	80%
Hardware	7	88%	45	80%
Software	3	94%	48	80%
Aire acondicionado	2	98%	50	80%
Instalación física	1	100%	51	80%

Grafico 1: Tabla de pareto de los errores del ISP

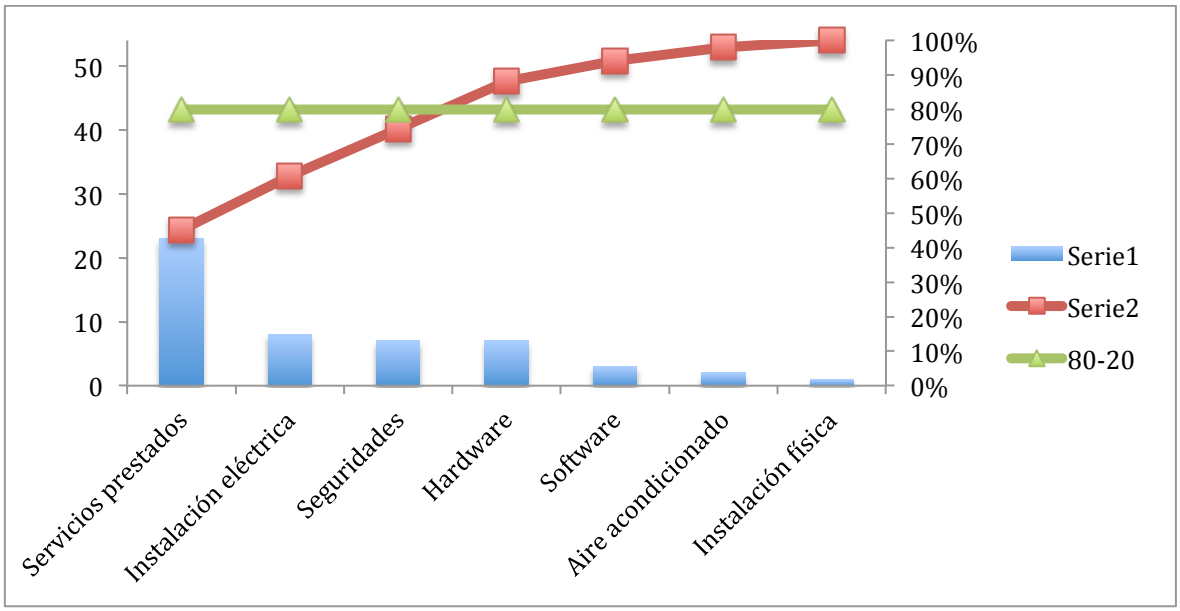


Grafico 2: Gráfico de Barras que representa el efecto de cada uno de los elementos contribuyentes

Procesos actuales del centro de cómputo del ISP

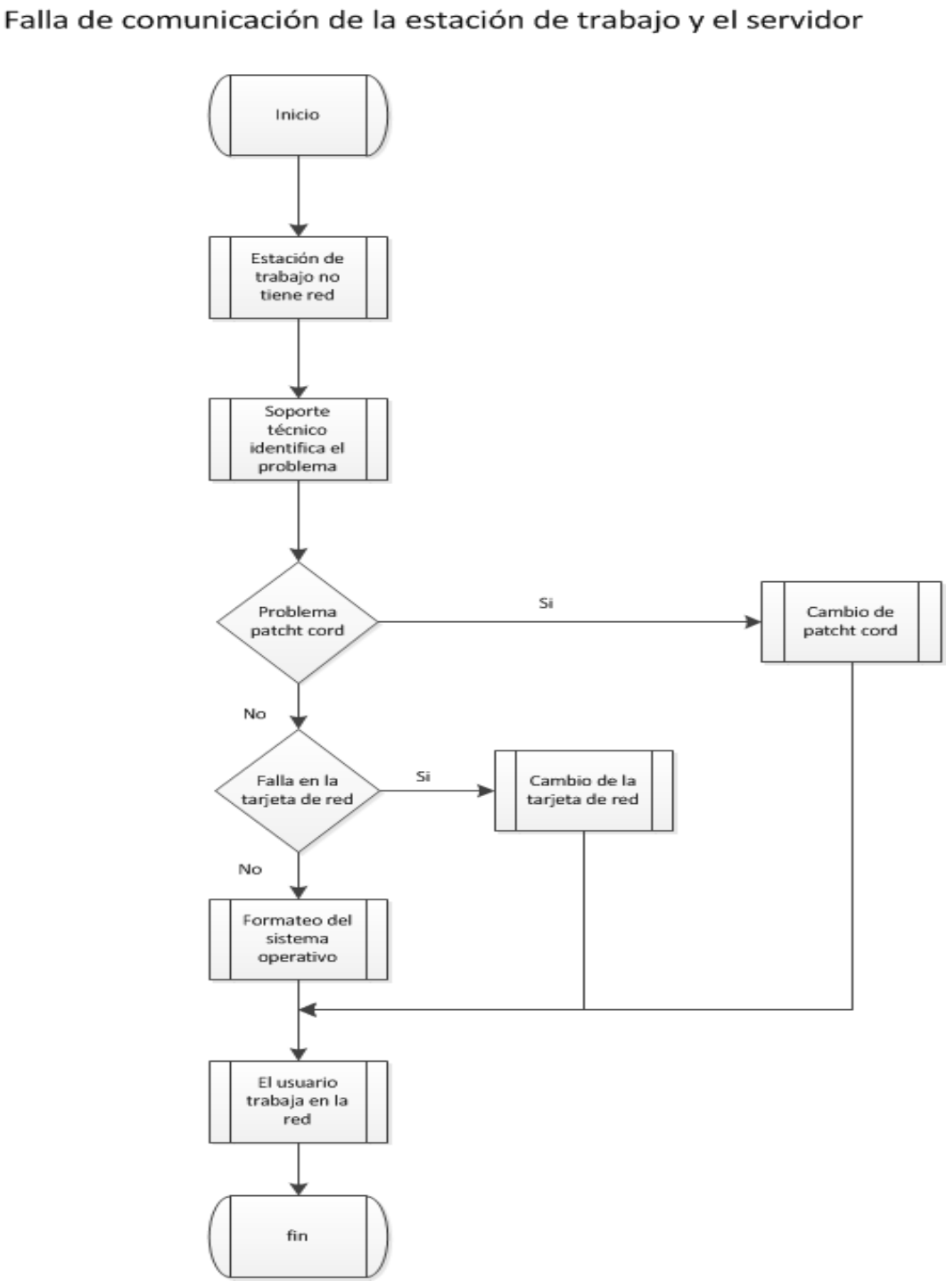


Grafico 3: Proceso actual para la recuperacion de la comunicación cliente servidor

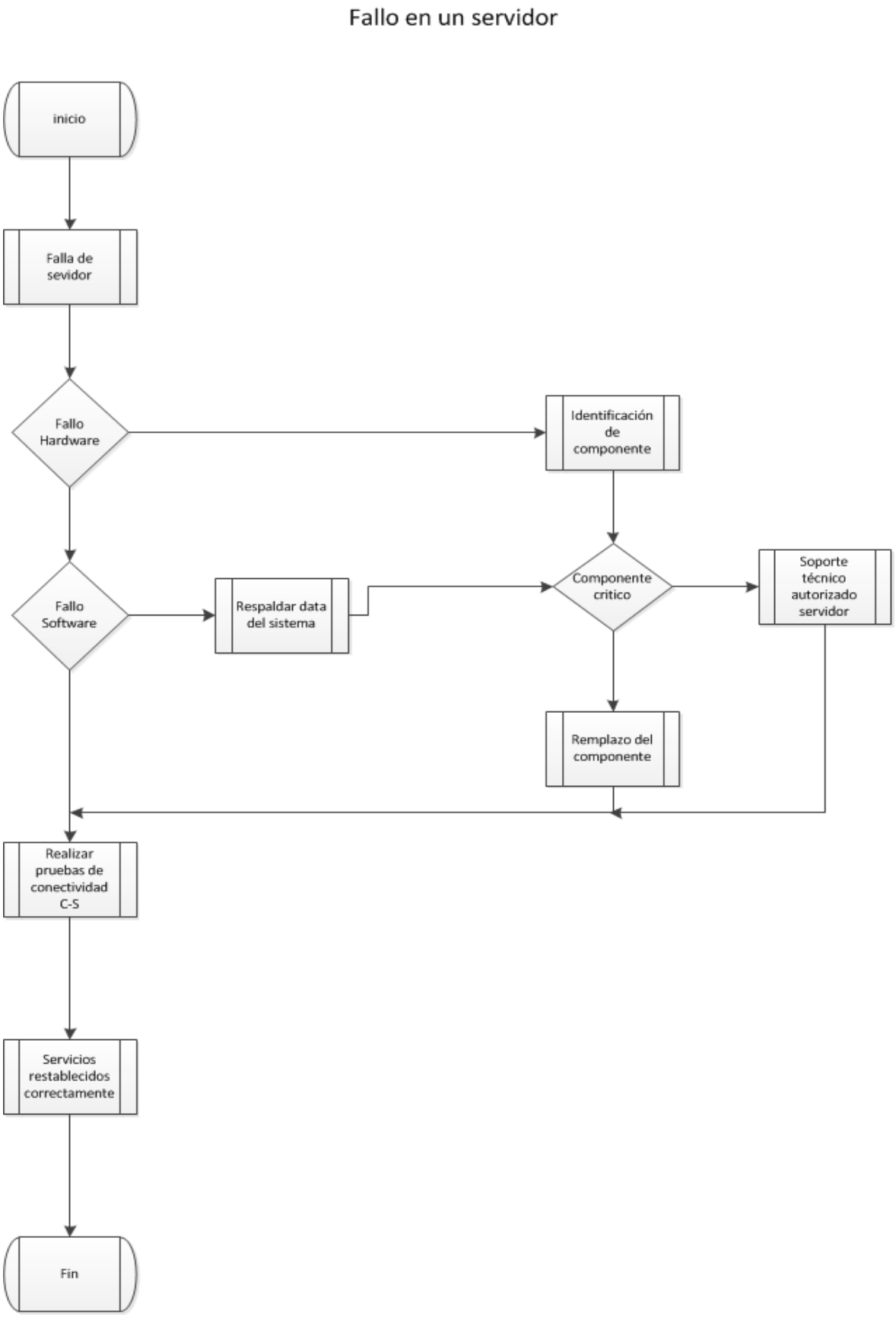


Grafico 4: Proceso actual para solucionar falla en el servidor

La carencia de un plan de contingencia adecuado que garantice el continuo funcionamiento del servicio en el ISP.

Falta de procesos adecuados para brindar disponibilidad del centro de cómputo y el servicio en el ISP.

1.3.2 Pronóstico

Al no poseer un plan de contingencia que garantice el servicio en el ISP, se pueden presentar inconvenientes al momento de que un inconveniente se haga efectivo, de tal manera que las operaciones que brinda el centro de cómputo y el ISP en si pueden verse afectadas es decir que el servicio brindado a los usuarios puede reflejar algún problema.

1.3.3 Control del Pronóstico

La Implementación de un centro de cómputo con alta disponibilidad facilitaría y garantizaría el funcionamiento y la continuidad del negocio en un 99%.

La capacitación al personal de cómo debería reaccionar al momento de una tragedia es de suma importancia, con esto se garantizaría la integridad del servicio y de las personas.

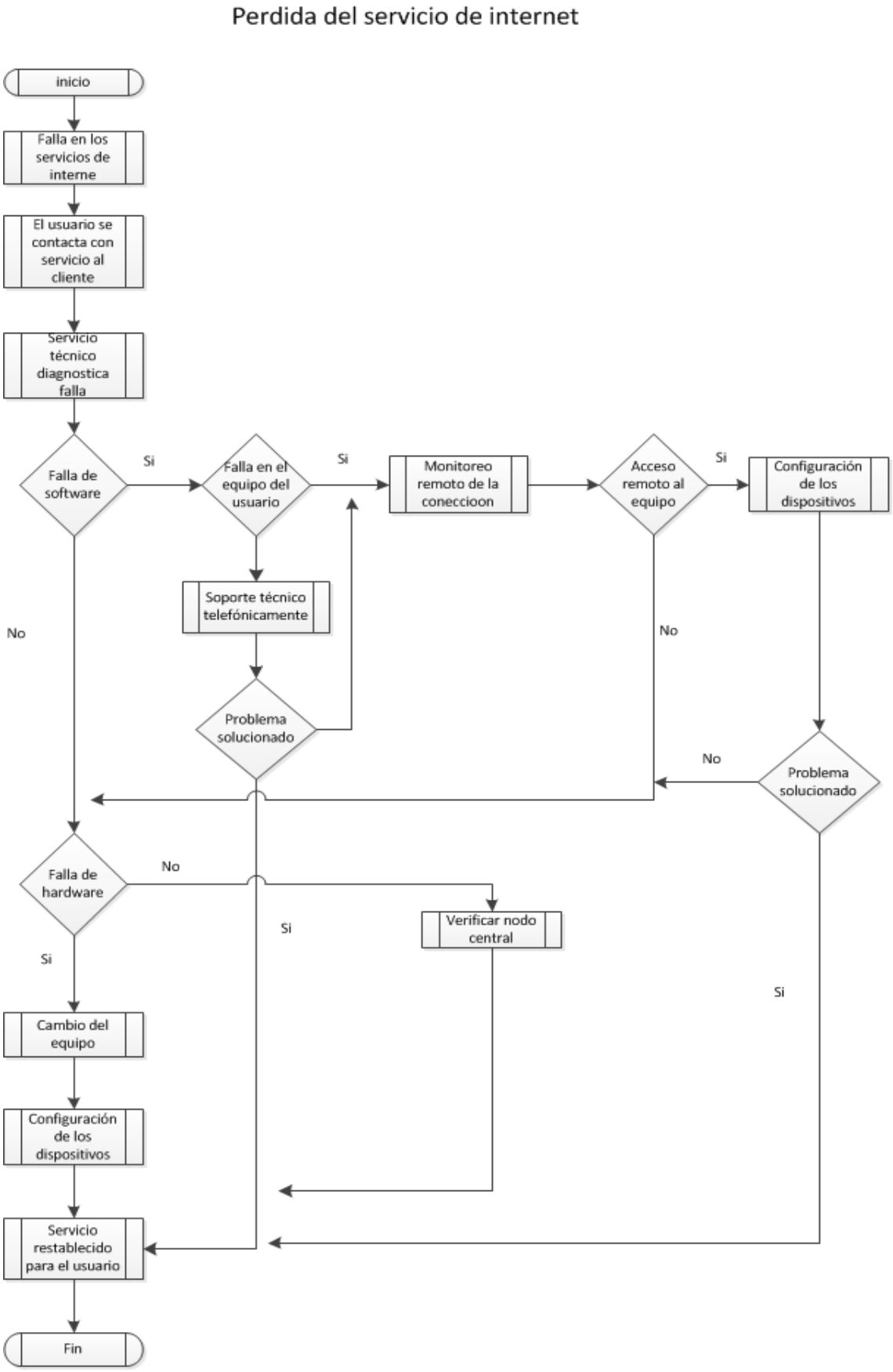


Grafico 5: Proceso diseñado para la recuperacin del servicio de internet.

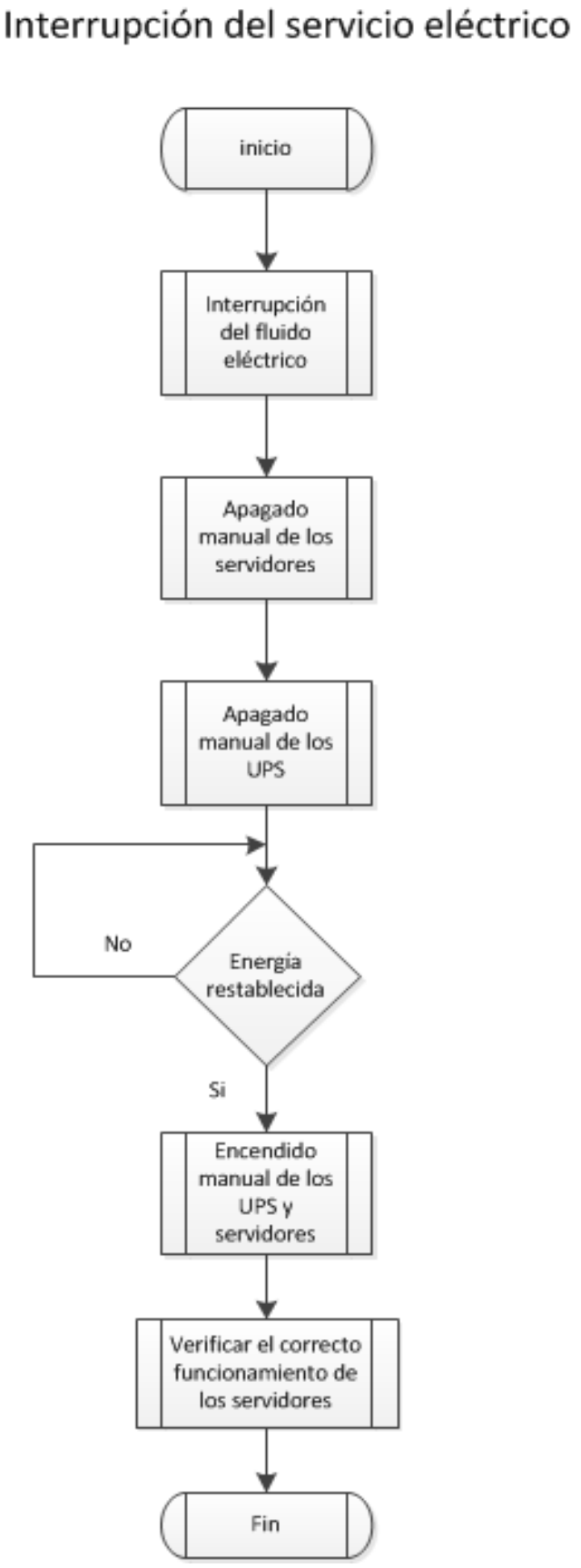


Grafico 6: Proceso diseñado para la recuperacin del servicio eléctrico.

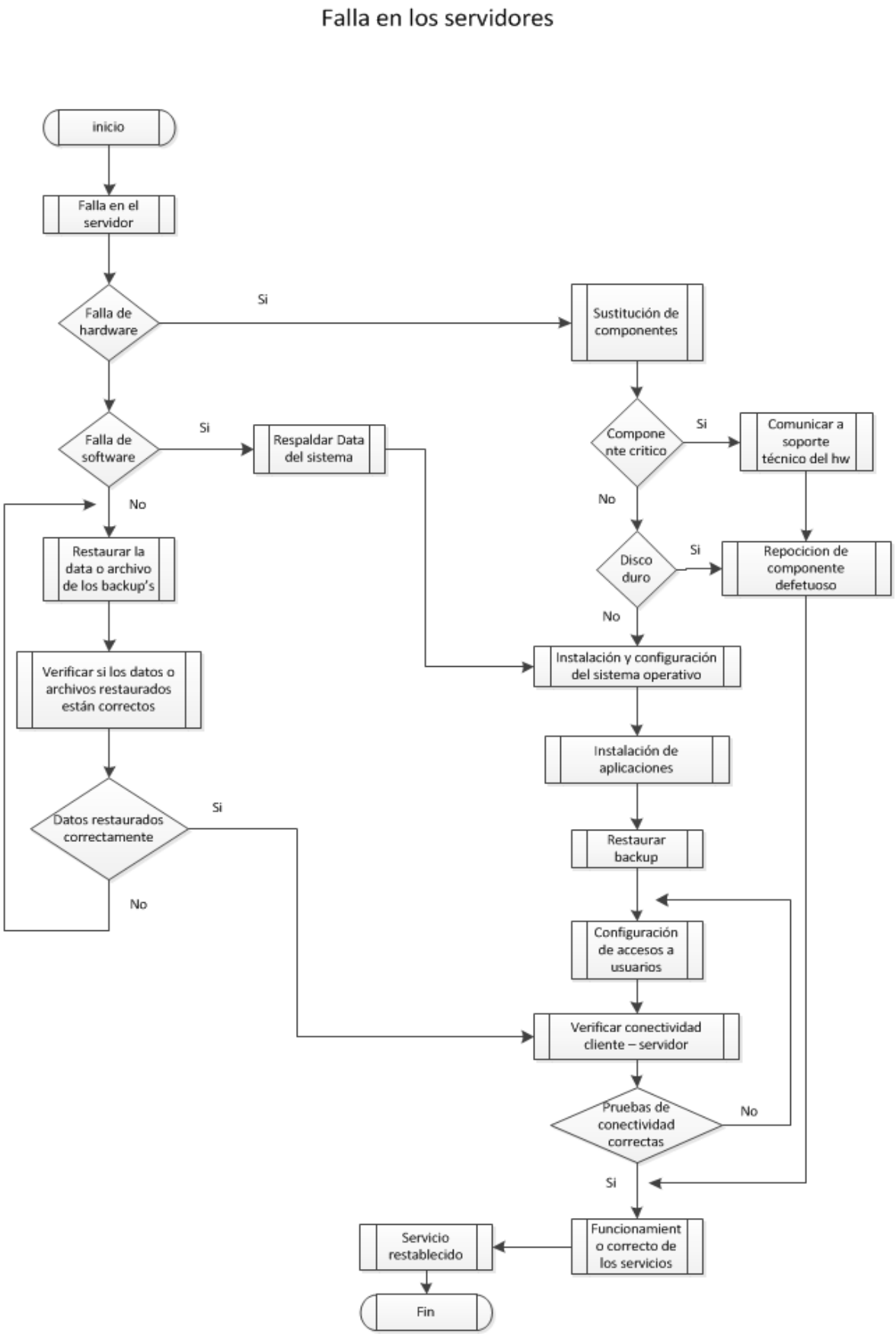


Grafico 7: Proceso diseñado para la recuperacin de los servidores.

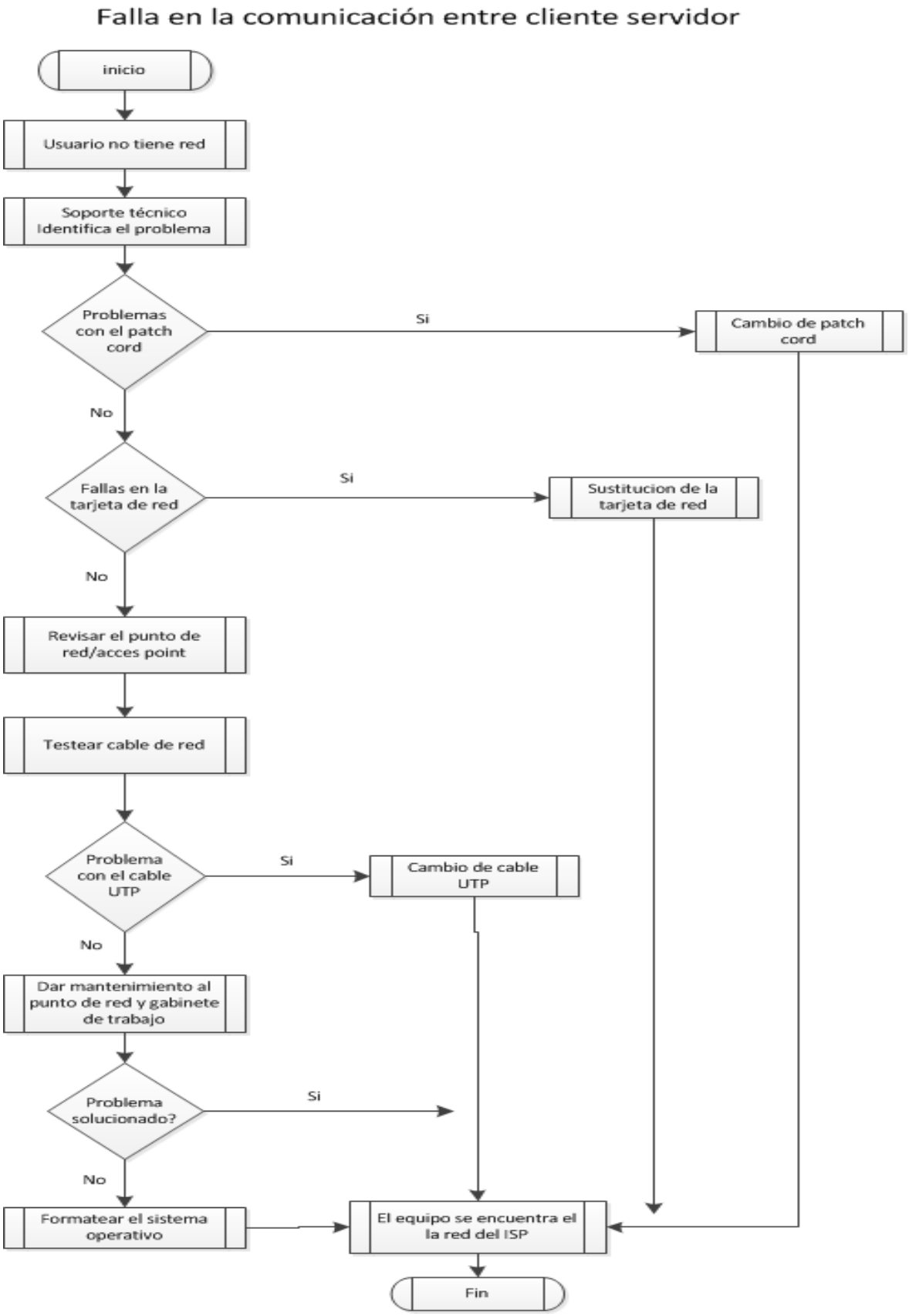


Grafico 8: Proceso diseñado para la recuperacin de la comunicación cliente servidor.

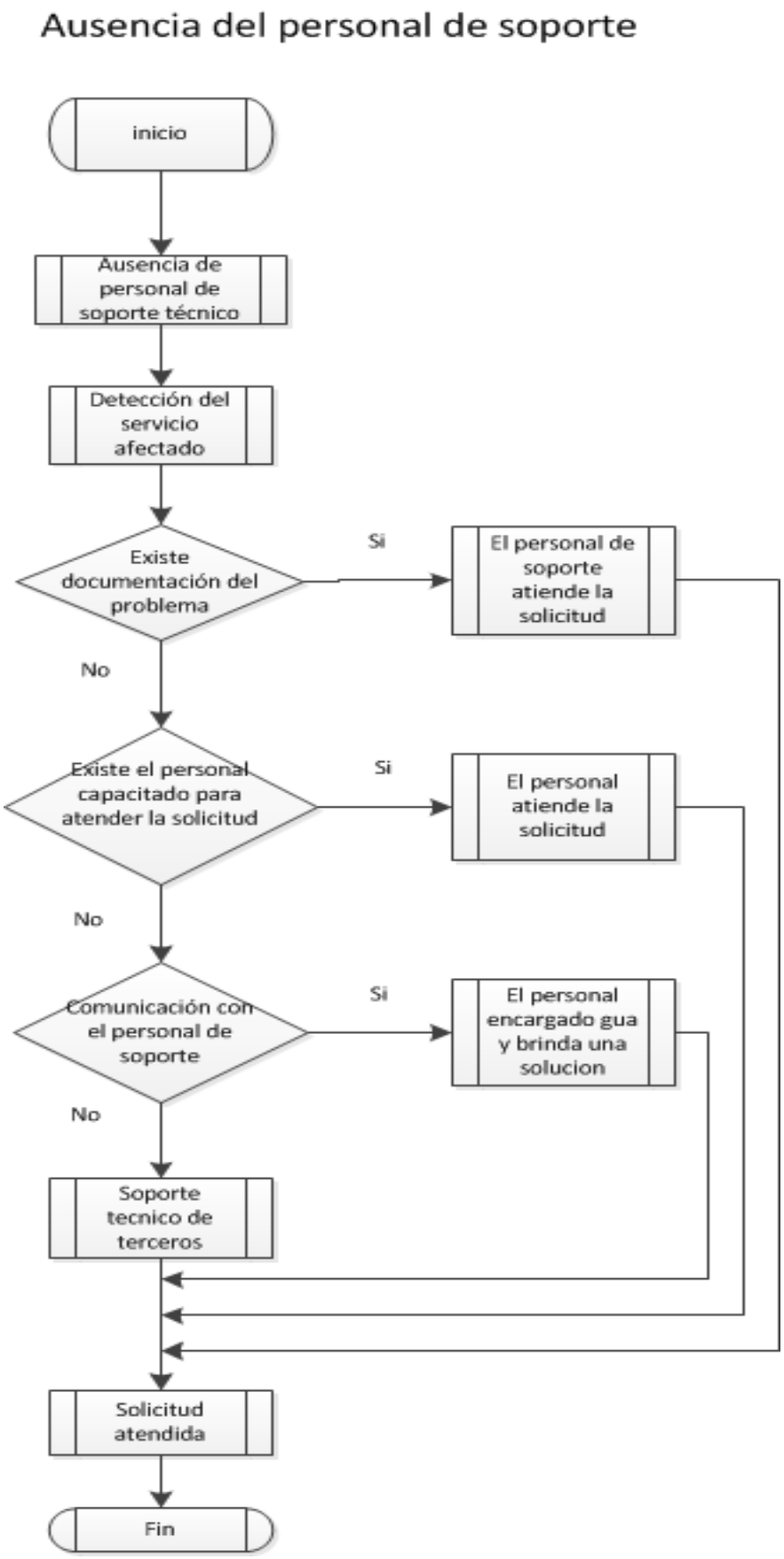


Grafico 9: Proceso diseñado para solucionar la ausencia de personal

1.4 Objetivos

1.4.1 Objetivo General

Elaborar un documento contenedor de las mejores prácticas de un plan de contingencia para el centro de cómputo de un ISP.

1.4.2 Objetivos Específicos

- Generar una guía que brinde las mejores prácticas para garantizar el continuo funcionamiento de las operaciones de los elementos considerados críticos que componen los sistemas de información.
- Definir acciones a realizar en un momento de contingencia para salvaguardar la integridad de la información y las personas.
- Establecer los procedimientos a ejecutar en caso de fallas de los elementos que componen un sistema de información.

1.5 Justificación

La información es uno de los recursos de un valor incalculable, al igual que los otros activos de una institución por lo tanto al igual que todos los activos deben estar protegidos. La implementación de políticas de seguridad ayudan a evitar amenazas y riesgos que obstaculicen la productividad de la empresa, las políticas de seguridad informática son creadas con el fin de garantizar la continuidad de los sistemas de información y alcanzar las metas de la institución.

De igual manera es importante recalcar que las políticas de seguridad deben ser parte de la cultura organizacional, esto con el objetivo de cumplir con la confidencialidad, integridad y disponibilidad de la información.

La elaboración de un plan de contingencia, suministra el respaldo necesario en caso de que la política falle, esto es creado con el objetivo de restaurar el servicio informático con la menor inversión de tiempo posible y de manera eficiente, con el menor costo y pérdida posible.

1.5.1 Justificación Teórica

Este proyecto de la elaboración de un plan de contingencia, permitirá implementar buenas prácticas para la creación de un centro de computo o a su vez mejorar el mismo, aumentando el rendimiento, la disponibilidad de los servicios prestados por dicho centro.

Cabe destacar que este proyecto está orientado a salvaguardar la integridad lógica del negocio ya que en esta se encuentra la información del mismo, a su vez busca proteger la integridad física de las personas.

1.5.2 Justificación Práctica

Un contexto global, nos muestra notables y determinantes cambios en la economía, lo cual exige mayor nivel de competitividad para las empresas. Desde esta perspectiva cada organización debe implementar normas y procedimientos de calidad para alcanzar dicha competitividad, es por esto que un plan de emergencias que brinde una rápida acción al momento de una tragedia puede marcar la diferencia a nivel organizacional y de mercado.

Dicho esto el plan de contingencia debe ser de fácil accesibilidad y comprensión para los usuarios recopilando así una serie de procesos que proporcionarán un desarrollo de actividades eficaz y eficiente al momento de una contingencia, evitando así un impacto fuerte en la organización y restableciendo las operaciones en el menor tiempo posible, una vez finalizada la contingencia se procederá a realizar las actualizaciones y mejoras del plan en el caso que existieran.

1.5.3 Justificación Metodológica

Para realizar este proyecto se va ayudar de los siguientes métodos de investigación:

Investigación deductiva al ser una investigación que permite recopilar información útil para el desarrollo del proyecto, generando una guía para combatir cualquier inconveniente.

ITIL Acrónimo de (Information Technology Infraestructure Library) Biblioteca de Infraestructura de Tecnología de Información, es una normativa que recopila las mejores prácticas para administrar los servicios de Tecnología de Información (TI). Su desarrollo se da a finales de los años 80 por un conjunto de entidades públicas y privadas con el fin de recopilar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Government Commerce, que es una entidad independiente de la tesorería del gobierno británico.

1.6 Alcance y Limitaciones

1.6.1 Alcance

Este plan está orientado a la infraestructura informática, así como los procedimientos relevantes asociados con la plataforma tecnológica, dicha infraestructura está conformada por hardware, software y elementos que complementan la transmisión e información de los datos críticos para el funcionamiento de la empresa.

El personal de la empresa puede hacer uso de las mejores prácticas para reaccionar al momento de una eventualidad de tal manera que los servicios sean restablecidos en el menor tiempo posible y con un bajo costo.

1.6.2 Limitaciones

El plan de contingencia obtenido de la investigación no será implementado en ninguna institución, el mismo que será tomado como guía recopilando las mejores prácticas para así diseñar una metodología acoplable para la creación de un plan de contingencia de una institución, tomando en cuenta los factores y subfactores críticos en todo ISP omitiendo así gran parte de los eventos posibles que puedan presentarse en un centro de cómputo.

1.7 Estudios de la Factibilidad

1.7.1 Técnica

Al implementar un protocolo de diseño de sistema de Alta disponibilidad se busca asegurar cierto grado absoluto de continuidad operacional durante un periodo de medición dado. La disponibilidad es la característica que brinda un servicio a los usuarios para acceder al sistema y realizar nuevas tareas: actualizar, eliminar, modificar trabajos existentes o tan solo para consultar información, Si un usuario no tiene acceso al servicio se dice que el mismo no está disponible, el termino downtime o tiempo de inactividad es el término usado para definir que el sistema no está disponible.

La implementación de un plan de contingencia permite restablecer el servicio en el caso de que un desastre se haga presente.

1.7.2 Operativa

El plan de contingencia proveerá de una alta disponibilidad de información para la organización, a su vez proporcionará una guía de procedimientos y protocolos a realizar en caso de que se efectúe algún inconveniente o desastre, al mismo tiempo que se presentará un Plan de Post-Contingencia.

2. MARCO DE REFERENCIAS

2.1 Marco Teórico

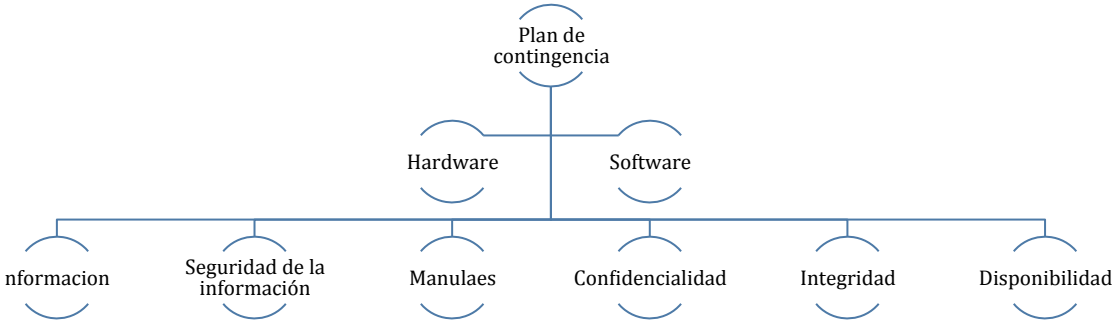


Grafico 10: Mapa conceptual de los tópicos principales a tratar.

2.2 Marco Conceptual

Plan de contingencia: "Un Plan de contingencias es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño (delivery and support, véase ITIL).

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante."[1]

ITIL: "Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un conjunto

[1]http://es.wikipedia.org/wiki/Plan_de_Contingencias

de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI."[2]

Hardware: Es el conjunto de elementos tangibles en un sistema integral de cómputo o CTI(Central de Tecnologías de Información.). Bajo esta terminología se incluyen la computadora como los diversos periféricos: impresoras, discos, tarjetas, etc. Esto es el primer elemento de un sistema de cómputo y comprende toda la maquinaria y equipos relacionados con el mismo.

Software: Es la parte intangible, es decir es el conjunto de instrucciones que son procesadas por la máquina para resolver un problema dado. Bajo este concepto se incluye al conjunto de instrucciones agrupadas en rutinas y programas, junto con la documentación respectiva que indican cómo resolver problemas de naturaleza diversa en una computadora.

Información: Es toda comunicación o representación de conocimiento como datos, en cualquier forma, con exclusión de forma textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

La seguridad informática: "Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información

[2]http://es.wikipedia.org/wiki/ITIL

contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable."[3]

Confidencialidad: Permite el acceso a la información solo a las personas autorizadas a la misma.

Integridad: Mantiene la información y procesos totalmente protegidos.

Disponibilidad: "El factor de disponibilidad de un equipo o sistema es una medida que nos indica cuanto tiempo está ese equipo o sistema operativo respecto de la duración total durante la que se hubiese deseado que funcionase. Típicamente se expresa en porcentaje. No debe de ser confundida con la rapidez de respuesta."[4]

Autenticidad: Asegura la validez de la información en distribución, forma y tiempo, garantiza el origen de la información, validando el emisor evitando así la suplantación de identidad.

---

[3]http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
[4]http://es.wikipedia.org/wiki/Disponibilidad

Confiabilidad de la Información: verifica que la información generada provenga de una fuente confiable para sustentar la toma de decisiones, ejecución y funciones.

Política de seguridad: "Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero.

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad.

Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos (véase referencias más adelante). Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera."[5]

Contingencia: "Es una eventualidad (un evento que ocurre en un momento cualquiera) y que puede haber sido provocada o no, puede ser la consecuencia de acciones o ser totalmente imprevista. La contingencia puede ser o no un evento que ocasiona un problema el cual puede requerir una acción postergable o una acción inmediata (transformándose en este último caso en una emergencia). Desde el momento en que una contingencia puede ser

[5]http://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad

imprevista, se habla de la posibilidad de que ocurra, más la contingencia no es en sí misma una posibilidad, sino un evento posible."[6]

2.3 Marco Legal

El marco legal en este caso no se aplica, porque el mismo no se sustenta en una normativa legal en nuestro país.

2.4 Marco Espacial

La investigación realizada en la empresa de telecomunicaciones "Puntonet" ubicada en el cantón Cuenca provincia del Azuay en las calles Remigio Crespo y Guayas (esq.) en el edificio San José, tercer piso; teniendo esta la sede matriz en la ciudad de Quito.

El plan de contingencia a ser desarrollado tomara datos reales de la sede cuenca.

La empresa brinda servicio de internet a 317 clientes corporativos y 2017 clientes residenciales distribuidos en todo el cantón, llegando a los mismo por distintos medios como so ADSL, WIFI, Fibra óptica, entre otros.

El centro de computo consta con los siguientes elementos:

Servidores:

- Proxy
- FTP
- Aplicaciones
- Fetchmail
- MySql
- Squid

[6]http://es.wikipedia.org/wiki/Contingencia

Instalación física:

- Rack de piso servidores
- Rack de piso switchs
- Rack de piso olt
- Rack de pared red interna y telefonía (internet y datos)
- Instalación de voz ip
- Telefonía convencional

Seguridad en la red:

- Firewall
- Autenticación por Mac
- Direcciones Ip estáticas
- SSID no difundidos en parte inalámbrica
- Registro de Log

Servicios que presta el ISP:

- Internet
- Correo electrónico
- Hosting
- Voz sobre IP
- Transmision de Datos
- Sistemas Satelitales
- Camaras IP

Los servidores se encuentran monitoreados y administrados por dos personas.

El NEGOCIO

La permanente evolución tecnológica en la que nos hallamos inmersos, hace que el mercado de las Telecomunicaciones constituya actualmente un factor diferenciador de éxito para las Empresas, es así como PuntoNet continuamente desarrolla nuevas soluciones de conectividad acordes a la demanda nacional, así como la inclusión de servicios multiplay, lo que en ámbito mundial de las Telecomunicaciones se encuentran en pleno auge.

Estamos seguros que contamos con la RED FISICA MAS ROBUSTA Y A PRUEBA DEL FUTURO del país, la cual es administrada por personal técnico certificado de primer nivel, lo que nos permite contar con un amplio portafolio de productos diseñados para soportar las necesidades de conectividad de hoy y del mañana.

3. METODOLOGÍA

3.1. Proceso de Investigación

3.1.1. Unidad de Análisis

El tema está dirigido a los jefes departamentales de tecnología, los mismos que tomaran esto como guía para mejorar o implementar su plan de contingencia. Aplicando ITIL ya que es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de buena calidad.

3.1.2. Tipo de Investigación

Para el desarrollo del proyecto se empleará la investigación documental y la explicativa.

La Investigación documental es aquella que como su nombre lo indica, parte del análisis de documentos, entendiendo a éste como toda realización humana que como prueba de su acción, puede revelar los conocimientos, las formas de pensar y de vivir de un grupo, comunidad o sociedad en un determinado contexto histórico-geográfico.

Investigación explicativa es aquella que tiene relación causal; no sólo persigue describir o acercarse a un problema, sino que intenta encontrar las causas del mismo. Existen diseños experimentales y NO experiméntales, desde un punto de vista estructural reconocemos cuatro elementos presentes en toda investigación: sujeto, objeto, medio y fin.

3.1.3. Método

El método a utilizar en nuestro tema es el deductivo por ser investigativo y recopilar información que se utilizará en el desarrollo del mismo generando una guía técnica sobre dicha plataforma que será de uso para los usuarios.

3.1.4. Técnica

Para el desarrollo de este proyecto nos basamos en la técnica de observación, la misma que es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis.

La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor numero de datos. Gran parte del acervo de conocimientos que constituye la ciencia ha sido lograda mediante la observación.

Existen dos clases de observación: la Observación no científica y la observación científica. La diferencia básica entre una y otra está en la intencionalidad: observar científicamente significa observar con un objetivo claro, definido y preciso: el investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación. Observar no científicamente significa observar sin intención, sin objetivo definido y por tanto, sin preparación previa.

3.1.5. Instrumento

Los instrumentos utilizados fueron los siguientes:

- Investigar, recopilar información y bibliografía relacionada con el proyecto.
- Consultas que se la realizará al tutor, docentes de la institución, etc.
- Aplicación de los conocimientos aprendidos en el transcurso de ciclos anteriores.
- Y por último el desarrollo general en sí del tema propuesto.

4. RESULTADOS

4.1. Levantamiento de procesos

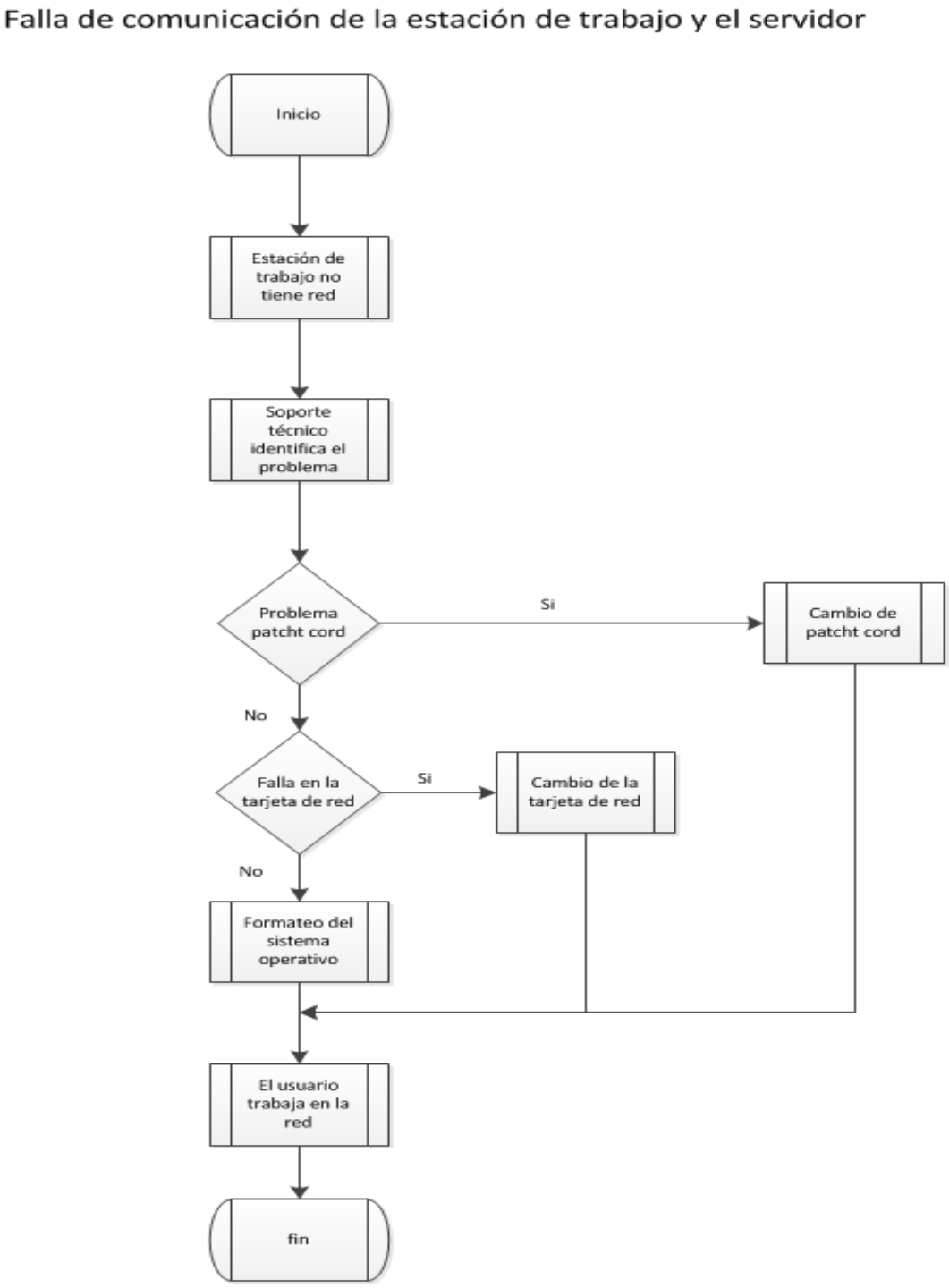


Grafico 11: Levantamiento del proceso actual de la falla en la comunicación cliente servidor.

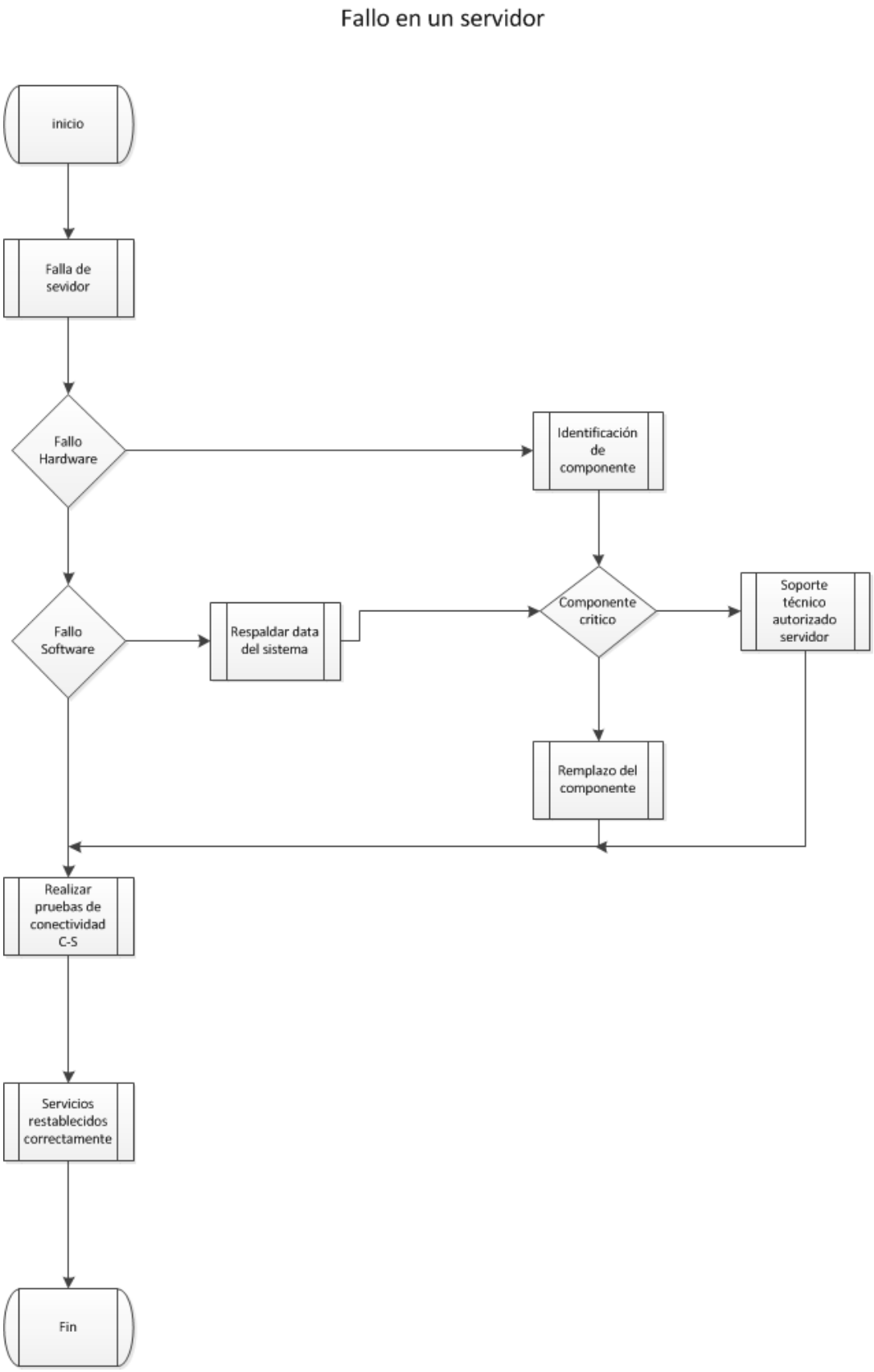


Grafico 12: Levantamiento del proceso actual de la falla de un servidor.

4.2. Documento de visión

Problema de:	**Falla en la comunicación entre la estacion de trabajo y el servidor.**
Afecta a:	Personal de la empresa
Impacto:	Retraso en las actividades del personal
Solucion:	• Brindar un soporte tecnico inmediao. • Documentar las acciones realizadas • Buscar la solucion adecuada para restablecer la comunicación.

Grafico 13: Declaración del Problema N°1

Problema de:	**Falla en el servidor**
Afecta a:	La empresa y clientes
Impacto:	Perdida general del servicio
Solucion:	• Poseer backups continuos de la data. • Contar con servicio tecnico autorizado de harware y software. • Restablecer en el menor tiempo posible el servidor.

Grafico: 14 Declaración del Problema N°2

Problema de:	**Perdida del servicio de internet**
Afecta a:	Clientes de la empresa
Impacto:	Malestar en los clientes
Solucion:	• Brindar soporte al cliente • Contar con un call center • Poseer coneccion remota a los equipos de la empresa • Repocicion de los equipos.

Grafico 15: Declaración del Problema N°3

Problema de:	**Falla en el servicio electrico**
Afecta a:	La empresa
Impacto:	Retraso en las actividades del personal
Solucion:	• Contar con fuentes alternas de energia. • Establecer procesos y actividades para la preservacion de los equipos y la información al momento que se de un corte de energis.

Grafico 16: Declaración del Problema Nº4

Problema de:	**Falta de personal de soporte tecnico**
Afecta a:	Personal de la empresa
Impacto:	Retraso en las actividades del personal
Solucion:	• Personal alterno dentro de la empresa que brinde soporte. • Contar con la documentacion adecuada de los fallos presentados y los posibles. • Posser soporte de terceros.

Grafico 17: Declaración del Problema Nº5

Para	**El personal de la empresa**
Quien	Necesita una guia con procedimientos y acciones al momento de que un problema se suscite.
El (Nombre del producto)	Plan de contingencia.
Que	Reunira las mejores practicas para las contingencias de un cento de computo.
Nuestro producto	Es un plan acoplado a las necesidades del centro de computo y de la empresa, a su vez incluye a los clientes de la empresa para mantener la operatividad de los servicios.

Grafico 18: Declaración de Posicionamiento del Producto

4.2.1 Organigrama del departamento técnico

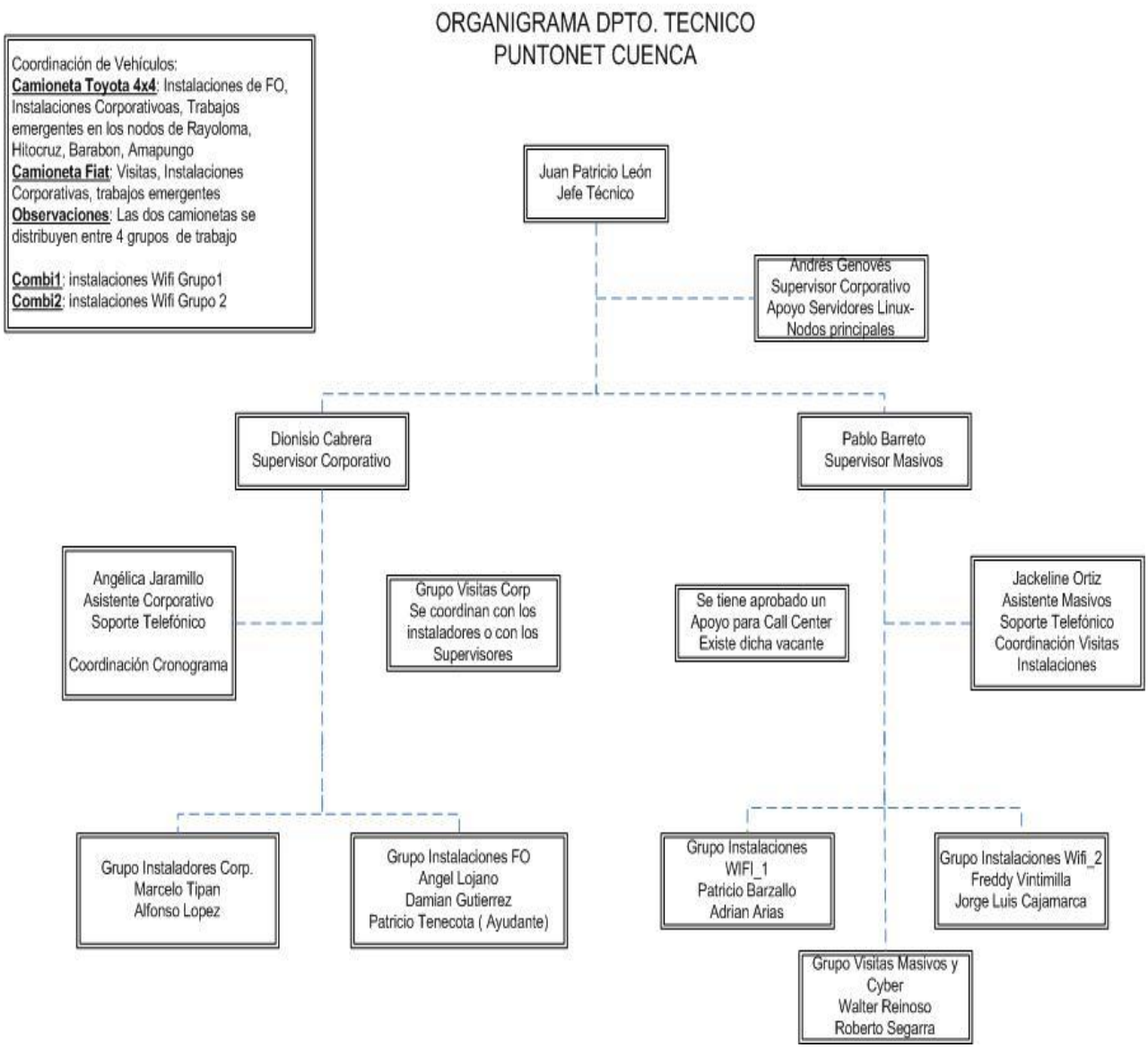


Grafico 19: Organigrama departamento tecnico PUNTONET Cuenca

Se desarrollará un plan de contingencia el cual este presto para solucionar problemas que se hagan presentes en la institución con un bajo costo y en el menor tiempo posible, con la finalidad de mantener el servicio informático de la empresa disponible un 99% del tiempo y brindar soluciones efectivas y eficaces para restablecer el servicio de internet de los usuarios.

4.2.2. Modelo de negocio.

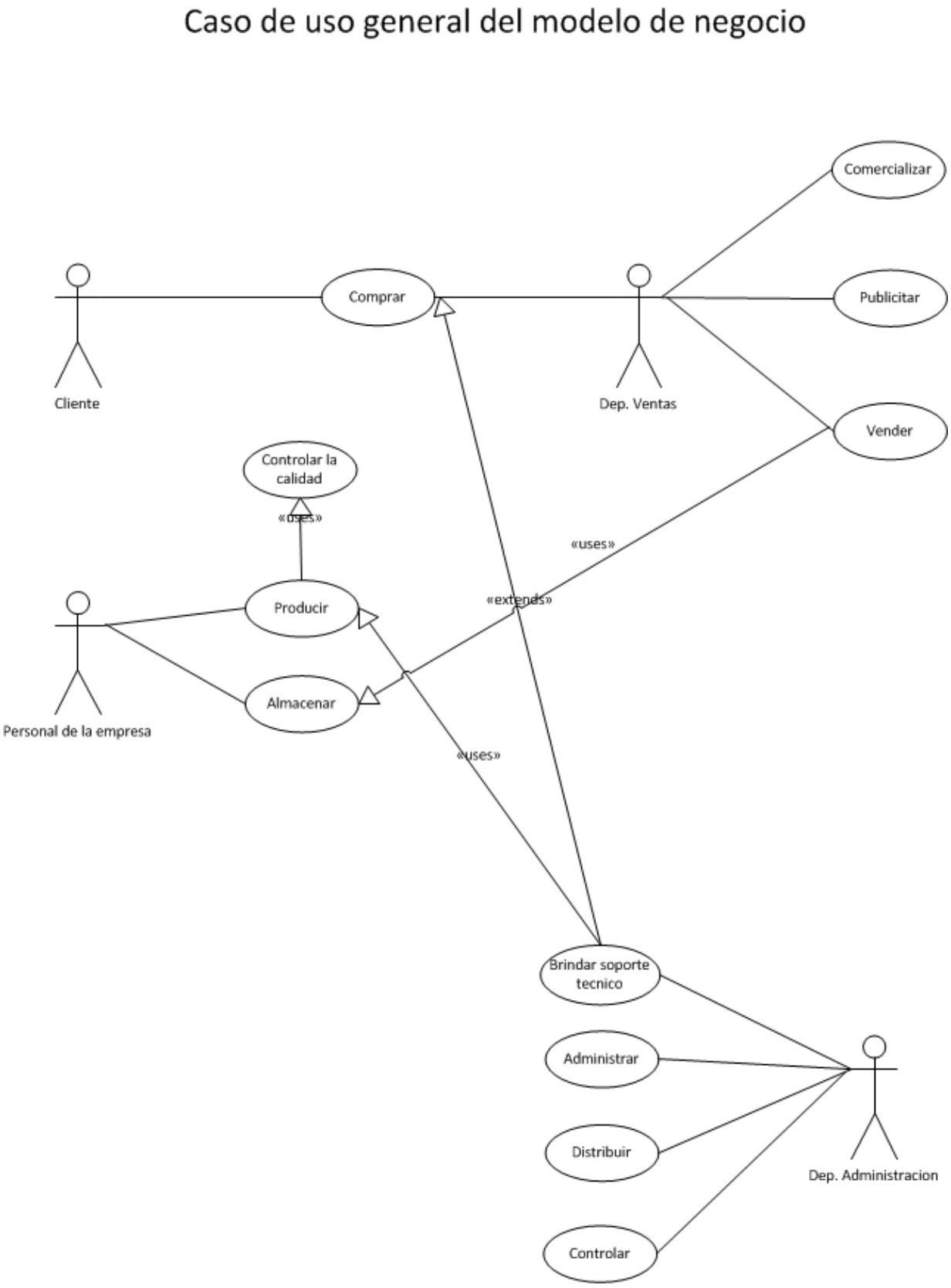


Grafico 20: Caso de uso general del modelo de negocio.

4.3. Modelo unificado de desarrollo

4.3.1. Fase 1: inicio

- ***Definir actores:***

Actor del negocio es todo individuo, grupo, entidad, organización, máquina o sistema de información externa con los que el negocio interactúa de manera permanente o casual. Lo que se modela como actor son los roles que se juegan cuando se interactúa con el negocio para beneficiarse de sus resultados.

Cada uno de los actores identificados debe poseer una breve descripción que incluya las responsabilidades y el porqué interactúa con el negocio.

La interacción de los actores con el negocio se realiza por el envío y recepción de mensajes, y para identificar el papel de cada actor se debe precisar en qué procesos se ve involucrado dicho actor. Esta es la llamada asociación de comunicación actor – negocio y el caso de uso del negocio que representa el proceso.

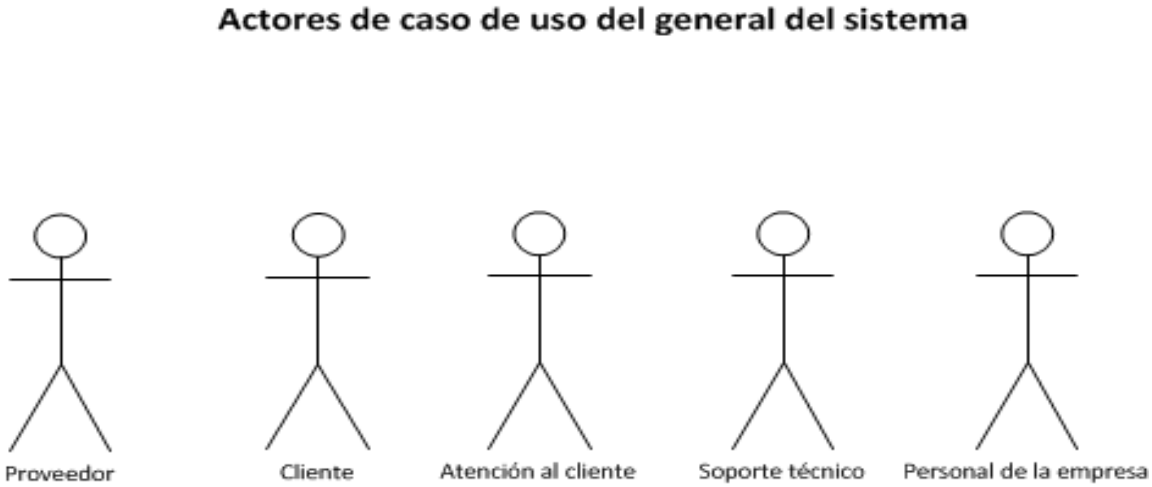


Grafico 21: Definicion de actores.

- ***Caso de uso general del plan de contingencia***

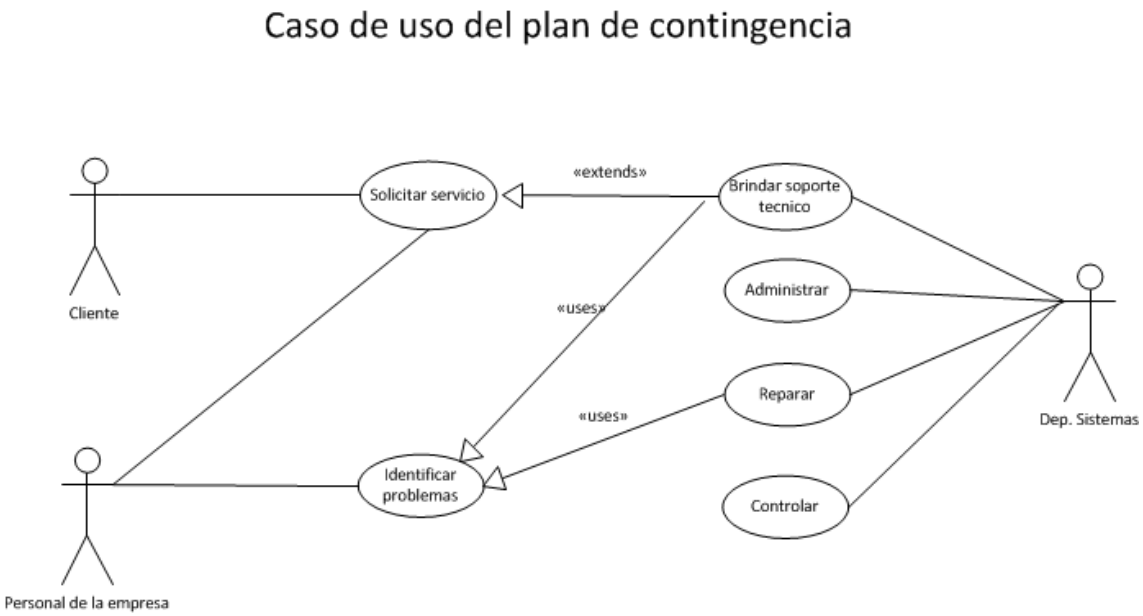


Grafico 22: Caso de uso general de el plan de contingencia.

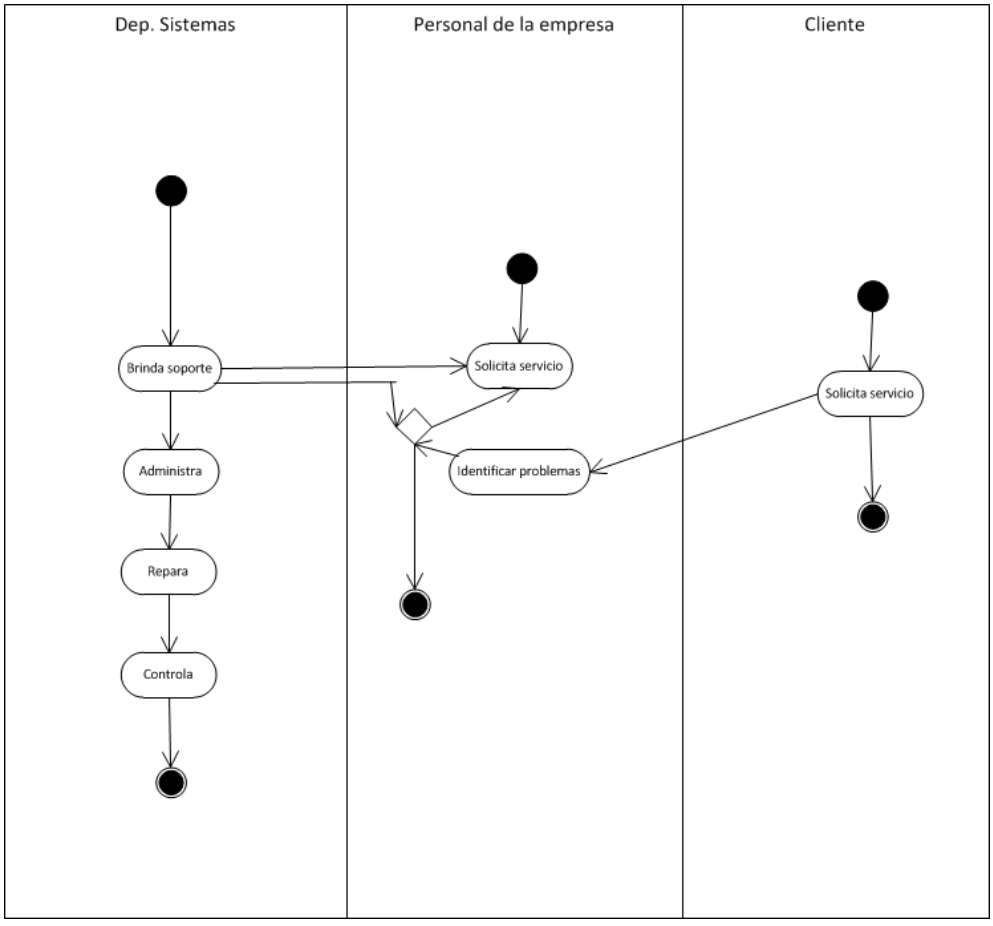


Grafico 23: Diagrama de actividad de el plan de contingencia.

- ***Mitigación de riesgo***

PROBLEMA	DESCRIPCIÓN	PRIORIDAD
Servicios prestados	Pocedimientos, para restablecer los servicios.	ALTA
Instalación eléctrica	Dotar de equipos que almacenan energia.	ALTA
Seguridades	Control de usuarios, vigilancia y seguridad logica.	MEDIA
Hardware	Mantenimiento preventivo y correctivo.	MEDIA
Software	Actualizaciones.	MEDIA
Aire acondicionado	Mantenimiento.	BAJA
Instalación física	Identificar posibles daños.	BAJA

Grafico 24: Tabla de riesgos.

- ***Requerimientos funcionales del sistema***

  - Mantener los Servicios prestados activos
  - Proveer de energía eléctrica a los componentes críticos del ISP
  - Mantener las Seguridades del centro de cómputo
  - Conservar de mejor manera el Hardware y Software
  - Velar por la integridad física de las Instalaciones y el personal
  - Restablecer los servicios informáticos de la institución en el menor tiempo posible y con bajo costo para la misma.

4.3.2. Fase 2: Elaboración

- ***Casos de uso con la propuesta de solución***

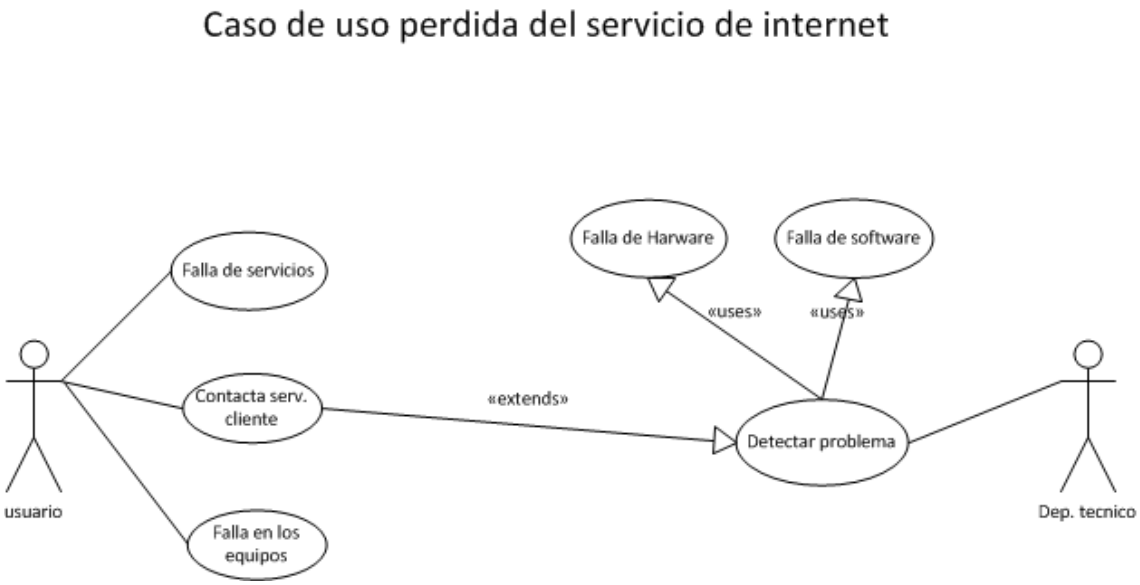


Grafico 25: Caso de uso perdida del servicio de internet.

Grafico 26: Caso de uso falla de servidores.

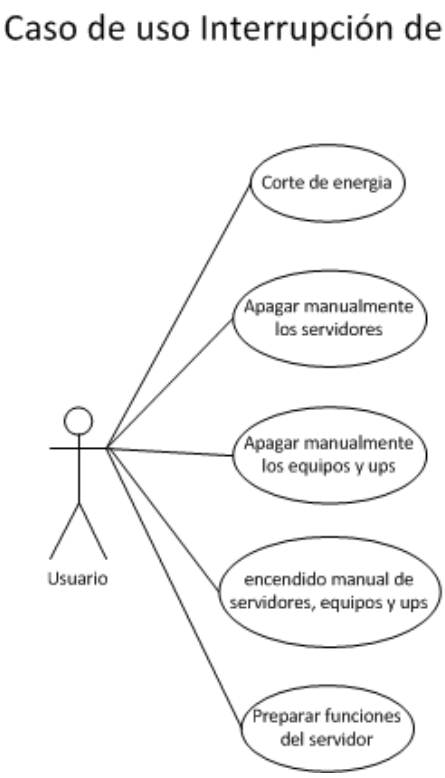


Grafico 27:Caso de uso interrupción del servicio eléctrico.

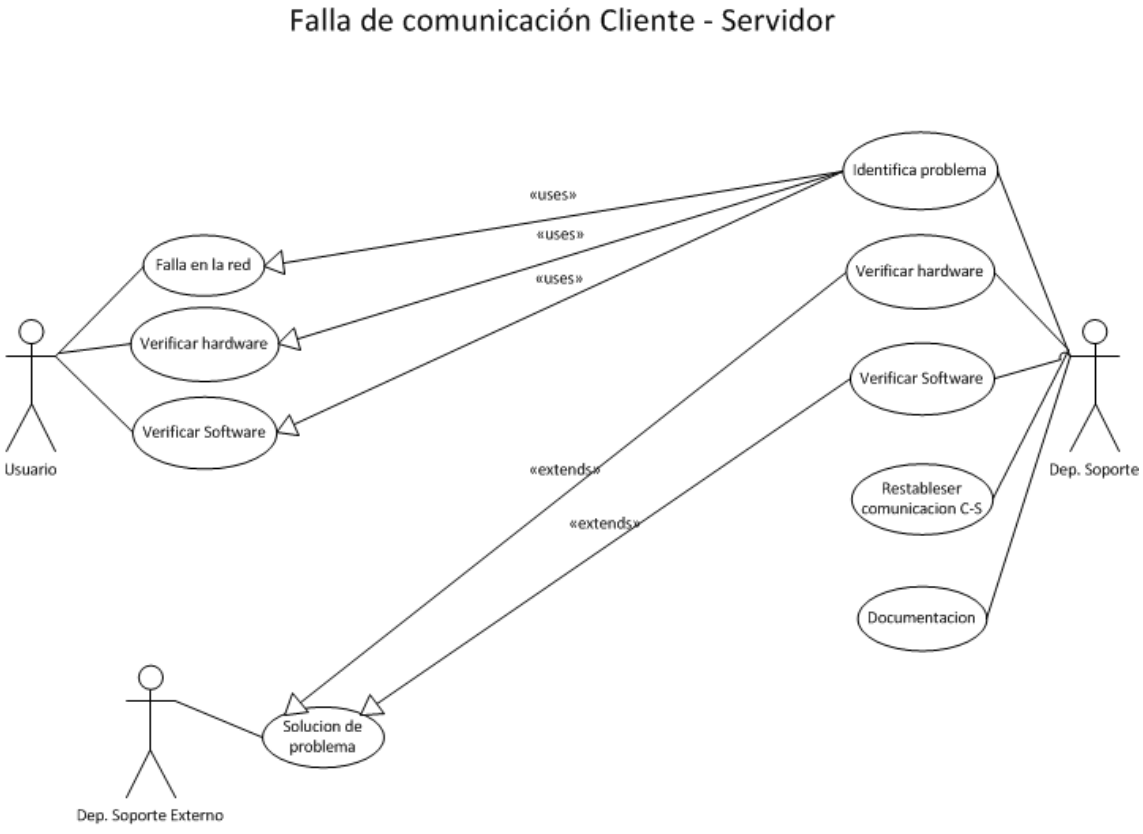


Grafico 28: Caso de uso falla en la comunicación cliente servidor.

- ***Mitigación de riesgos***

Descripción de la causa	Medidas a tomar
· **Servicio del ISP**	Mantener un monitoreo permanente de los servicios
· **Hardware**	Brindar mantenimiento preventivo y correctivo permanente
· **Comunicaciones**	Mantenimiento preventivo en las redes de comunicación
· **Software**	Actualizaciones permanentes de antivirus
· **Equipos diversos**	Mantener UPS, APA entre otros en un buen estado
· **Servicios Públicos**	Identificar y prevenir fallas en los servicios públicos
· **Recursos Humanos**	Brindar capacitaciones

Grafico 29: Tabla de mitigacion de riesgos.

- ***Arquitectura básica de un plan de contingencia***

  - Ciclo de vida
  - Contenido del plan de contingencia
  - Plan de prevención
  - Plan de ejecución
  - Plan de recuperación
  - Plan de pruebas

4.3.3. Fase 3:Construcción.

- ***Introducción***

En la actualidad tanto personas como organizaciones se han convertido en dependientes de las computadoras, redes de datos para el manejo de actividades cotidianas y disponibilidad de los sistemas informáticos, ya que la carencia de dichos recursos dificultaría las labores. Todas las empresas deberían estar preparadas para absorber inconvenientes, es decir la interrupción prolongada de los servicios informáticos, se debe tomar en cuenta en el caso de que un desastre se haga presente podría ocasionar pérdidas materiales, información sea de clientes, proveedores, productos y en el peor de los casos pérdidas humanas.

Un plan de contingencia tiene como finalidad proveer a la organización de requerimientos y alternativas para su recuperación ante desastres. La elaboración de dicho plan debe

contar con la intervención del nivel ejecutivo de la organización, personal, usuarios y el técnico de los procesos.

- ***Plan de Contingencia***

Es un instrumento de gestión para obtener un buen gobierno de las TI, dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. "Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante."[7]

Plan de contingencia informático es un documento que recopila los procedimientos alternativos para facilitar el normal funcionamiento de las tecnologías de información y de comunicación, cuando algún servicio se ve afectado negativamente por cualquier inconveniente interno o externo a la organización.

Acciones a ser consideradas:

- Antes, como un plan de respaldo o de prevención para moderar los efectos de los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

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

El plan de contingencia ayuda a minimizar las consecuencias en caso de que un incidente se presente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término "incidente" en este contexto será entendido como la interrupción de las actividades cotidianas que influyan en la normal operación en cualquier proceso informático de la organización.

- ***Ciclo de vida de un plan de contingencia***

El ciclo de vida iterativo de un plan de contingencia es el conocido PDCA(plan-do-check-act, es decir, planificar-hacer-comprobar-actuar). Parte de un análisis de riesgo en el cual, entre otras amenazas, se identifican aquellas que afectan la continuidad del negocio.

Cuya base están seleccionadas las contramedidas más adecuadas entre diferentes alternativas, siendo estas plasmadas en el plan de contingencia junto a los recursos necesarios para ponerlo en marcha.

El plan debe estar sometido a una revisión periódica. Por lo general la revisión será consecuencia de un nuevo análisis de riesgo. "En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.
- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa del fallo y proponer nuevas contramedidas.

- Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos. Es posible que las contramedidas adoptadas fueran eficaces para una amenaza no prevista. No obstante, esto no es excusa para evitar el análisis de lo ocurrido."[8]

- ***Contenido de un plan de contingencia***

Un plan de contingencia comprende tres sub planes. Cada uno de estos sub planes contiene las contramedidas necesarias para cada momento del tiempo en el que surge la materialización de cualquier amenaza.

- ***Plan de Prevención***

  Es un conjunto de acciones, decisiones y comprobaciones recopiladas para prevenir eventos con el fin de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

  El plan de prevención es la parte primordial del plan de contingencia porque aminora y atenúa la probabilidad de que ocurra un estado de contingencia.

- ***Plan de Ejecución***

  Es un conjunto detallado de acciones a realizar en el momento dado que se presente un incidente de contingencia el mismo que activa un mecanismo alterno que permitirá remplazar a la actividad normal cuando este no esté disponible o sufra algún fallo.

  Las acciones que se encuentran descritas dentro del plan de ejecución deben ser lo más claras y definidas posible de tal manera que sean de fácil asimilación y entendimiento para el personal involucrado en atender la contingencia.

[8]http://es.wikipedia.org/wiki/Plan_de_Contingencias#Ciclo_de_vida

- ***Plan de Recuperación***

Es el conjunto de acciones cuyo objetivo es restablecer oportunamente las operaciones, procesos y recursos de él ó los servicios que fueron afectados por una eventual contingencia.

Un plan de contingencia informático debe constar de una recursividad que permita la retroalimentación para mejorar continuamente los planes en cada etapa.

- ***Plan de Pruebas***

El plan de pruebas, será presentado a la dirección ejecutiva de la organización para la aprobación previa a la implementación.

- ***Desarrollo de la metodología para un plan de contingencia***

Para elaborar un Plan de Contingencia se seguirá una metodología que consta de las siguientes fases:

- Organización
- Identificación y priorización de riesgos
- Definición de eventos susceptibles de contingencia
- Elaboración del Plan de Contingencia
- Definición y Ejecución del Plan de Pruebas

- ***Organización del Plan de Contingencia***

Una característica seria y formal de toda organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan superar de manera provisional mientras dura dicho evento.

Entonces es necesario definir un plan de contingencia informático el mismo que deba realizarse de manera formal y responsable de tal manera que involucre a toda la

organización en el Plan de Prevención, Ejecución y recuperación, sin antes definir un grupo responsable para su elaboración, validación y mantenimiento.

Grafico 30: Organización Administrativa del plan de Contingencia

Descripción de las funciones y roles de la organización Administrativa del Plan de Contingencia:

A. Coordinación Ejecutora del Plan

La coordinación ejecutora del plan de contingencia es la responsabilidad del Director Ejecutivo, el mismo que define todas las acciones y políticas que se llevarán a cabo al momento de presentarse una eventualidad, también bajo este se encontrará la responsabilidad de que todas las actividades se cumplan de acuerdo a lo planeado.

Funciones y Roles de la Coordinación Ejecutora del Plan:

- Permanente actualización del plan de contingencia.

- Posee la responsabilidad de la ejecución del plan de contingencia, en el momento que se presente la eventualidad que lo active.
- Se encarga de la evaluación de impacto de las contingencias presentadas.
- La elaboración de los informes referentes a las contingencias.
- Plantear la integración de nuevos eventos necesarios al plan de contingencia al Comité de contingencia.
- Proponer la capacitación para el personal nuevo del servicio, acerca de las actividades a realizar al momento de presentarse una contingencia.
- Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el plan de contingencia.
- Establecer reuniones periódicas para aclarar puntos referentes al plan de contingencia.

B. Comité de contingencia

Dicho comité es el órgano encargado de coordinar y aprobar todas las actividades previamente planificadas para ejecutarse en el caso de contingencias del servicio.

El comité mantendrá reuniones trimestrales en las mismas que se definirán los lineamientos para sustentar el plan de contingencia.

El comité constara de los siguientes miembros:

- Gerente General
- Gerente de Comercialización
- Gerente de Contabilidad y Finanzas
- Gerente de Sistemas

- Director de Tecnologías y Sistemas Informáticos
- Jefe de Departamento de Desarrollo de Sistemas
- Jefe de Departamento de Soporte Técnico
- Jefe de Departamento de Comunicaciones

Los miembros del comité pueden ser modificados según el organigrama de la empresa.

Los Gerentes y Director de Tecnología y Sistemas Informáticos, podrán designar a otros integrantes que consideren necesarios para formar parte del comité.

Funciones y Roles del Comité del Plan de Contingencia

Participar en las reuniones periódicas que serán planteadas por el Coordinador del Plan de Contingencia.

Proponer la incorporación y/o modificación de procedimientos del Plan de Contingencia.

Aprobar y/o rechazar las incorporaciones y/o modificaciones del Plan de Contingencia propuestos por los miembros ó coordinador de contingencia.

Verificar que todo el personal a su cargo reciba una correcta capacitación para la ejecución del plan de contingencia.

Coordinar una correcta ejecución de las actividades del plan de pruebas.

Aprobar los informes presentados por la coordinación del plan referente a cualquier evento relacionado con el mismo.

Determinar prioridades y tiempos de recuperación de los diversos servicios que pueden verse afectados por cualquier imprevisto.

Coordinar con los proveedores de recursos externos necesarios para soportar y restaurar los servicios afectados por las contingencias.

Coordinar y ejecutar una capacitación efectiva al personal nuevo, sobre las actividades que se deben llevar a cabo al momento de presentarse una contingencia.

C. Contraloría del plan de contingencia

En caso de que existiera una oficina de Auditoría Interna sería el órgano encargado de supervisar todos los elementos y recursos descritos que intervendrán en una situación de contingencia, estén disponibles y sean viables de tal modo que se garantice un correcto funcionamiento sin carencias ni fallas en una situación real de contingencia, bajo los roles y funciones siguientes:

- Verificar que el plan de contingencia se encuentre actualizado.
- Revisar y verificar que el documento de plan de contingencia se encuentre dentro de los alcances establecidos.
- Suministrar los recursos necesarios para una ejecución viable del plan de contingencia.
- Corroborar que el plan de contingencia se cumpla de la mejor manera.
- Presentar los informes necesarios del plan de contingencia al comité de contingencia de la empresa.
- Certificar la viabilidad de los recursos descritos en el plan de contingencia y que los mismos se encuentren para que sean usados cuando un evento de contingencia lo requiera.

- Auditar los procesos que forman parte del plan de contingencia, corroborando que se cumpla correctamente.
- Informar al comité cualquier evento, anomalía o inconveniente encontrado, que ponga en riesgo la ejecución del plan.
- Proponer mejoras que permitan minimizar los riesgos de operación.

- ***Identificación y priorización de riesgos del plan***

Se denomina INCIDENCIA a todo hecho que se pueda presentar en cualquier instante, bajo una probabilidad de ocurrencia.

Riesgo: Está definido como un suceso incierto que pueda llegar a presentarse en un futuro dependiendo de variables internas o externas. Entonces vendría siendo la cuantificación de una amenaza.

A. Análisis de riesgo

El análisis de riesgo está basado 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, existen tres elementos que permitirán aproximar un valor objetivo de riesgo de la lista de riesgos principales: Probabilidad, impacto y exposición del riesgo. Los mismos que permiten al equipo coordinador categorizar los riesgos, lo que a su vez permite priorizar los riesgos más importantes.

B. Probabilidad del Riesgo

Es la probabilidad de que un evento de contingencia se produzca realmente. La probabilidad del riesgo debe ser mayor a cero, caso contrario el riesgo no sería una amenaza para el servicio. Así mismo, la probabilidad debe ser menor al 100% o el riesgo seria una certeza.

La probabilidad puede ser entendida como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia sería del 100%.

C. Impacto del Riesgo

El impacto del riesgo se encarga de medir la gravedad de los efectos adversos, o la magnitud de una pérdida, que podría causar la consecuencia.

Se aplica una calificación al riesgo, para describir su impacto con relación al grado de afectación del nivel de servicio normal. Mientras mas alto sea el número, mayor seria el impacto.

Para nuestro caso, clasificaremos el impacto con una escala del 1 al 4.

D. Exposición al Riesgo

La exposición al riesgo viene siendo el resultado de multiplicar la probabilidad por el impacto. En ocasiones un riesgo de alta probabilidad tienen un bajo impacto y puede ser ignorada sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad por lo que también puede ser ignorado, en este caso se tendría que considerar la criticidad de dicho evento.

Aquellos riesgos que contienen un alto nivel de probabilidad y de impacto son los que más necesidad de administración, pues son los que producirán los valores más elevados de exposición.

E. Definición de eventos controlables y no controlables

La identificación de los riesgos, estos deben estar categorizados en función a las acciones preventivas que pueden estar en manos de la empresa, o cuya ocurrencia no pueda ser predicha con anterioridad. Así los eventos pueden ser:

Eventos Controlables, al momento de identificarlos se pueden plantear acciones que eviten la ejecución o reduzca el impacto.

Eventos No Controlables, cuando la ocurrencia es impredecible y únicamente se pueden plantear acciones que permitan minimizar su impacto.

La identificación se la realizará en la siguiente matriz de riesgo explicada a continuación.

F. Definición de la Matriz de Riesgo

La ejecución de un evento tiene una consecuencia sobre las actividades operativas del servicio, en tal sentido, es de suma importancia conocer el impacto del evento cuando este se presente, por lo que es necesario cuantificar la misma, a efectos de ser bastante objetivos en el análisis.

El factor numérico que se le asigna es directamente proporcional y va ascendiendo con respecto al impacto o gravedad que su presencia pueda generar sobre los diferentes alcances del servicio y se clasificaran como se explica en el Grafico Nº31.

Impacto	Descripción	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 critica, daño severo	4

Grafico 31: Cuadro de Impactos

Probabilidad de ocurrencia	Descripción
Remoto	Poco probable que suceda
Ocasional	Incidentes aislados
Probable	Sucede alguna vez
Frecuente	Incidentes repetitivos

Grafico 32: Cuadro de Probabilidad de Ocurrencia

De la misma manera la probabilidad de que ocurra un evento resulta de gran importancia para la determinación de la posibilidad de que dicho evento se presente en la realidad. La determinación de dicha probabilidad será obtenida de la recolección estadística de los eventos que se hayan presentado a lo largo de la administración de los servicios, así como la información obtenida de otros planes de contingencia.

Exposición/Ponderación = Impacto x Probabilidad

Impacto

Por último, luego de haber validado y ponderado objetivamente las probabilidades de ocurrencia y los impactos asociados, se establecen las políticas que se han de considerar para la determinación de aquellos eventos que formarán parte del plan de contingencia, como sigue:

Todo evento cuya puntuación este en “Gran Impacto: 4”, se lo considerara de manera obligatoria dentro del plan de contingencia.

Todo evento cuya exposición al riesgo este dada con una puntuación mayor o igual a 0.15 también será considerado en el plan de contingencia (ver Cuadro Nº33).

Posterior a todo lo expuesto, se construirá la "Matriz de Riesgo de Contingencia" en la que se tomara en cuenta todos los eventos susceptibles de entrar en contingencia, indicando su consideración y categorización (controlable ó no controlable) para la construcción del plan de contingencia. De igual modo se empleara los siguientes tópicos como forma de agrupar a dichos eventos:

- Contingencias relacionadas a Siniestros
- Contingencias relacionadas a los Sistemas de Información
- Contingencias relacionadas a los Recursos Humanos
- Plan de Seguridad Física

o ***Definición de Eventos Susceptibles de Contingencia***

El plan de contingencia hace referencia a todos los aspectos que hacen parte del servicio informático, de tal manera que resulta de vital importancia considerar todos los aspectos susceptibles de provocar eventos que provoquen la activación de la contingencia. Los elementos primordiales a considerar para su evaluación son:

- **Servicio del ISP**
  - ❖ Internet
  - ❖ Correo electrónico
  - ❖ Hosting
  - ❖ Voz sobre IP
  - ❖ Transmisión de Datos

- **Hardware**
  - ❖ Servidores
  - ❖ Estaciones de trabajo(máquinas de escritorio y laptops)
  - ❖ Impresoras, scanner's, copiadoras e impresoras multifunción
  - ❖ Equipos multimedia
  - ❖ Equipos de radio frecuencia
  - ❖ Sistemas de control biométrico
- **Comunicaciones**
  - ❖ Equipos de comunicaciones switch
  - ❖ Equipos de comunicaciones router
  - ❖ Equipos de telefonía fija
  - ❖ Cableado de red de datos
  - ❖ Enlaces de cobre y fibra óptica
- **Software**
  - ❖ Servidor de Bases de datos (SQL, MySQL, Oracle, etc.)
  - ❖ Servidor web(Tomcat, Apache, Weblogic, etc.)
  - ❖ Software Base (OS y Ofimática)
  - ❖ Aplicativos usados por la empresa
  - ❖ Antivirus
- **Información sobre Sistemas Informáticos**
  - ❖ Respaldos de información y configuración de los servidores.
  - ❖ Respaldos de Base de Datos
  - ❖ Respaldo de información generada por el software base y de ofimática
  - ❖ Respaldo de las aplicaciones utilizadas por la empresa
  - ❖ Bases de datos usados por los aplicativos

- **Equipos diversos**
  - ❖ UPS
  - ❖ Aire Acondicionado
  - ❖ Grupo Electrógeno (si existiera)
- **Infraestructura Física**
  - ❖ Oficinas (Matriz y Sucursales)
  - ❖ Laboratorios descentralizados
- **Operativos**
  - ❖ Logística operativa (Suministros Informáticos).
- **Servicios Públicos**
  - ❖ Energía Eléctrica
  - ❖ Telefonía (fija y móvil)
  - ❖ Agua
- **Recursos Humanos**
  - ❖ Disponibilidad de personal de dirección
  - ❖ Disponibilidad de personal operativo

o ***Elaboración del Plan de Contingencia***

Una fase muy importante del plan de contingencia es la revisión y documentación de toda la información que será plasmada en una guía práctica y de fácil entendimiento por él para el personal de la empresa.

De manera que una fase importante en la metodología es considerar un formato estándar para el registro de todos los eventos definidos que forman parte del plan, al final se conseguirá un entregable ajustado a los requerimientos y políticas definidas para tal fin.

El contenido de los eventos que conforman el plan de contingencia son:

- ***Formato de Registro del Plan de Contingencia***

Para facilitar y agilitar la lectura del plan de contingencia, se diseñó un formato, An2: "Formato de Registro de Plan de Contingencia" el mismo que se describe a continuación y está formado de las siguientes partes:

Encabezado: El formato posee un encabezado, cuyo contenido es presentado de la siguiente manera:

Elaborado: Se indicará en todos los casos el nombre de la empresa.

Código del Formato: FrPlC – XX (matriz de riesgo de Contingencia).

Nombre del evento: especificación clara y muy comprensiva.

Cuerpo Principal: En él se desarrollará uno por uno de los eventos que forman parte del plan de contingencia y describe el contenido de cada campo.

- ***Definición y Ejecución del Plan de Pruebas***

Estando consientes de que una situación de contingencia puede presentarse en cualquier instante, de tal manera llegar a convertirse en un problema prioritario de atención si el mismo se efectuara en horario de oficina que pueda resultar de gran impacto en el desarrollo de las actividades de la empresa; de tal modo se hace necesario definir específicamente todas las acciones necesarias para asegurar que, si un caso real de contingencia se hiciera presente tener las prestaciones y funcionalidades mínimas que permitan la posterior ejecución del plan de recuperación de manera rápida y segura.

De tal manera que la garantía del "éxito" del plan de contingencia está basada en una validación y certificación anticipada del mismo, en cada uno de sus procesos.

A. Alcance y objetivos

En vista de que gran parte de los planes de contingencia están orientados a los siniestros, recursos humanos y seguridad, cuyas situaciones son imposibles de reproducir en la vida real (Ejm: robo, terremotos, incendios, etc.), el plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas en los equipos, información procesos; los mismos que son manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

En este contexto se puede precisar los objetivos a alcanzar con la realización de las pruebas:

Programar la validación y pruebas de todas las actividades que se llevan a cabo como parte del plan de ejecución del plan de contingencia con respecto a una posible interrupción de los procesos identificados como críticos de la empresa.

Identificar mediante pruebas las posibles causas que pueden atentar contra el normal funcionamiento, ejecución y medidas correctivas que puedan ser aplicadas para subsanar los errores o deficiencias que se deriven de ellas (retroalimentación del plan).

Establecer roles y funciones que deben cumplir los responsables en las pruebas, los mismos que serán asignados para la ejecución en caso de que se presente una situación real de contingencia.

Con la finalidad de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que deben ser ejecutados por un grupo determinado de usuarios de las diferentes direcciones y jefaturas de la empresa, los mismos que se encargarán de verificar, observar y probar cualquier incidencia durante la ejecución de dicha prueba, con el fin de retroalimentar cualquier acción que pueda mejorar o corregir el plan.

"La información a desarrollar como parte del plan de pruebas, posee el siguiente esquema:"[9]

1. OBJETIVOS DE LA PRUEBA DEL PLAN DE CONTINGENCIA
   - Definir los Objetivos
2. ALCANCE Y LIMITACIÓN
   - Identificar Áreas Afectadas (relación)
   - Personal involucrado (relación)
   - Que no contendrá la prueba
3. DESCRIPCIÓN DE LA PRUEBA A EFECTUARSE
   - Evaluación de una situación de Emergencia
   - Medios disponibles para operar
   - Fechas y horas
4. RESULTADOS ESPERADOS DE LAS PRUEBAS
   - Relación de posibles acciones

B. Validación y Registro de Pruebas

Las actividades generales que forman parte de la prueba, deben validarse, registrarse y firmarse por todos los responsables que intervinieron en cada una de ellas con el fin de corroborar su ejecución y certificación, esto debe incluir las observaciones del caso.

(Torres, 2011)(fopae, 2012)(EDUARDOJOSÉGONZÁLEZANGULO, 2012)[9]http://auditoriadesistemas.galeon.com/productos2227783.html

En el anexo An4 “Control y Certificación de Pruebas de Contingencia” indica el formato que se debe usar para la validación y registro de dichas pruebas, así también el detalle de la información que se debe ingresar en cada uno de los campos.

4.3.4 Desarrollo de las fases y actividades

Fases de un plan de contingencia

En esta parte del capítulo la Unidad informática, plantea el desarrollo de los siguientes puntos, empleando la metodología propuesta anteriormente. El desarrollo constará de las siguientes fases de la metodología:

- Identificación y Priorización de riesgos
- Definición de Eventos susceptibles de Contingencia.
- Elaboración del Plan de Contingencia.

Identificación y priorización de riesgos

El cuadro N °3 muestra la matriz de Riesgo de Contingencia, ponderado tomando en cuenta los valores de riesgo e impacto en el servicio (operatividad), empleando los conocimientos y la experiencia práctica de Informática en Gestión de Sistemas de Información, en la columna de categoría cada evento es categorizado en Controlables (C) y No Controlables(NC).

Ítem	Descripción del riesgo	Probabilidad	Impacto	ponderancia	Categoría	Alerta
Sub Factor. Riesgos relacionadas a Siniestros						
	Infraestructura					
1	Sismo	0.1	4	0.4	Nc	R
2	Incendio	0.04	4	0.16	C	R
3	Inundación por lluvias	0.2	1	0.02	Nc	
4	Inundación por fallo en las tuberías o servicio sanitario	0.1	2	0.2	C	R
5	Terremoto	0.04	4	0.16	Nc	R
	Servicios públicos					
6	Interrupción del servicio eléctrico	0.1	4	0.16	Nc	R
7	Falla en el servicio de agua potable	0.01	3	0.03	Nc	
8	Avería en el servicio telefónico	0.01	3	0.03	Nc	
	Equipo					
9	Daño del grupo electrógeno	0.03	4	0.12	C	
Sub Factor. Riesgos relacionadas a Sistemas de Información						
	Información					
10	Perdida de documentos	0.02	3	0.06	C	
11	Robo o sustracción de información	0.02	3	0.06	C	
	Software					
12	Perdida del sistema central	0.05	4	0.2	C	R
13	Virus en los equipos	0.05	4	0.2	C	R
14	Perdida del servidor de correo	0.01	2	0.02	C	
15	Fallo en el motor de base de datos	0.04	4	0.16	C	R
16	Fallas en el sistema operativo	0.04	4	0.16	C	R
	Comunicación					
17	Daño en la red de datos	0.02	4	0.08	C	
	Hardware					
18	Avería de los pc´s	0.02	2	0.04	C	
	Recursos operativos y logísticos					
19	Daño en los equipos multimedia, impresoras, scanner's y otros	0.01	2	0.02	C	
Sub factor: Riesgos relacionadas a recursos humanos						
	Recursos humanos					
20	Ausencias imprevista del personal de soporte técnico	0.05	3	0.15	C	R

21	Ausencia de personal ejecutivo para la toma decisiones ante situaciones de riesgo informático	0.05	3	0.15	C	R
22	Falta de capacidad del personal en la reserva de información en la DB	0.01	4	0.04	Nc	
Sub factor: Plan de seguridad Física						
	Infraestructura					
23	Sustracción de equipos y software diversos	0.05	4	0.2	C	R
24	Sabotaje	0.01	2	0.02	Nc	
25	Vandalismo	0.01	3	0.03	Nc	
26	Actos terroristas	0.01	1	0.01	Nc	

Grafico 33: Matriz de Riesgo de Contingencia

Nota: Los casilleros marcados con la letra "R" nos indica que dicho evento produce un alto impacto a la empresa por consiguiente debe ser controlado.

La categorización de los eventos C (Controlables) y NC (No Controlables) están resumidos en los cuadros Nº31 y Nº32:

ITEM	**Eventos Controlables**
Cuadro Nº3	
2	Incendio
4	Inundación por fallo en las tuberías o servicio sanitario
9	Daño del grupo electrógeno
10	Perdida de documentos
11	Robo o sustracción de información
12	Perdida del sistema central
13	Virus en los equipos
14	Perdida del servidor de correo
15	Fallo en el motor de base de datos
16	Fallas en el sistema operativo
17	Daño en la red de datos
18	Avería de los pc´s

19	Daño en los equipos multimedia, impresoras, scanner's y otros
20	Ausencias imprevista del personal de soporte técnico
21	Ausencia de personal ejecutivo para la toma decisiones ante situaciones de riesgo informático
23	Sustracción de equipos y software diversos

Grafico 34: Eventos Controlables

ITEM	**Eventos Controlables**
Cuadro N°3	
1	Sismo
3	Inundación por lluvia
5	Terremoto
6	Interrupción del servicio eléctrico
7	Falla en el servicio de agua potable
8	Avería en el servicio telefónico
22	Falta de capacidad del personal en la reserva de información en la DB
24	Sabotaje
25	Vandalismo
26	Actos terroristas

Grafico 35*:* Eventos no Controlables

Definición de Eventos susceptibles de Contingencia

A continuación se presentan todos los eventos de contingencia detallados en el cuadro Nº7 "elementos vs subfactores", donde se expone la relación existente entre elementos mínimos definidos por la unidad informática, realizando referencias de los planes de contingencia con relación el mismo indicando a que subfactor desarrollado pertenecen. En adelante se emplea "FrPlC" en los códigos, haciendo referencia al formato del plan de contingencia.

Elemento	Plan de contingencia desarrollado		
	Código	Alcance	Subfactor
software			
Servidor de Bases de datos (SQL, MySQL, Oracle, etc.)	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -15	Software	Contingencia sistemas de información
Servidor web(Tomcat, Apache, Weblogic, etc.)	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -15	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
	FrPlC -17	Software	Contingencia sistemas de información
Software Base (OS y Ofimática)	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
	FrPlC -17	Software	Contingencia sistemas de información
Aplicativos usado por la empresa	FrPlC -10	Información	Contingencia sistemas de información
	FrPlC -11	Información	Contingencia sistemas de información
	FrPlC -12	Software	Contingencia sistemas de información
	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -14	Software	Contingencia sistemas de información
	FrPlC -15	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
	FrPlC -17	Comunicaciones	Contingencia sistemas de información
Antivirus	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -14	Software	Contingencia sistemas de información
	FrPlC -15	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
	FrPlC -17	Software	Contingencia sistemas de información
Información			
Respaldos de información y configuración de los servidores.	FrPlC -15	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
Respaldos de Base de Datos	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -15	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
Respaldo de información generada por el software base y	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -15	Software	Contingencia sistemas de información

de ofimática	FrPlC -16	Software	Contingencia sistemas de información
Respaldo de las aplicaciones utilizadas por la empresa	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
Bases de datos usados por los aplicativos	FrPlC -13	Software	Contingencia sistemas de información
	FrPlC -16	Software	Contingencia sistemas de información
Equipos diversos			
UPS	FrPlC -06	Servicios Públicos	Contingencia siniestros
Aire Acondicionado	FrPlC -06	Servicios Públicos	Contingencia siniestros
Grupo Electrógeno (si existiera)	FrPlC -09	Operativo	Contingencia sistemas de información
Infraestructura Física			
Oficinas (Matriz y Sucursales)	FrPlC -01	Infraestructura	Contingencia siniestros
	FrPlC -02	Infraestructura	Contingencia siniestros
	FrPlC -03	Infraestructura	Contingencia siniestros
	FrPlC -04	Infraestructura	Contingencia siniestros
	FrPlC -05	Infraestructura	Contingencia siniestros
	FrPlC -25	Infraestructura	Contingencia de seguridad física
	FrPlC -26	Infraestructura	Contingencia de seguridad física
Laboratorios descentralizados	FrPlC -01	Infraestructura	Contingencia siniestros
	FrPlC -02	Infraestructura	Contingencia siniestros
	FrPlC -03	Infraestructura	Contingencia siniestros
	FrPlC -04	Infraestructura	Contingencia siniestros
	FrPlC -05	Infraestructura	Contingencia siniestros
	FrPlC -25	Infraestructura	Contingencia de seguridad física
	FrPlC -26	Infraestructura	Contingencia de seguridad física
Servicios Públicos			
Energía Eléctrica	FrPlC -06	Servicios Públicos	Contingencia siniestros
Telefonía (fija y móvil)	FrPlC -08	Servicios Públicos	Contingencia siniestros
Agua	FrPlC -07	Servicios Públicos	Contingencia siniestros
Recursos Humanos			
Disponibilidad de personal de dirección	FrPlC -21	Recursos Humanos	Contingencia recursos humanos
	FrPlC -22	Recursos Humanos	Contingencia recursos humanos
	FrPlC -24	Infraestructura	Contingencia de seguridad física
	FrPlC -25	Infraestructura	Contingencia de seguridad física

Disponibilidad de personal operativo	FrPlC -20	Recursos Humanos	Contingencia recursos humanos
	FrPlC -22	Recursos Humanos	Contingencia recursos humanos
	FrPlC -24	Infraestructura	Contingencia de seguridad física
	FrPlC -25	Infraestructura	Contingencia de seguridad física

Grafico 36*:* Elementos Vs. Subfactores a desarrollar

Elaboración del Plan de Contingencia

Luego de identificar los eventos de contingencia y los elementos que se consideran que pueden ser afectar o causar algún inconveniente, se procede a desarrollar los planes de contingencia agrupados por subfactores.

En forma de resumen se presenta la serie de pasos sucesivos que ilustra la manera de responder ante la presencia de algún evento de contingencia:

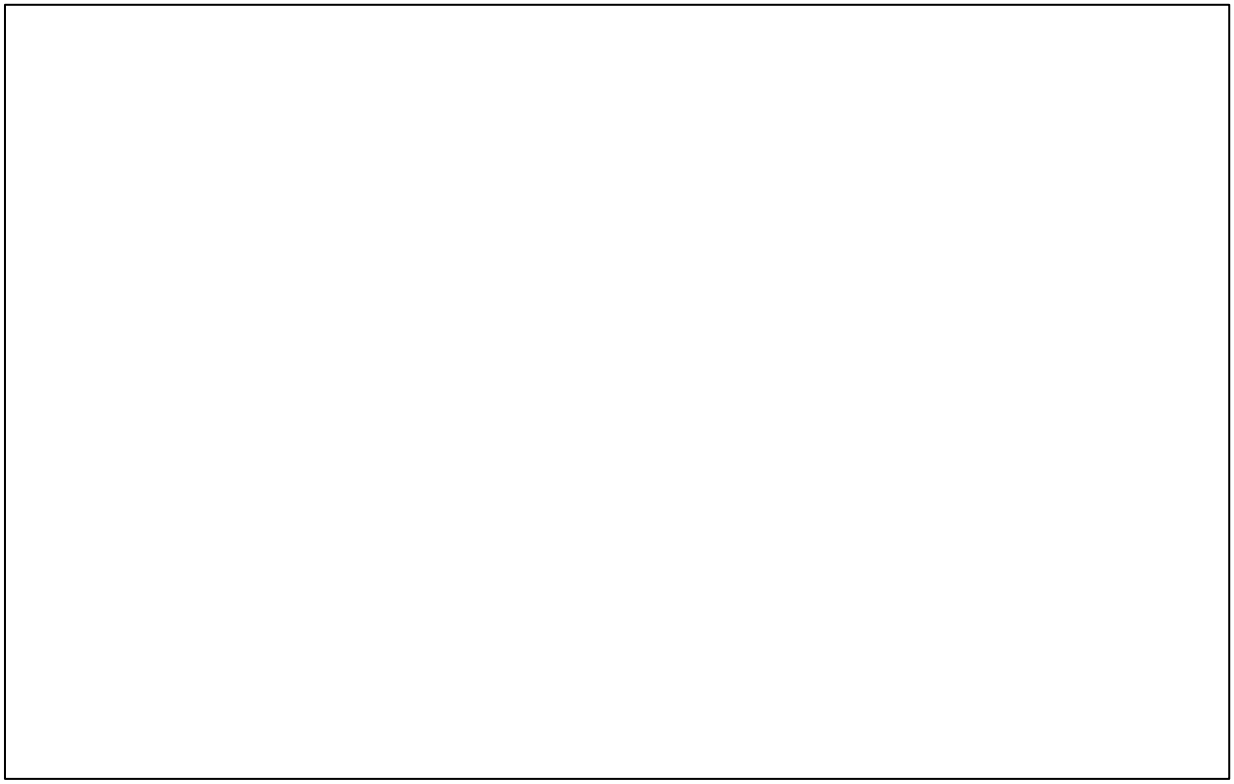


Grafico 37*:* Pasos sucesivos para responder una contingencia.

En los siguientes recuadros se indican los funcionarios encargados de cada evento de contingencia que se ha identificado, vale recalcar que la tabla que se muestra a continuación no consta la columna TELEFONO la misma que es de suma importancia, esta columna fue omitida porque no consta con datos para la presentación.

Subfactor: Siniestros		
Código	Descripción del evento de contingencia	Responsables titulares o sus representantes
FrPlC -01	Incendio	Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración
FrPlC -02	Sismo	Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración
FrPlC -03	Inundación por lluvia	Gerente General, Gerente de Sistemas, Director de administración, y/o Director de Tecnologías y Sistemas Informáticos,
FrPlC -04	Inundación por fallo en las tuberías o servicio sanitario	Gerente General, Gerente de Sistemas, Director de administración, y/o Director de Tecnologías y Sistemas Informáticos,
FrPlC -05	Terremoto	Gerente General, Gerente de Sistemas, Director de administración, y/o Director de Tecnologías y Sistemas Informáticos,
FrPlC -06	Interrupción del servicio eléctrico	Gerente General, Gerente de Sistemas, Director de administración, Director de Tecnologías y Sistemas Informáticos, y/o Jefe de Departamento de Soporte Técnico
FrPlC -07	Falla en el servicio de agua potable	Gerente General, Gerente de Sistemas, Director de administración, y/o Director de Tecnologías y Sistemas Informáticos,
FrPlC -08	Avería en el servicio telefónico	Gerente General, Gerente de Sistemas, Director de administración, Director de Tecnologías y/o Sistemas Informáticos,

FrPlC -09	Daño del grupo electrógeno	Gerente General, Gerente de Sistemas, Director de administración, Director de Tecnologías y Sistemas Informáticos, y/o Jefe de Departamento de Soporte Técnico

Grafico 38*:* Subfactor siniestros

Subfactor: Sistemas de Información		
Código	Descripción del evento de contingencia	Responsables titulares o sus representantes
FrPlC -10	Perdida de documentos	Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración
FrPlC -11	Robo o sustracción de información	Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración
FrPlC -12	Perdida del sistema central	Gerente de Sistemas, Director de Tecnologías y Sistemas Informáticos, Jefe de Departamento de Desarrollo de Sistemas, Jefe de Departamento de Soporte Técnico y/o Jefe de Departamento de Comunicaciones
FrPlC -13	Virus en los equipos	Jefe de Departamento de Soporte Técnico
FrPlC -14	Perdida del servidor de correo	Jefe de Departamento de Soporte Técnico
FrPlC -15	Fallo en el motor de base de datos	Jefe de Departamento de Soporte Técnico
FrPlC -16	Fallas en el sistema operativo	Jefe de Departamento de Soporte Técnico
FrPlC -17	Daño en la red de datos	Jefe de Departamento de Comunicaciones
FrPlC -18	Avería de los pc´s	Jefe de Departamento de Soporte Técnico
FrPlC -19	Daño en los equipos multimedia, impresoras, scanner's y otros	Jefe de Departamento de Soporte Técnico

Grafico 39*:* Subfactor Sistema de Información

Subfactor: Recursos Humanos		
Código	Descripción del evento de contingencia	Responsables titulares o sus representantes
FrPlC -20	Ausencias imprevista del personal de soporte técnico	Gerente de Sistemas, Director de administración y/o Director de Tecnologías y Sistemas Informáticos
FrPlC -21	Ausencia de personal ejecutivo para la toma decisiones ante situaciones de riesgo informático	Director de administración y/o Director de Tecnologías y Sistemas Informáticos
FrPlC -22	Falta de capacidad del personal en la reserva de información en la DB	Director de administración

Grafico 40*:* Subfactor Recursos Humanos

Subfactor: Sistemas de Información		
Código	Descripción del evento de contingencia	Responsables titulares o sus representantes
FrPlC -23	Sustracción de equipos y software diversos	Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas, Director de administración y/o Director de Tecnologías y Sistemas Informáticos
FrPlC -24	Sabotaje	Gerente General y/o Director de administración
FrPlC -25	Vandalismo	Gerente General y/o Director de administración
FrPlC -26	Actos terroristas	Gerente General y/o Director de administración

Grafico 41*:* Subfactor Sistemas de Información

A continuación se tratan los puntos referentes al desarrollo de los planes de contingencia por cada uno de los subfactores identificados empleando el formato establecido en el anexo An2: “Formato de Registro del Plan de Contingencia”

- ***Desarrollo de las Actividades***

  - ***Subfactor: Contingencias relacionadas a siniestros***

    Siniestro: Un siniestro es toda aquella emergencia causada por la naturaleza (sismos, terremotos, inundaciones, deslaves entre otros), o a su vez eventos no controlables como la caída de un poste eléctrico, explosiones, etc.

    A. Objetivo

    Incorporar en el plan de contingencia todos los eventos referentes a siniestros que promuevan una serie de acciones orientadas a la planificación, organización, preparación y mitigación de una emergencia que se presente en las instalaciones, con el fin de minimizar las posibles consecuencias humanas y operativas TIC que pudiera generarse por dicha eventualidad.

    B. Alcance

    El alcance está limitado a los eventos de contingencia o eventualidades que puedan afectar, detener o dañar las instalaciones, personal o recursos tecnológicos TIC’s.

    Adicionalmente se debe tomar en cuenta ante la presencia de un siniestro que pueda inhabilitar parcial o totalmente el “centro de datos”, es la coordinación a realizar con la dirección de la empresa para la determinación de ambientes alternos para la continuidad operativa, hasta que las operaciones se estabilicen nuevamente.

Por otra parte, se considera como elemento del desarrollo del subfactor de siniestros, que debe incluir los elementos referentes a servicios públicos, por afectar o ser consecuencia de siniestros que están latentes.

- Interrupción de energía eléctrica; una vez restablecido el servicio eléctrico se puede generar picos de voltaje que pueden causar algún tipo de siniestro, comprometiendo la seguridad física.

A continuación se indica un resumen de la matriz de riesgos, tomando en cuenta las contingencias relacionadas a los siniestros.

Código	**Descripción del evento de contingencia**	**Probabilidad de ocurrencia**	**impacto**	**Ponderación**	**Alerta**
SUBFACTOR: Contingencia relacionada a siniestros					
FrPlC -01	Sismo	0.1	4	0.4	R
FrPlC -02	Incendio	0.04	4	0.16	R
FrPlC -03	Inundación por lluvias	0.2	1	0.02	
FrPlC -04	Inundación por fallo en las tuberías o servicio sanitario	0.1	2	0.2	R
FrPlC -05	Terremoto	0.04	4	0.16	R
	Servicios públicos				
FrPlC -06	Interrupción del servicio eléctrico	0.1	4	0.16	R
FrPlC -07	Falla en el servicio de agua potable	0.01	3	0.03	
FrPlC -08	Avería en el servicio telefónico	0.01	3	0.03	
	Equipo				
FrPlC -09	Daño del grupo electrógeno	0.03	4	0.12	

Grafico 42*:* Subfactor Contingencias relacionadas a siniestros

C. Plan de pruebas

El plan de pruebas corresponde al desarrollo de los eventos como parte del Subfactor de Siniestros, siguiendo con la metodología expuesta en el plan contingencia.

Un plan de pruebas es determinado posterior al análisis de los procesos críticos del servicio y de la identificación de los eventos que pudieran presentarse. El comité de contingencia es el encargado de la aprobación del plan de pruebas luego de efectuar dicha prueba.

D. Descripción de Planes

Los eventos de mayor impacto identificados en la matriz de riesgo de contingencia se presentan a continuación.

Para la presentación del plan de contingencia de cada uno de los eventos se debe llenar en el formato que se muestra en el anexo An2: "Formato de Registro del Plan de Contingencia"

Evento: ***Sismo***

1. Plan de prevención

a. Descripción del evento

Sismo es un movimiento que se produce en el interior de la tierra el mismo que libera repentinamente energía la cual es propagada en forma de ondas produciendo el movimiento de la tierra.

Esta eventualidad involucra los siguientes elementos identificados por la empresa los cuales por su naturaleza se pueden considerar como parte afectada

o causa de él estado de contingencia, tales elementos son mostrados a continuación:

Infraestructura

Sede matriz de la empresa

Sucursal de la empresa

Recursos Humanos

Personal

b. Objetivo

Plantear las acciones que se ejecutarán en el momento dado que un sismo se efectúe a fin de minimizar el tiempo de interrupción de las actividades cotidianas de la empresa evitando exponer la integridad física del personal.

c. Criticidad

La empresa determina que el evento ya mencionado produce un gran impacto para la empresa por lo tanto se identifica como crítico.

d. Entorno

Este evento se da en las instalaciones de la empresa afectando la alta dirección, direcciones de líneas, y la operatividad de la empresa en su matriz y sucursal.

e. Personal encargado

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración son quienes

deben dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

f. Condiciones de prevención del riesgo

Poseer un plan adecuado de evacuación de la empresa, el mismo que debe ser de conocimiento de todo el personal que labora en la empresa.

El desarrollo de simulacros con la intervención de todo el personal de la empresa en la sede matriz como en las sucursales.

Mantener las salidas libres de obstáculos.

Señalizar todas las salidas.

Señalizar las zonas seguras.

Definir los puntos de reunión en caso de evacuación.

2. Plan de ejecución

a. Eventos que activan la contingencia

Sismo.

El proceso se activará inmediatamente una vez ocurrido el evento.

b. Procesos relacionados antes del evento

Tener la lista de los empleados por Direcciones y/o Oficinas actualizada.

Mantenimiento del orden y limpieza.

Inspecciones diarias de seguridad interna.

Inspecciones trimestrales de seguridad externa.

Realización de simulacros internos en horarios que no afecten las actividades.

c. Personal que autoriza la contingencia

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración pueden activar la contingencia

d. Descripción de las actividades después de activada la contingencia

Inhabilitación del fluido eléctrico y cierre de las llaves de agua.

Evacuar las oficinas de acuerdo al director administrativo empleando las rutas previamente establecidas durante los simulacros, considerando las escaleras de emergencia, zonas de agrupamiento del personal, señalización de rutas, etc.

Estrictamente prohibido el uso de ascensores

Verificar la integridad de todo el personal que labora en la empresa.

Brindar primeros auxilios al personal en el caso de ser necesario.

Alejarse de las ventanas o archiveros para evitar cortes por el desprendimiento de vidrios.

Evaluación de daños provocados por el sismo en las instalaciones físicas, ambientes de trabajo, estantería, documentos, instalaciones eléctricas, etc. En el caso de ser necesario se empleará personal especializado (defensa civil), esto debe estar controlado por la coordinación ejecutora del plan.

Inventario general del personal, equipos, documentos entre otros recursos afectados indicando el estado de operatividad de los mismos.

Limpieza de las instalaciones

La coordinación ejecutora del plan de contingencia coordinará con la alta dirección de la empresa en el caso que fuera necesario improvisar ambientes de trabajo para retomar el normal funcionamiento de la empresa.

e. Duración

Los procesos de evacuación del personal de la empresa serán calmados y demorará 5 minutos como máximo.

La duración total del evento dependerá del grado del sismo, la probabilidad de replicas y los daños a la infraestructura.

3. Plan de recuperación

a. Personal encargado

El personal encargado del Plan de Recuperación es la Jefatura y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Institución.

b. Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible la producción pendiente durante la interrupción del servicio.

c. Mecanismo de comprobación

El Director y/o Jefe del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte del Servicio u operaciones ha sido afectada y cuáles son las acciones tomadas.

d. Mecanismo de recuperación

El Director y/o Jefe del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte del Servicio u operaciones ha sido afectada y cuáles son las acciones tomadas.

e. Desactivación del plan de contingencia

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

f. Proceso de actualización

El proceso de actualización será en base al informe presentado por El Director de Administración quien determinará las acciones a tomar.

Evento: ***Incendio***

1. Plan de prevención

a. Descripción del evento

Un incendio es un evento de fuego no controlado que puede perjudicar objetos que no están destinados a quemarse. El mismo que puede afectar estructuras, seres vivos y objetos. Es producido en materiales sólidos o líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.

Esta ocurrencia compromete los siguientes elementos mínimos identificados por la empresa, los mismos que pueden ser comprometidos por la contingencia.

Infraestructura

"Centro de datos" local matriz

"Centro de datos" local sucursal

Recursos Humanos

Personal debidamente capacitado para afrontar la contingencia

b. Criticidad

La empresa establece que el presente evento es de alto impacto en la operatividad de la empresa, por lo tanto es planteado como CRITICO.

c. Entorno

Es probable que dicho evento pueda darse en la instalación matriz como en la sucursal.

d. Personal encargado

El Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración, son quienes deben hacer cumplir lo descrito en las condiciones de prevención de riesgo del presente plan.

e. Condiciones de prevención del riesgo

Llevar a cabo periódicamente inspecciones de seguridad.

- Capacitación del uso de extintores de cada uno de sus tipos instalados en la empresa.
- Mantener las instalaciones eléctricas dentro del rango de su vida útil.

- Acatar las indicaciones de la Defensa Civil, con respecto al evento.
- Contar con una lista de números de emergencia, la misma que contenga los números de: Bomberos, Cruz roja y personal de la empresa responsable encargada de las acciones y prevención de la contingencia.

De la misma manera se debe contar con los siguientes componentes para la detección y extinción de un posible incendio, los mismos que cubren las instalaciones del "Centro de Datos" y ambientes afines a centros de información de la empresa.

- Implementar detectores de humo en el "centro de Datos"
- Mantener los extintores en optimas condiciones
- Implementar paredes protectoras de fuego alrededor del "Centro de Datos" para evitar fuego originado en las áreas adyacentes
- Instalar monitores y alarmas eficientes

2. Plan de ejecución

a. Eventos que activan la contingencia

La Contingencia se activará al ocurrir un incendio.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos relacionados antes del evento

Identificar la ubicación de las estaciones manuales de alarma contra incendio.

Identificar la ubicación de los extintores.

Conocer el número de emergencia del Departamento de seguridad y Vigilancia de la empresa.

Tener números de teléfono del personal responsable en seguridad Informática y contingencia de la empresa.

Conocer el número de emergencia de los bomberos.

c. Personal que autoriza la contingencia

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración o sus Representantes pueden activar la contingencia.

d. Descripción de las actividades después de activada la contingencia

Tratar de apagar el incendio con extintores.

Comunicar al personal responsable de la empresa.

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.

En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de la empresa en caso que se requiera la habilitación de

ambientes provisionales alternos para restablecer la función de los ambientes afectados.

e. 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 la Dirección Administrativa y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la empresa

b. Descripción

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

c. Mecanismo de comprobación

El Jefe y/o Director del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

d. Mecanismo de recuperación

Se efectuará de acuerdo a las instrucciones impartidas que se menciona en el punto 1 literal a.

e. Desactivación del plan de contingencia

Director de Administración, Director(a) o sus representantes desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

f. Proceso de actualización

El proceso de actualización será en base al informe presentado por el Director de Administración luego de lo cual se determinará las acciones a tomar.

Evento: ***Inundación por fallo en las tuberías o servicio sanitario***

1. Plan de prevención

a. Descripción del evento

Se da por fallas en las tuberías o sistema de drenaje sanitario,

b. Objetivo

Establece las acciones que se tomarán ante una fuga de agua en las instalaciones, con el fin de minimizar el tiempo de interrupción del servicio brindado por la empresa.

c. Criticidad

El nivel de este evento es considerado CRÍTICO.

d. Entorno

Este evento se da en las instalaciones de la empresa afectando la alta dirección, direcciones de líneas, y la operatividad de la empresa en su matriz y sucursal.

e. Personal encargado

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración son quienes deben de dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

f. Condiciones de prevención del riesgo

Al interior del Centro de Cómputo se dispondrá de sumideros para el desfogue en casos de derrame de agua debidamente mantenidos por el Departamento.

Mantener cubiertas debidamente adecuadas para evitar filtraciones al centro de cómputo, de igual manera aislar las puertas para evitar que el agua entre al centro de cómputo.

2. Plan de ejecución

a. Eventos que activan la contingencia

Inundación.

Este evento se activa una vez se localiza una fuga o la explosión de alguna tubería interna.

b. Procesos relacionados antes del evento

Todos los procesos que afecten la operatividad de la empresa.

c. Personal que autoriza la contingencia

Director administrativo, Director de Tecnologías y Sistemas Informáticos.

d. Descripción de las actividades después de activada la contingencia

Inhabilitación del fluido eléctrico.

Informar al Director administrativo de la fuga o filtración de agua.

Retirar el agua mediante sistemas de bombeo

Evaluar los daños ocasionados en los equipos e instalaciones.

Realizar un inventario general de la documentación y equipos afectados.

e. Duración

La duración del evento dependerá del tamaño de la fuga o filtración.

3. Plan de recuperación

a. Personal encargado

La persona encargada del plan de recuperación es el Director administrativo.

b. Descripción

Una vez controlado el evento las actividades regresan a su normalidad.

c. Mecanismo de comprobación

El director administrativo presenta un informe de que áreas fueron las afectadas que parte del servicio y que acciones fueron realizadas.

d. Desactivación del plan de contingencia

El Director de Administrativo desactivará el Plan de Contingencia una vez que se haya tomado las acciones redactadas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e. Proceso de actualización

El proceso de actualización será en base al informe presentado por El Director de Administración quien determinará las acciones a tomar.

Evento: ***Terremoto***

1. **Plan de prevención**

a. Descripción del evento

Terremoto es un sismo de mayor magnitud es decir es un movimiento que se produce en el interior de la tierra el mismo que libera repentinamente energía la cual es propagada en forma de ondas produciendo el movimiento de la tierra.

Esta eventualidad involucra los siguientes elementos identificados por la empresa los cuales por su naturaleza se pueden considerar como parte afectada o causa del estado de contingencia, tales elementos son mostrados a continuación:

Infraestructura

Sede matriz de la empresa

Sucursal de la empresa

Recursos Humanos

Personal

b. Objetivo

Plantear las acciones que se ejecutarán en el momento dado que un sismo se efectué a fin de minimizar el tiempo de interrupción de las actividades cotidianas de la empresa evitando exponer la integridad física del personal.

c. Criticidad

La empresa determina que el evento ya mencionado produce un gran impacto para la empresa por lo tanto se identifica como crítico.

d. Entorno

Este evento se da en las instalaciones de la empresa afectando la alta dirección, direcciones de líneas, y la operatividad de la empresa en su matriz y sucursal.

e. Personal encargado

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas y/o Director de administración son quienes deben de dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

f. Condiciones de prevención del riesgo

Poseer un plan adecuado de evacuación de la empresa, el mismo que debe ser de conocimiento de todo el personal que labora en la empresa.

El desarrollo de simulacros con la intervención de todo el personal de la empresa tanto en la sede matriz como en las sucursales.

Mantener las salidas libres de obstáculos.

Señalizar todas las salidas.

Señalizar las zonas seguras.

Definir los puntos de reunión en caso de evacuación.

2. Plan de ejecución

a. Eventos que activan la contingencia

Terremoto

El proceso se activará inmediatamente una vez ocurrido el evento.

b. Procesos relacionados antes del evento

Tener la lista de los empleados por Direcciones y/o Oficinas actualizada.

Mantenimiento del orden y limpieza.

Inspecciones diarias de seguridad interna.

Inspecciones trimestrales de seguridad externa.

Realización de simulacros internos en horarios que no afecten las actividades

c. Personal que autoriza la contingencia

El Director Ejecutivo y/o Director de Administración pueden activar la contingencia

d. Descripción de las actividades después de activada la contingencia

Inhabilitación del fluido eléctrico y cierre de las llaves de agua.

Evacuar las oficinas de acuerdo al director administrativo empleando las rutas previamente establecidas durante los simulacros, considerando las escaleras de emergencia, zonas de agrupamiento del personal, señalización de rutas, etc.

Estrictamente prohibido el uso de ascensores

Verificar la integridad de todo el personal que labora en la empresa.

Brindar primeros auxilios al personal en el caso de ser necesario.

Alejarse de las ventanas o archiveros para evitar cortes por el desprendimiento de vidrios.

Evaluación de daños provocados por el terremoto en las instalaciones físicas, ambientes de trabajo, estantería, documentos, instalaciones eléctricas, etc. En el caso de ser necesario se empleará personal especializado (defensa civil), esto debe estar controlado por la coordinación ejecutora del plan.

Inventario general del personal, equipos, documentos entre otros recursos afectados indicando el estado de operatividad de los mismos.

Limpieza de las instalaciones

La coordinación ejecutora del plan de contingencia coordinará con la alta dirección de la empresa en el caso que fuera necesario improvisar ambientes de trabajo para retomar el normal funcionamiento de la empresa.

e. Duración

Los procesos de evacuación del personal de la empresa serán calmados y demorará 5 minutos como máximo.

La duración total del evento dependerá del grado del terremoto, la probabilidad de replicas y los daños a la infraestructura.

3. Plan de recuperación

a. Personal encargado

El personal encargado del Plan de Recuperación es la Jefatura y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Institución.

b. Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible la producción pendiente durante la interrupción del servicio.

c. Mecanismo de comprobación

El Director y/o Jefe del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte del Servicio u operaciones ha sido afectada y cuáles son las acciones tomadas.

d. Mecanismo de recuperación

El Director y/o Jefe del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte del Servicio u operaciones ha sido afectada y cuáles son las acciones tomadas.

e. Desactivación del plan de contingencia

Gerente General, Gerente de Sistemas, Director de administración, y/o Director de Tecnologías y Sistemas Informáticos desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

f. Proceso de actualización

El proceso de actualización será en base al informe presentado por El Director de Administración quien determinará las acciones a tomar.

Evento: ***Interrupción del servicio eléctrico***

1. Plan de prevención

a. Descripción del evento

Falla general en el suministro de energía eléctrica.

Los elementos identificados por la empresa que por su naturaleza pueden ser afectados o causantes de dicha contingencia.

Servicios Públicos

- Suministro de Energía Eléctrica

Hardware

- Servidores
- Estaciones de Trabajo

Equipos Diversos

- UPS

b. Objetivo

Restablecer la funcionalidad de los servicios considerados como críticos para la empresa.

c. Criticidad

Este evento está considerado como CRÍTICO

d. Entorno

Es probable que se dé el momento menos esperado, afectando el fluido eléctrico y de esta manera interrumpiendo las actividades de la empresa.

e. Personal encargado

El Director de Administración y/o Jefe de Informática de la empresa son las personas encargadas de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

f. Condiciones de prevención del riesgo

Durante el desarrollo de las actividades cotidianas de la empresa se contará con los UPS necesarios que aseguren el suministro de energía en los puestos de trabajo considerados críticos para la empresa.

Asegurar que los UPS's reciban el mantenimiento adecuado y que cuenten con la carga necesaria para soportar una operación continua de 30 minutos, el tiempo puede ser variable de acuerdo a la función que realizan los UPS's.

Ejecutar periódicamente pruebas en los UPS's para asegurar el funcionamiento de los mismos.

Contar con UPS's para suministrar energía a los servidores previniendo así la perdida de datos y servicios durante las labores.

Los UPS's deben poseer una autonomía no menor a 30 minutos.

Los equipos de vigilancia y de control de acceso de la empresa deben estar suministrados por un UPS.

Instalar luces de emergencia con una carga mínima de 15 minutos, y cuya activación sea automáticamente una vez exista un corte de energía.

2. Plan de ejecución

a. Eventos que activan la contingencia

La suspensión del servicio eléctrico en las instalaciones de la empresa.

b. Procesos relacionados antes del evento

Todas las actividades de servicios en la empresa.

c. Personal que autoriza la contingencia

El Director de administración y/o Jefe de Informática pueden activar la contingencia.

d. Descripción de las actividades después de activada la contingencia

Se procede a informar al Director Administrativo y/o jefe de informática de los inconvenientes presentados.

Dar a conocer al personal de todas las áreas de la empresa que se suscito un corte de energía, para tomar las acciones necesarias.

En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.

En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores hasta que regrese el fluido eléctrico.

e. Duración

El tiempo de duración de la contingencia es variable dependiendo del proveedor del servicio.

3. Plan de recuperación

a. Personal encargado

Las personas encargadas del Plan de Recuperación son el director de administración y/o el jefe de informática quienes serán los encargados en realizar las acciones necesarias.

b. Descripción

Si el caso lo amerita el evento debe ser evaluado y registrado en el formato de ocurrencia de eventos

Se informará a la coordinación ejecutora del plan el problema y los procedimientos empleados para atender el problema.

c. Mecanismo de comprobación

El Director de Administración y/o Jefe de Informática presentará un informe a la Coordinación Ejecutora del Plan dando a conocer que partes de servicio, operación o actividades fallaron y cuáles son las soluciones preventivas o correctivas a realizar.

d. Desactivación del plan de contingencia

El Director de Administración y/o Jefe de Informática desactivará el Plan de Contingencia una vez el suministro eléctrico funcione con normalidad.

e. Proceso de actualización

En base al informe que describe los problemas presentados, determinarán las acciones de prevención a tomar.

- ***Subfactor: Contingencias relacionadas a los sistemas de información***

A. Objetivo

Los planes de contingencia relacionados a este subfactor tienen como objetivo disponer de alternativas de solución frente a cualquier evento que pueda perjudicar el normal funcionamiento del hardware o software ya sea un factor interno o externo relacionado al mismo, asegurado la operatividad o reduciendo el tiempo de interrupción.

B. Alcance

El alcance de dicho plan esta ajustado al uso de los sistemas y de las aplicaciones empleadas por la empresa.

A continuación se indica un resumen de la matriz de riesgos, tomando en cuenta las contingencias relacionadas a los Sistemas de Información.

Código	Descripción del evento de contingencia	Probabilidad de ocurrencia	impacto	Ponderación	Alerta
SUBFACTOR: Contingencia relacionada a Sistemas de información					
	Información				
FrPlC -10	Perdida de documentos	0.02	3	0.06	
FrPlC -11	Robo o sustracción de información	0.02	3	0.06	
	Software				
FrPlC -12	Perdida del sistema central	0.05	4	0.2	R
FrPlC -13	Virus en los equipos	0.05	4	0.2	R
FrPlC -14	Perdida del servidor de correo	0.01	2	0.02	
FrPlC -15	Fallo en el motor de base de datos	0.04	4	0.16	R
FrPlC -16	Fallas en el sistema operativo	0.04	4	0.16	R
	Comunicación				
FrPlC -17	Daño en la red de datos	0.02	4	0.08	
	Hardware				
FrPlC -18	Avería de los pc´s Recursos operativos y logísticos	0.02	2	0.04	
FrPlC -19	Daño en los equipos multimedia, impresoras, scanner's y otros	0.01	2	0.02	

Grafico 43: Subfactor Contingencias relacionadas a los sistemas de información

C. Plan de pruebas

El plan de pruebas corresponde al desarrollo de los eventos como parte del Subfactor de Sistemas de Información, siguiendo con la metodología expuesta en el plan de contingencia.

Un plan de pruebas es determinado posterior al análisis de los procesos críticos del servicio y de la identificación de los eventos que pudieran presentarse. El

comité de contingencia es el encargado de la aprobación del plan de pruebas luego de efectuar dicha prueba.

D. Descripción de Planes

Los eventos identificados en la matriz de riesgo de contingencia se presentan a continuación.

Evento: ***Perdida del sistema central***

1. **Plan de prevención**

a. Descripción del evento

Es la falta de interacción de Hardware y Software que hace inoperativa la máquina, es decir el hardware no recibe instrucciones del software haciendo imposible el funcionamiento.

Para este evento se han identificado los elementos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Software

Software base

Software base de datos

Hardware

Servidores Información

Respaldo de base de datos

Respaldo de las aplicaciones utilizadas por la empresa

Respaldo de Software Base .

b. Objetivo

Mantener la operatividad de los servidores en donde se ejecutan las aplicaciones de la empresa.

c. Criticidad

Es un evento considerado crítico.

d. Entorno

Los servidores deben estar situados en el data center de la empresa

e. Personal encargado

El responsable de asegurar el correcto funcionamiento de los servidores es el Director de Tecnologías y Sistemas Informáticos, el coordinará las acciones pertinentes para restablecer los servicios en caso de que se presente algún evento.

f. Condiciones de prevención del riesgo

Implementar acciones preventivas en la Unidad de Informática de dicha empresa para asegurar el servicio de las aplicaciones usadas en la empresa:

Poseer equipos de respaldo para garantizar la disponibilidad de los servicios.

Brindar mantenimiento preventivo a los equipos.

Poseer backups de la información pertinente para restablecer las aplicaciones Anexo “An3: Copias de Respaldo”

Disponer de backups de las aplicaciones y bases de datos véase el Anexo "An3: Copias de Respaldo"

Almacenar en un lugar seguro los backups referidos a aplicaciones.

Es recomendable almacenar los respaldos fuera de las instalaciones de la empresa.

2. Plan de ejecución

a. Eventos que activan la contingencia

Imperfecciones en el acceso a aplicaciones

Daño en la conexión a la base de datos.

b. Procesos relacionados antes del evento

Todos los procesos que tengan relación con el uso de las aplicaciones en los servidores de la empresa

c. Personal que autoriza la contingencia

Director de Tecnologías y Sistemas Informáticos

d. Descripción de las actividades después de activada la contingencia

Acogerse a los procedimientos de recuperación de sistemas planteados por la empresa.

e. Duración

El tiempo de duración está basado en la complejidad del problema presentado. Se esperan indicaciones del Director de Tecnologías y Sistemas Informáticos para reanudar las operaciones.

3. Plan de recuperación

a. Personal encargado

El Director de Tecnologías y Sistemas Informáticos, luego de verificar la solución del problema en los servidores se coordinará con los jefes de área para la inmediata reanudación de las operaciones.

b. Descripción

Se informa a la alta dirección lo que originó la paralización de los servicios. En función de esto se toman las medidas del caso y se revisa el plan de contingencia para actualizarlo en el caso de que sea necesario.

c. Mecanismo de comprobación

Se procede a llenar el formato de ocurrencia de evento y se envían a la coordinación ejecutora del plan para la revisión.

d. Desactivación del plan de contingencia

Con el permiso del Director de Tecnologías y Sistemas Informáticos el plan se procederá a la desactivación del mismo.

e. Proceso de actualización

En el supuesto caso de que exista información que no conste acerca de los sistemas centrales, se coordina con el director para iniciar con las labores de actualización de los sistemas

Evento: ***Virus en los equipos***

1. **Plan de prevención**

a. Descripción del evento

Un virus informático es un programa computacional que es propagado de un computador a otro el mismo que interfiere con el normal funcionamiento de los equipos, incluso eliminando o dañando información del computador.

Esta ocurrencia compromete los siguientes elementos mínimos identificados por la empresa, los mismos que pueden ser comprometidos por la contingencia.

Hardware

Software

Servidores

Software Base

Estaciones de Trabajo

Aplicativos utilizados por la empresa

b. Objetivo

Restablecer el funcionamiento de los equipos luego de eliminados los virus o reinstalación de programas afectados.

c. Criticidad

El nivel de éste evento es considerado CRÍTICO.

d. Entorno

Las computadoras se encuentran instaladas en la matriz y en la sucursal de la empresa.

e. Personal encargado

Director de Tecnologías y Sistemas Informáticos y/o Jefe de Departamento de Soporte Técnico son los encargados de la supervisión de los equipos informáticos funcionen correctamente.

f. Condiciones de prevención del riesgo

Establecer las políticas de seguridad para prevenir la instalación de aplicaciones maliciosas en las estaciones de trabajo.

Restringir el acceso a internet en las estaciones de trabajo que por su uso no lo requieren.

Suspender unidades de CD y lectores de tarjetas en equipos que no son necesarios.

Deshabilitar los puertos USB en las estaciones de trabajo que no son requeridos, evitando así la conexión de dispositivos de almacenamiento externo.

Implementar filtros de correo entrante y revisión de archivos adjuntos en los correos evitando así la infección de las terminales de trabajo.

Instalar antivirus en cada estación de trabajo, el mismo que debe mantenerse actualizado permanentemente.

Contar con equipos de respaldo los mismos que remplazaran

provisionalmente a las estaciones afectadas.

2. Plan de ejecución

a. Eventos que activan la contingencia

Acceso lento a las aplicaciones.

Mensajes de error del sistema operativo ó durante la ejecución de programas.

Falla general en el equipo.

b. Procesos relacionados antes del evento

Todos los procesos relacionados con el uso de aplicaciones en las estaciones de trabajo.

c. Personal que autoriza la contingencia

Director de Tecnologías y Sistemas Informáticos, Jefe de Departamento de Desarrollo de Sistemas, Jefe de Departamento de Soporte Técnico y/o Jefe de Departamento de Comunicaciones

d. Descripción de las actividades después de activada la contingencia

Separar el equipo infectado de la red de la empresa.

Verificar si el equipo está infectado, empleando detectores de virus actualizados.

Si el caso lo amerita rastrear el origen de la infección (correo electrónico, archivo infectado, entre otros).

Eliminar los archivos causantes de la infección.

Remover el virus del sistema

Poner a prueba el sistema

Si el problema persiste:

Formatear el equipo

Personalizar la estación para el usuario

Conectar la estación a la red de la empresa.

Efectuar las pruebas necesarias con el usuario.

e. Duración

El evento no deberá tener un tiempo mayor a DOS hora en el caso de que se confirmara la presencia de virus.

3. Plan de recuperación

a. Personal encargado

El Jefe de Departamento de Soporte Técnico asignará a un técnico para la reparación del computador y coordinará con el usuario o responsable del área para reanudar el trabajo en equipo.

b. Descripción

Se informará al Director de Tecnologías y Sistemas Informáticos de la empresa el tipo de virus encontrado y los procedimientos empleados para removerlos. En función de esto se tomarán las medidas preventivas del caso dando a conocer al personal de la empresa mediante correo interno dichas medidas. El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c. Mecanismo de comprobación

Será llenado en el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

d. Mecanismo de recuperación

Con el aviso del departamento técnico de sistemas de la empresa, se procede a la desactivación del plan.

e. Proceso de actualización

La infección presentada en las estaciones de trabajo, no debe paralizar la aplicación de actualización de datos en las aplicaciones de la empresa.

Evento: ***Fallo en el motor de base de datos***

1. Plan de prevención

a. Descripción del evento

Daño en el servicio principal para almacenar, procesar y proteger los datos de las transacciones realizadas por la empresa.

Esta eventualidad involucra los siguientes elementos identificados por la empresa los cuales por su naturaleza se pueden considerar como parte afectada o causa del estado de contingencia, tales elementos son mostrados a continuación:

Software

Aplicativos utilizados por la empresa

Respaldo de Base de Datos

Respaldo del Software Base

Hardware

Servidores de Información

b. Objetivo

Asegurar la disponibilidad de los servicios, con los medios de respaldos adecuados para restaurar los datos de las aplicaciones de los servidores centrales.

c. Criticidad

Este evento se considera como CRÍTICO.

d. Entorno

Es producido en el data center de la empresa durante la ejecución de los servicios, afectando a las aplicaciones empleadas para soportar el funcionamiento de la empresa.

e. Personal encargado

El Gerente de Sistemas es el encargado en designar al responsable de la base de datos.

f. Condiciones de prevención del riesgo

Realizar revisiones periódicas de los logs de la Base de Datos evitando así el mal funcionamiento de la misma.

Realizar backups diariamente de los datos de aplicaciones en desarrollo o producción de la empresa, esto se realiza con la finalidad de asegurar la información almacenada en la base de datos.

Las copias de seguridad de la información son procesos diarios, las cuales buscan asegurar la integridad de la información. Por otro lado se pueden obtener copias de seguridad de la base de datos después o antes de un determinado proceso Anexo An3: Copias de respaldo.

Mantener debidamente actualizado el software de gestor de base de datos, parchado adecuadamente según especificaciones del fabricante del producto.

Contar con servicios de soporte vigentes para el software de gestión de BD. En caso sea necesario, este soporte debe incluir actividades de prevención, revisión del sistema y mantenimiento general a la base de datos.

2. Plan de ejecución

a. Eventos que activan la contingencia

Defecto en las conexiones

Sistema aplicativo no disponible

Visualización de errores en las pantallas de las estaciones de trabajo y/o servidores.

b. Procesos relacionados antes del evento

Disponibilidad de respaldos en los servidores de la empresa.

c. Personal que autoriza la contingencia

El Director de Tecnologías y Sistemas Informáticos es quien considera la activación de la contingencia.

d. Descripción de las actividades después de activada la contingencia

Sistemas desarrollados por la empresa.- En el momento de producirse una falla en la operación de los sistemas el Director de Sistemas de Informática asumirá, delegará o coordinará los trabajos de corrección o modificación.

Sistemas de Proveedores.- En el momento de producirse una falla en la operación de los sistemas se deberá informar directamente a los proveedores del sistema cliente o base de datos.

e. Duración

La contingencia no podrá exceder el periodo de CINCO horas.

3. Plan de recuperación

a. Personal encargado

El Director de Tecnologías y Sistemas Informáticos es el encargado del plan de recuperación de las operaciones.

b. Descripción

Se le informará al Director de Tecnologías y Sistemas Informáticos de la empresa los causantes del problema suscitado y las acciones usadas para atender el problema. En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo interno al personal de la empresa.

Dichos eventos serán evaluados y registrados si el caso lo amerita en el formato de ocurrencia de eventos.

c. Mecanismo de comprobación

El Director de Tecnologías y Sistemas Informáticos de la empresa dará a conocer el informe a la coordinación ejecutora del plan, indicando de la manera más clara que parte del Sistema ha fallado y que medidas correctivas o preventivas se tomaron.

d. Desactivación del plan de contingencia

El Director de Tecnologías y Sistemas Informáticos de la empresa desactivará el plan de contingencia una vez recuperada la funcionalidad del sistema, base de datos y aplicaciones.

e. Proceso de actualización

Basándose en el informe que indica las causas de la perdida del sistema operativo en estaciones de trabajo o servidores, se determinará las acciones preventivas necesarias que deberá contener el plan.

Si el caso lo amerita y existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o jefes de áreas, para iniciar las labores de actualización de los sistemas.

Evento: ***Fallos en el sistema operativo***

1. **Plan de prevención**

    a. Descripción del evento

    Fallo en el manejo de las computadoras, en la coordinación hombre-máquina. Para este evento se han identificado los elementos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

    Software

    Aplicativos utilizados por la empresa

    Respaldo de Base de Datos

    Respaldo de las Aplicaciones utilizadas por la empresa

    Hardware

    Servidores de Información

b. Objetivo

Asegurar la persistencia de las operaciones, empleando medios de respaldos adecuados para la restauración de los elementos afectados.

c. Criticidad

Este evento se considera como CRÍTICO.

d. Entorno

Puede producirse durante la operatividad, involucrando estaciones de trabajo y servidores.

e. Personal encargado

El Director de Tecnologías y Sistemas Informáticos de la empresa es el encargado de coordinar todas las acciones necesarias para mantener el correcto funcionamiento de las aplicaciones.

f. Condiciones de prevención del riesgo

Se deben cumplir los siguientes aspectos necesarios:

Contar con los respectivos backups de datos de las aplicaciones usadas por la institución Anexo An3: Copias de respaldo.

Contar con los debidos soportes para los causantes del evento.

Mantener acuerdos con los proveedores de servicios.

Contar con revisiones periódicas de los logs de actividad de los servidores para evitar inconvenientes.

2. Plan de ejecución

a. Eventos que activan la contingencia

Identificar las funciones de cada una de las áreas de trabajo y servidores.

Detección de fallas en el monitor de servidores y áreas de trabajo.

b. Procesos relacionados antes del evento

Disponibilidad de los respaldos de los sistemas para la ejecución de aplicaciones en los servidores.

c. Personal que autoriza la contingencia

El Director de Tecnologías y Sistemas Informáticos es que considera activar la contingencia.

d. Descripción de las actividades después de activada la contingencia

En las estaciones de trabajo:

Revisión de las estaciones de trabajo para identificar lo que está causando la falla.

Verificar si el equipo no se encuentra infectado por virus (revisar Evento: Virus en los equipos)

Probar el sistema.

Realizar pruebas con el usuario.

Solicitar conformidad del servicio.

En los servidores:

Reportar el problema al área de soporte técnico.

Coordinar las acciones a realizarse y plantear un tiempo aproximado de interrupción del servicio.

Comunicar a los directores o jefes de área para que tomen las debidas acciones del caso para evitar afecciones en las operaciones.

e. Duración

La contingencia no debe sobrepasar un periodo máximo de CINCO horas

3. Plan de recuperación

a. Personal encargado

El Director de Tecnologías y Sistemas Informáticos es el encargado del plan de recuperación de las operaciones.

b. Descripción

Se informará al Director de Tecnologías y Sistemas Informáticos de la empresa el causante del problema presentando y los procedimientos empleados para atender el problema. Sabiendo esto se procederá a tomar las medidas correctivas y preventivas pertinentes enviando una alerta vía correo interno al personal de la empresa.

Se evaluará y registrará el evento si es necesario en el formato de ocurrencia de eventos.

c. Mecanismo de comprobación

El Director de Tecnologías y Sistemas Informáticos de la empresa presentará un informe a la coordinación ejecutora del plan, exponiendo que partes del servicio son las que fallaron y que medidas preventivas o correctivas se emplearon.

d. Desactivación del plan de contingencia

El Director de Tecnologías y Sistemas Informáticos de la empresa desactivará el plan de contingencia una vez sea recuperada la funcionalidad de trabajo.

e. Proceso de actualización

Basándose en el informe presentado que identificó las causantes de la perdida del sistema en las estaciones de trabajo y servidores.

En el caso de que exista información pendiente de actualización, debido a la falla en el sistema central, los directores y jefes de área coordinarán las labores de actualización de los sistemas.

- ***Subfactor: Contingencias relacionadas a los Recursos Humanos***

A. Objetivo

Este tipo de contingencias están ligados a los elementos y factores que puedan sufrir alguna afección por parte del personal de la empresa.

B. Alcance

La seguridad referente al personal es contemplada desde la etapa de selección del mismo y se incluirá en el contrato la definición de puestos de trabajo para reducir los riesgos de:

- Incapacidad temporal o permanente
- Indisponibilidad por enfermedad
- Emergencias médicas
- Renuncias o ceses

La definición de puestos de trabajo debe contemplar todo lo necesario en cuanto a responsabilidades encomendadas.

A continuación se indica un resumen de la matriz de riesgos, tomando en cuenta las contingencias relacionadas a los Recursos Humanos

Código	Descripción del evento de contingencia	Probabilidad de ocurrencia	impacto	Ponderación	Alerta
SUBFACTOR: Contingencia relacionada a Recursos humanos					
	Recursos humanos				
FrPlC -20	Ausencias imprevista del personal de soporte técnico	0.05	3	0.15	R
FrPlC -21	Ausencia de personal ejecutivo para la toma decisiones ante situaciones de riesgo informático	0.05	3	0.15	R
FrPlC -22	Falta de capacidad del personal en la reserva de información en la DB	0.01	4	0.04	

Grafico 44*:* Subfactor Contingencias relacionadas a los Recursos Humanos

C. Plan de pruebas

El plan de pruebas corresponde al desarrollo de los eventos como parte del Subfactor de Recursos Humanos, siguiendo con la metodología expuesta en el plan contingencia.

Un plan de pruebas es determinado posterior al análisis de los procesos críticos del servicio y de la identificación de los eventos que pudieran presentarse. La alta dirección de la empresa será la encargada de la aprobación del plan de pruebas previa ejecución.

D. Descripción de Planes

Los eventos identificados en la matriz de riesgo de contingencia se presentan a continuación.

Evento: ***Ausencias imprevista del personal de soporte técnico***

1. **Plan de prevención**

a. Descripción del evento

La ausencia de personal de soporte relevante (enfermedad, renuncias, ceses), que es personal clave que garantice el funcionamiento de redes de datos, servidores y estaciones de trabajo.

Para este evento se han identificado los elementos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Recursos Humanos

Personal

b. Objetivo

Garantizar la disponibilidad de los servicios informáticos de la empresa.

c. Criticidad

Este evento se considera como CRÍTICO para la empresa.

d. Entorno

Dicho evento se presenta en la instalación matriz como en las sucursales de la empresa

e. Personal encargado

El Director de Tecnologías y Sistemas Informáticos y/o Los jefes de los distintos departamentos de sistemas son quienes dispondrán que se cumplan las condiciones de prevención de riesgo del plan.

f. Condiciones de prevención del riesgo

Este evento puede producirse en cualquier instante dependiendo de las circunstancias personales por lo que se considera lo siguiente:

Contar con personal capacitado en las áreas de soporte, desarrollo y comunicaciones que cumplan con el perfil, conocimientos y capacidad de remplazar ausencias en el personal.

El Gerente de Sistemas debe asegurarse en tener como mínimo dos profesionales técnicos y un asistente.

El personal debe comunicar con anticipación la inasistencia o abandono de centro de labores.

Para el control del personal se cuenta con un software de control de asistencia, de donde se proveerá información al Gerente de Sistemas, para que tome las acciones preventivas correspondientes.

2. Plan de ejecución

a. Eventos que activan la contingencia

Reporte de inasistencia del personal de las áreas de sistemas:

Administrador de la red

Soporte técnico

Helpdesk

Administrador de la base de datos

La contingencia se activará durante las DOS primeras horas de labores..

b. Procesos relacionados antes del evento

Conocimiento del Gerente de Sistemas por informe escrito del personal.

Conocimiento del Gerente de Sistemas por informe telefónico.

Conocimiento del Gerente de Sistemas por alerta del sistema de control de asistencia.

c. Personal que autoriza la contingencia

El Gerente de Sistemas.

d. Descripción de las actividades después de activada la contingencia

Una vez confirmada la inasistencia del personal de soporte el Gerente de sistemas asignará a alguien del área de sistemas a remplazar en las funciones a la persona titular. El Jefe de Informática solicitará al Director Ejecutivo de la empresa, el reemplazo del personal.

e. Duración

Tiene un periodo máximo de OCHO horas. El fin de dicho evento es la presencia del remplazo el mismo que asume la responsabilidad hasta la reincorporación del personal, en caso de una renuncia o fuerza mayor.

Máximo OCHO (08) horas. El fin del presente evento es la presencia del reemplazo que asume la responsabilidad; hasta que se confirme la presencia del personal de Soporte Técnico en caso de renuncia u otras por fuerza mayor.

3. Plan de recuperación

a. Personal encargado

El Director de Tecnologías y Sistemas Informáticos es la persona encargada del plan de recuperación cuya función es garantizar una alta disponibilidad del servicio informático.

b. Descripción

Control permanente de los servicios atendidos si fuera el caso.

Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

Regularizar los servicios pendientes mientras el personal está ausente.

c. Mecanismo de comprobación

El Director de Tecnologías y Sistemas Informáticos presentará un informe a la coordinación ejecutora del plan dando a conocer las partes del servicio afectadas y que acciones se tomaron.

d. Desactivación del plan de contingencia

El Director de Tecnologías y Sistemas Informáticos desactivará el plan una vez tomadas las acciones necesarias descritas en el plan de recuperación.

e. Proceso de actualización

Basándose en el informe pasado al Director de Tecnologías y Sistemas Informáticos y las causas identificadas en el servicio informático se determinan las acciones a tomar.

Evento: ***Ausencia de personal ejecutivo para la toma decisiones ante situaciones de riesgo informático***

1. Plan de prevención

a. Descripción del evento

La ausencia de los directivos o jefes de las distintas áreas por diversos motivos como son: enfermedad, renuncia, calamidad domestica, entre otros, que son personas clave para la toma de decisiones que garantizan el normal funcionamiento de las actividades.

Esta ocurrencia compromete los siguientes elementos mínimos identificados

por la empresa, los mismos que pueden ser comprometidos por la contingencia.

Recursos Humanos

Personal

b. Objetivo

Fortalecer la continuidad del normal funcionamiento en las diferentes gerencias, direcciones o jefaturas de la empresa, evitando el quiebre de la cadena de mandos, implementando remplazos del personal ejecutivo.

c. Criticidad

La empresa establece que el presente evento es de alto impacto en la tolerabilidad de la empresa, por lo tanto es planteado como CRÍTICO.

d. Entorno

Este evento se puede dar en las instalaciones de la Alta Dirección, Sede matriz y sucursal

e. Personal encargado

El directorio ejecutivo es el encargado en hacer cumplir lo descrito en la prevención de riego del presente plan.

f. Condiciones de prevención del riesgo

El evento puede hacerse presente en cualquier instante dependiendo de las circunstancias de cada persona por lo que se considera lo siguiente:

La alta dirección asegurará la capacitación de un empleado con una experiencia mayor a 5 años en la empresa que cumpla con el perfil profesional, conocimientos para que sustituya al personal mientras se

da el evento.

Como parte de las funciones del personal incluir la comunicación anticipada de la inasistencia al centro de labores.

2. Plan de ejecución

a. Eventos que activan la contingencia

El proceso de contingencia es activado durante las DOS horas iniciales del día, una vez recibido el reporte de inasistencia de directores o jefes.

b. Procesos relacionados antes del evento

Se da por la falta de decisión de parte de los directores o jefes de área para dar solución ante algún inconveniente en las actividades de la empresa.

c. Personal que autoriza la contingencia

El encargado de autorizar el proceso de contingencia es el Director Administrativo.

d. Descripción de las actividades después de activada la contingencia

Una vez confirmada la inasistencia de directores, se coordina el remplazo con la gerencia de la empresa.

Confirmada la inasistencia de jefes de área, el Director de área coordinará con los directores el remplazo correspondiente.

e. Duración

La duración máxima del plan es de TRES horas, y el fin del mismo es el remplazo correspondiente o a su vez que se confirme la presencia del director o jefe de área en caso de renuncia o fuerza mayor.

3. Plan de recuperación

a. Personal encargado

El Director o jefe de área es la persona encargada del plan de recuperación, cuyo rol principal es de asegurar el normal desarrollo de las funciones de la empresa.

b. Descripción

Regularizar la coordinación pendiente durante la ausencia.

Delimitar los ajustes que permitan asegurar una rápida prevención del evento.

c. Mecanismo de comprobación

El Director o jefe de área presenta el informe a la coordinación ejecutora del plan dando a conocer que parte del servicio fue afectado y que acciones se tomaron.

d. Desactivación del plan de contingencia

El Gerente administrativo desactivará el plan de contingencia una vez realizadas las acciones necesarias presentadas en la descripción del presente plan de recuperación.

e. Proceso de actualización

El proceso de actualización será en base al informe presentado por El Director de Administración quien determinará las acciones a tomar.

- ***Subfactor: Contingencias relacionadas a Seguridad Física***

A. Objetivo

Limitar acciones de prevención con el fin de mitigar o eliminar riesgos que puedan afectar la integridad física tanto de instalaciones como de los elementos

que operan dentro de la institución(mobiliario, información, equipos, etc.), por motivos de incidentes causados de manera intencional, eventual o natural y que puedan afectar la operación normal de la empresa.

B. Alcance

Se tomarán en cuenta los siguientes elementos:

Ubicación

Disposición física

Elementos de seguridad de los ambientes de trabajo

Control de accesos de personal interno y externo a la empresa

Actos de vandalismo o terroristas que pudieran afectar la infraestructura, personal o la documentación.

A continuación se indica un resumen de la matriz de riesgos, tomando en cuenta las contingencias relacionadas a los Seguridad Física.

Código	**Descripción del evento de contingencia**	**Probabilidad de ocurrencia**	**impacto**	**Ponderación**	**Alerta**
SUBFACTOR: Plan de seguridad física					
	Infraestructura				
FrPlC -23	Sustracción de equipos y software diversos	0.05	4	0.2	R
FrPlC -24	Sabotaje	0.01	2	0.02	
FrPlC -25	Vandalismo	0.01	3	0.03	
FrPlC -26	Actos terroristas	0.01	1	0.01	

Grafico 45*:* Subfactor Contingencias relacionadas a Seguridad Física

C. Plan de pruebas

El plan de pruebas corresponde al desarrollo de los eventos como parte del Subfactor de Seguridad Física, siguiendo con la metodología expuesta en el plan de contingencia.

Un plan de pruebas es posteriormente determinado al análisis de los procesos críticos del servicio y de la identificación de los eventos que pudieran presentarse. La alta dirección de la empresa son los encargados de la aprobación del plan de pruebas luego de efectuar dicha prueba.

D. Descripción de Planes

Los eventos identificados en la matriz de riesgo de contingencia se presentan a continuación.

Evento: ***Sustracción de equipos y software diversos***

1. **Plan de prevención**

    a. Descripción del evento

    Sustracción de equipos y software diversos:

    Hurto es el apoderamiento ilegitimo de un bien ajeno, a diferencia del robo es realizado sin emplear la fuerza, violencia o intimidación en las personas.

    Robo la enajenación de bienes, empleando la intimidación, fuerza o violencia hacia las personas.

    Esta ocurrencia compromete los siguientes elementos mínimos identificados por la empresa, los mismos que pueden ser comprometidos por la contingencia.

    Hardware y Software

b. Objetivo

Plantear las acciones que se deben ejecutar al momento de presentarse dicha eventualidad con la finalidad de reducir el impacto de la perdida de información y de los equipos.

c. Criticidad

La empresa establece que el presente evento es de alto impacto en la operatividad de la empresa, por lo tanto es planteado como CRÍTICO.

d. Entorno

La eventualidad puede suscitarse en la sede matriz como en la sucursal

e. Personal encargado

Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas, Director de administración y/o Director de Tecnologías son quienes deben hacer cumplir lo descrito en las condiciones de prevención del riesgo del presente plan.

f. Condiciones de prevención del riesgo

Para la prevención de un posible robo hurto en el Centro de Cómputo, se deberá tomar las acciones necesarias para evitar perdida de equipos e información.

- Disponer de un plan de turnos para brindar soporte, el plan debe estar planificado por la Gerencia y dirección de sistemas conjuntamente, lo que garantizará la continuidad del servicio.
- Organice vigilancia de equipos y materiales restantes del Centro de Cómputo.
- Mantener los respaldos diarios adecuados de toda la información de la empresa.

- Implementar un circuito cerrado de vigilancia para la empresa.
- Seguridad deberá informar al respecto a la Policía con urgencia del caso para tratar de recuperar ante todo la información sustraída.

2. Plan de ejecución

a. Eventos que activan la contingencia

La Contingencia se activará al ocurrir un hurto o robo en las instalaciones.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos relacionados antes del evento

Cualquier proceso relacionado con la perdida de hardware y software en la empresa

c. Personal que autoriza la contingencia

La persona de turno encargada de brindar soporte y cualquier miembro de la empresa.

d. Descripción de las actividades después de activada la contingencia

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

e. Duración

El tiempo de duración está basado en la complejidad del problema presentado. Se esperan indicaciones del Director de Tecnologías y Sistemas Informáticos para reanudar las operaciones.

Las actividades deben reanudarse en un periodo máximo de CUATRO HORAS una vez activado el plan.

3. Plan de recuperación

a. Personal encargado

Las personas encargadas del Plan de Recuperación son el Gerente General, Gerente de Comercialización, Gerente de Contabilidad y Finanzas, Gerente de Sistemas, Director de administración y/o Director de Tecnologías y Sistemas Informáticos, quienes serán los encargados en realizar las acciones necesarias.

b. Descripción

Se informa a la alta dirección lo que originó la paralización de los servicios. En función de esto se toman las medidas del caso y se revisa el plan de contingencia para actualizarlo en el caso de que sea necesario.

c. Mecanismo de comprobación

Se procede a llenar el formato de ocurrencia de evento y se envía a la coordinación ejecutora del plan para la revisión.

d. Desactivación del plan de contingencia

Con el permiso de la alta Gerencia, Director de Tecnologías y Sistemas Informáticos el plan se procederá a la desactivación del plan.

e. Proceso de actualización

En el supuesto caso de que exista información que no conste acerca de los sistemas centrales, se coordina con el director para iniciar con las labores de actualización de los sistemas

4.4 Estrategias

La estrategia implementada en el presente plan es contar con:

- Plan de prevención, ejecución, recuperación y pruebas desarrolladas en el presente plan de contingencia.
- Organización propuesta para la gestión del plan de contingencia planteado la ”Organización del Plan de Contingencia”
- Desarrollar y documentar los principales eventos planteados en el presente plan de contingencia ”Desarrollo de las Actividades”

4.5 Programas

El presente plan de contingencia ha desarrollado un conjunto de ítems (cuadro Nº3), eventos que permiten dar valores a los sub-factores que tienen prioridad para la empresa

En el presente Plan de Contingencia se ha desarrollado un conjunto de ítems (cuadro Nro. 4), eventos o programas que permitan añadir valor a los sub-factores que ha priorizado la empresa.

4.6 Políticas

El plan de contingencia constará de una actualización periódica anual y entregado a la alta dirección para la aprobación y validación del mismo.

Las actualizaciones que vendrán de la segunda versión en adelante poseerá un sub-capitulo el mismo que incluirá las altas, bajas y mejoras de los planes de contingencia,

Se mantendrán 2 copias vigentes de respaldo y se repartirá una copia a todas las áreas involucradas en los planes.

Se realizará plan de pruebas semestralmente.

4.7 responsables

En el literal “4.4. Desarrollo de las actividades, fases, estrategias, programas y/o políticas” del presente Plan fueron considerados todos los responsables de la ejecución de los diferentes eventos que pueden ocasionar contingencia, por tal motivo esto se desarrolló empleando el formato del Anexo An2: “Formato Registro Plan de Contingencia” para el plan de prevención, ejecución, recuperación y pruebas.

4.8 Recursos

En el literal “4.4. Desarrollo de las actividades, fases, estrategias, programas y/o políticas” del presente Plan; se ha considerado los recursos a emplear durante la ejecución de los diferentes eventos susceptibles de contingencia. Para esto se ha desarrollado utilizando el formato An2: “Formato Registro Plan de Contingencia”.

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El presente Plan de Contingencia para el centro de computo, tiene como punto fundamental salvaguardar la información y la infraestructura física del centro de computo aplicando las mejores practicas de seguridad para proteger y preparar al personal cuando alguna contingencia se haga presente.
- La implementación del Plan de Contingencia requiere las siguientes actividades: Análisis de riesgos, Definición de eventos controlables y no controlables, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.
- El Plan de Contingencia es un herramienta que toda institución debe poseer para garantizar la sobrevivencia del personal y la continuidad del servicio en caso de que algún evento se haga presente ocasionando así la interrupción parcial o total de las funciones.
- No existe un plan de contingencia único que se acople a todas las organizaciones, es decir que cada empresa puede crear su propio plan de contingencia dependiendo de la infraestructura y los servicios que preste el centro de computo.
- La mejor manera de que una institución reaccione adecuadamente ante cualquier eventualidad, es mediante la elaboración, prueba y actualización de los Planes.

5.2. Recomendaciones

- Es recomendable planear las actividades propuestas en el presente Plan de Contingencia, apoyándose de un cronograma de actividades.
- Dar a conocer a todo el personal de la empresa el contenido del Plan de Contingencia, con la finalidad de que el personal conste con la instrucción adecuada.
- Se debe desarrollar reglas de control adicionales para la verificación de la efectividad de las acciones en el caso de que una eventualidad llegue a presentarse.
- Poseer una seguridad adecuada a proteger todos los recursos informáticos desde el dato mas simple hasta el mas valioso,

Bibliografía

School, I. -I. (2012). Retrieved 15 de Septiembre de 2012 from itmadrid: http://www.itmadrid.com/blog/que-es-itil/

Seguinfo. (2008). *seguinfo.wordpress.com*. Retrieved 9 de Septiembre de 2012 from http://seguinfo.wordpress.com/2008/12/03/%C2%BFque-es-itil-2/

Fundación Wikimedia, Inc. (17 de Septiembre de 2012). *wikipedia*. Retrieved 1 de Octubre de 2012 from http://es.wikipedia.org/wiki/Disponibilidad

Fundación Wikimedia, Inc. (27 de enero de 2012). *wikipedia*. Retrieved 8 de Octubre de 2012 from http://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad

Tuya, J. D. (2009). *itil*. Retrieved 10 de Septimbre de 2012 from net16: http://itilunfv.net16.net/index.php

Torres, L. R. (23 de Junio de 2011). Retrieved 26 de Septiembre de 2012 from slideshare.net: http://www.slideshare.net/FabinE1/7capitulo-vii-plan-de-contingencia#btnNext

Angulo, E. J. (2 de Marzo de 2012). Retrieved 29 de Septiembre de 2012 from slideshare: http://www.bvsde.paho.org/bvsade/fulltext/manual_peem/marco.pdf

Fundación Wikimedia, Inc. (5 de Junio de 2012). *wikipedia*. Retrieved 1 de Octubre de 2012 from http://es.wikipedia.org/wiki/ITIL

Fundación Wikimedia, Inc. (16 de Enero de 2012). *wikipedia*. Retrieved 1 de Octubre de 2012 from http://es.wikipedia.org/wiki/Plan_de_Contingencias

Fundación Wikimedia, Inc. (29 de Agosto de 2012). *wikipedia*. Retrieved 1 de Octubre de 2012 from Fundación Wikimedia, Inc

fopae. (Marzo de 2012). *fopae.* Retrieved 18 de Septiembre de 2012 from http://www.fopae.gov.co/portal/page/portal/sire/manuales/documentos/PEB/Anexo3-Guias/ANEXO%203-%20GUIA%20PLANES%20EMERGENCIA%20Y%20CONTINGENCIAS.pdf

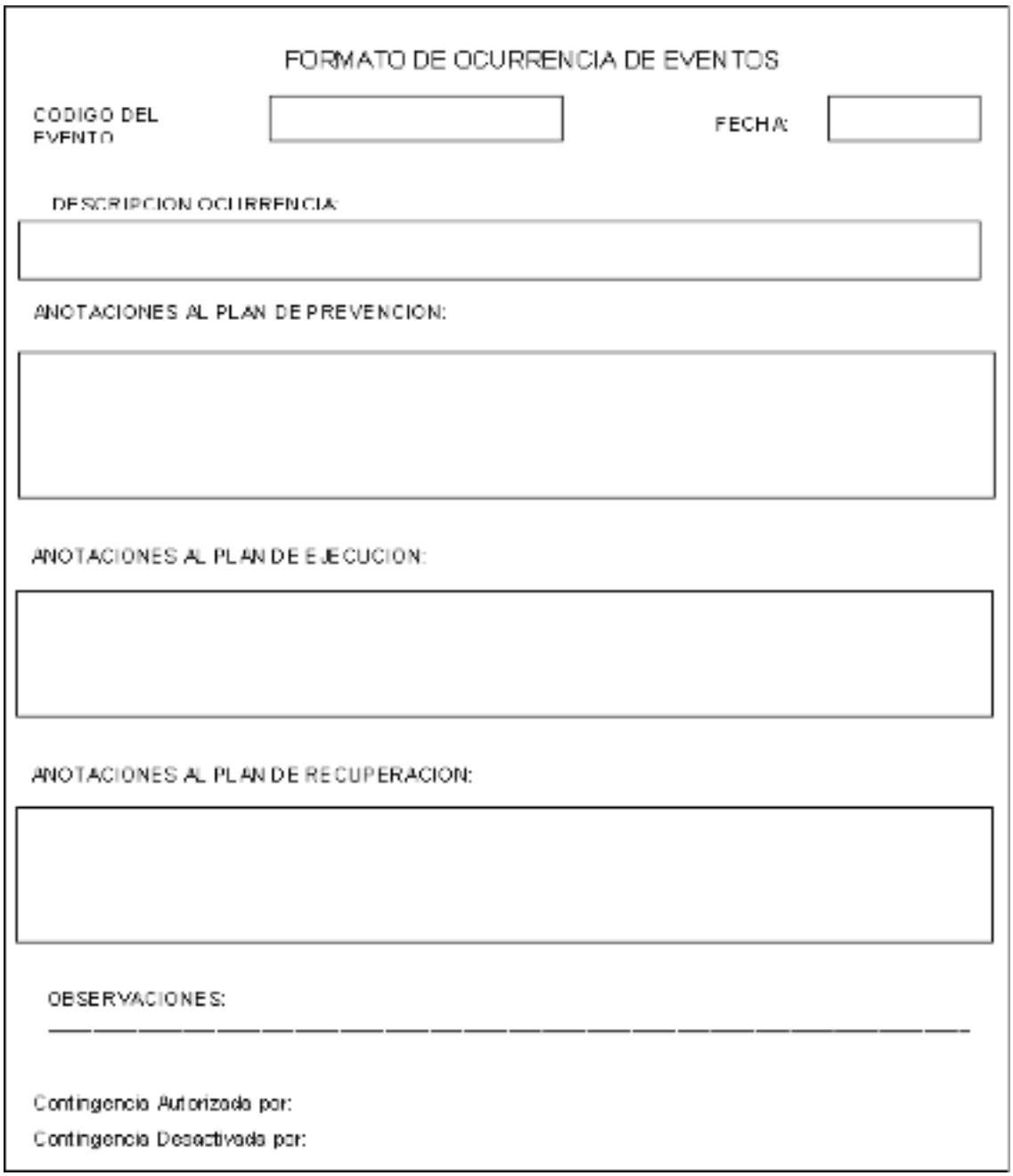
galeon. (n.d.). Retrieved 4 de Septiembre de 2012 from auditoriadesistemas: http://auditoriadesistemas.galeon.com/productos2227783.html

Jan van Bon, Arjen de Jong, Axel Kolthof, Mike Pieper, Ruby Tjassing, Annelies van der Veen, et al. *Fundamentos de la Gestión de Servicios de TI Basados en ITIL* (3ª edición ed.). Estados Unidos: Van Haren Publishing, Zaltbommel.

jdiaz1985. (2009). *scribd.com/.* Retrieved 22 de Septiembre de 2012 from http://es.scribd.com/doc/16253152/PLANEACION-Y-ELABORACION-DE-UN-CENTRO-DE-COMPUTO

Anexos.

An1: Formato de ocurrencia del Evento



FORMATO DE OCURRENCIA DE EVENTOS

CODIGO DEL EVENTO

FECHA:

DESCRIPCION OCURRENCIA:

ANOTACIONES AL PLAN DE PREVENCION:

ANOTACIONES AL PLAN DE EJECUCION:

ANOTACIONES AL PLAN DE RECUPERACION:

OBSERVACIONES:

Contingencia Autorizada por:

Contingencia Desactivada por:

An2: “Formato de Registro del Plan de Contingencia”

<table>
<tr><td>Empresa</td><td colspan="2">Evento: “Nombre del Evento”</td><td>“Código”</td></tr>
<tr><td>“Nombre Empresa”</td><td colspan="2"></td><td>Versión: 1.1</td></tr>
<tr><td>Fecha:</td><td>Entidad responsable: “nombre empresa”</td><td>Entidad involucrada: “nombre empresa”</td><td>Pagina.</td></tr>
<tr><td colspan="4">1. PLAN DE PREVENCIÓN</td></tr>
<tr><td colspan="4">a) Descripción del evento
b) Objetivo
c) Criticidad
d) Entorno
e) Personal encargado
f) Condiciones de prevención del riesgo</td></tr>
<tr><td colspan="4">2. PLAN DE EJECION</td></tr>
<tr><td colspan="4">a) Eventos que activan la contingencia
b) Procesos relacionados antes del evento
c) Personal que autoriza la contingencia
d) Descripción de las actividades después de activada la contingencia
e) Duración</td></tr>
<tr><td colspan="4">3. PLAN DE RECUPERACION</td></tr>
<tr><td colspan="4">a) Personal encargado
b) Descripción
c) Mecanismo de comprobación
d) Mecanismo de recuperación
e) Desactivación del plan de contingencia
f) Proceso de actualización</td></tr>
</table>

An3: “Copias de Respaldo”

Todos los desarrolos de aplicaciones nuevos en la empresa se debe realizar un proceso de respaldos de información que incluye el codigo fuente, ejecutables,bases de datos, configuracion de equipos, documentacion, software entre otros.

El area de soporte tecnico del departamento de Tecnologia Informatica sera el encargado de la ejecución de los respaldos, se basa en una rutina de copias de seguridad tipo Basico o normal, Los contenidos y frecuancia de dichas copias de respaldo se las debe realizar como se da a conocer en el siguiente cuadro:

Grafico 46: Rutinas de Respaldo

Rutina de Respaldos					
Frecuencia del respaldo	Contenido	Día de entrega	Periodo de retención	Cantidad de copias	Destino
Diario	Base de datos	Lunes a domingo	Una semana	1	Departamento de sistemas
Semanal	Base de datos	Domingo	Seis meses	3	Departamento de sistemas, local matriz y empresa aseguradora.
Anual	Base de datos y códigos fuente	Primer día laborable del siguiente año	Tres años	3	Departamento de sistemas, local matriz y empresa aseguradora

Los respaldos de información deben cumplir con las siguientes característica:

Los respaldos serán realizados en medios magnéticos removibles(LTO-3 de 400Gb, LTO-4 de 800Gb), una vez realizado el backup se procederá inmediatamente a la etiquetación del dispositivo, Los términos empleados para el proceso de etiquetado para la identificación de cartuchos, estará basada en el tipo de data que almacena y la fecha que se realizo.

El almacenamiento de los cartuchos se lo realizara en las instalaciones de la empresa y una copia en la empresa aseguradora, esto como medidas de contingencia.

An4: “Control y Certificación de Pruebas de Contingencia”

Código Nº (del plan)

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: (Nombre del proceso a probar/certificar)

Area responsable: (Area responsable del proceso probar/certificar)

Fecha : / / Hora Inicio : Hora Fin : (de prueba)

Información del Proceso

Metodologia y Alcance: (Que se va a hacer en la prueba y hasta donde va a abarcar la misma)

Condiciones de Ejecución:

Equipo : (Nombre del servidor / pc / maquina en proceso de prueba o certificación)

Aplicación/Software : Version:

Fecha de Backup : / /

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☐ Satisfastorio con Observaciones: ☐ Deficiente: ☐

Observaciones: (en el caso de haber observaciones o que la prueba haya sido deficiente se iniciaran los motivos de dichas deficiencias, así como resultados de las pruebas en todos los casos)

Actualalización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia (Se indicará los cambios que se realizarán en el Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

Participantes Vº Bº y Aprobación

Participante	Cargo	Firma

Plan de negocio de un plan de contingencia para el centro de computo de un ISP

Diseñado para: Empresa de telecomunicaciones "Puntonet"

El: 4/ENERO/2013 Iteración Nº: 1

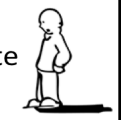
Diseñado por: Israel Rubén Bermeo C.

<table>
<tr>
<td rowspan="2">Socios clave 

1. Capacitar a los empleados de manera independiente en cada una de las areas de la Empresa.
2. Incentivar a los empleados a explotar su potencial que beneficie a la empresa.
3. Mejorar la organización Interna de la Empresa.</td>
<td>Actividades clave 

1. Alta disponibilidad del servicio
2. Respuesta inmediata en problemas emergentes.
3. Migraciones continuas a nuevas tecnologías.
4. Servicio de post venta a clientes.</td>
<td rowspan="2">Propuesta de valor 

1. Vanguardia con la tecnologia para mejorar costos hacia los usuarios.
2. Calidad de Servicio.
3. Valor Agregado.
4. Servicio Técnico 24/7/365</td>
<td rowspan="2">Relación con clientes 

1. Asesoría.
2. Confianza.
3. Disponibilidad Inmediata</td>
<td rowspan="2">Segmento cliente 

1. Asistencia Personalizada telefónico y presencial.
2. Diagrama de red y equipos instalados.
3. Seguros de Equipos.
4. Uptime Efectivo.</td>
</tr>
<tr>
<td>Recursos clave 

1. Personal de soporte técnico calificado.
2. Equipamento de</td>
<td>Canales 

Correo interno.
Asistencia telefónica
Documento físico.</td>
</tr>
<tr>
<td colspan="3">Estructura de costes 

1. Arrendamiento a proveedor Internacional
2. Pago Servicio Ultima Milla
3. Costes de Infraestructura
4. Empleados
5. Costes de Operabilidad</td>
<td colspan="3">Fuentes de ingresos 

1. Alquiler de Servicio de Internet.
2. Alquiler de Equipos.
3. Webhosting.
4. Arrendamiento de Nodos</td>
</tr>
</table>

An6: Guia de Procedimientos del plan para el servicio wifi

PLAN DE CONTINGENCIA WIFI

Objetivo

Nuestro objetivo a través de este plan de contingencia, es asegurar un uptime mayor al que se tiene en los nodos wifi y así asegurar el prestigio y la imagen de la empresa.

Queremos asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, y de los medios de almacenamiento.

La función principal será comunicar a todo el personal técnico de Puntonet los pasos a seguir en caso de cualquier riesgo.

La vigencia de este plan está sujeto a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con Puntonet.

La evaluación del pan de contingencia se lo realizara en 5 pasos:

- Evaluación.
- Planificación.
- Pruebas de viabilidad.
- Ejecución.
- Recuperación.

EVALUACIÓN:

1. Constitución del grupo de desarrollo del plan.

Este grupo estará liderado por un supervisor y formado por dos apoyos. Su elaboración ha de desarrollarse con la continua supervisión del supervisor ya que durante la elaboración y/o ejecución de éste, deberán comprometerse recursos y aprobarse procedimientos especiales que requieran un nivel de autorización superior "JEFE TECNICO".

2. Documentación de los posibles escenarios con los que podemos encontrarnos.

Puede tratarse de problemas en el hardware, software de base, de telecomunicaciones, software de aplicación propio o provisto por terceros, etc. También deben incluirse en

esta categoría los siniestros provocados por rayos, etc. una utilización indebida de medios magnéticos de resguardo o back up o cualquier otro daño de origen físico que pudiera provocar la pérdida masiva de información.

3. Análisis del impacto del desastre en cada función crítica.

Se realizar un análisis del impacto de cada problema sobre cada una de las funciones críticas de la organización, teniendo en cuenta las siguientes prioridades:

Reanudar las operaciones lo antes posible.

Lograr las conexiones al 100% a los clientes lo más pronto posible.

Mantener la confianza en sí mismo y en la empresa.

4. Niveles mínimos de servicio.

Se trata de definir los mínimos niveles de servicio aceptables para cada problema que se pueda plantear. Es importante que dicho nivel se consensué con cada uno de los responsables del Stanby.

5. Identificación de las alternativas de solución.

En esta subfase deberán identificarse las soluciones alternativas para cada uno de los problemas previsibles. Para ello se puede considerar:

- Realizar simulacros al momento de caída de un nodo.
- Contratar las tareas críticas con terceros por ejemplo desinstalaciones.
- Buscar, sugerir o actuar con otra medida que permita continuar las operaciones.

6. Relación coste/beneficio de cada alternativa.

De cada alternativa identificada en el punto anterior y sobre la base del impacto económico de cada problema, deberá determinarse la mejor solución desde el punto de vista coste/beneficio para cada proceso crítico y su tiempo de elaboración con un nivel de servicio que satisfaga el nivel mínimo.

PLANIFICACIÓN:

1. Planificación de contingencia.

Es necesario documentar el plan, cuyo contenido mínimo será:

- Modo de ejecución.
- Tiempo de duración.
- Costes estimados en el caso que sea necesario realizar gastos extras.
- Recursos necesarios.
- Evento a partir del cual se pondrá en marcha el plan.
- Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

PRUEBAS DE VIABILIDAD:

1. **Puntuar y documentar las pruebas del plan.**

Es necesario puntuar las pruebas del plan y el personal y recursos necesarios para su realización. Una correcta documentación ayudará a la hora de realizar las pruebas.

2. **Obtener los recursos necesarios para las pruebas.**

Deben obtenerse los recursos para las pruebas, ya sean recursos físicos (equipos) y el personal respectivo que se encuentre de Stanby.

3. **Ejecutar las pruebas y documentarlas**

Se realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles.

4. **Actualizar el plan de contingencia de acuerdo a los resultados obtenidos en las pruebas**

Se actualizará el plan de acuerdo a los resultados obtenidos en las pruebas.

Hay que tener en cuenta que el plan de contingencia WIFI de Puntonet Cuenca contiene los planes de contingencia específicos para cada problema definido. Los distintos planes como Corporativos deben integrarse en un todo, considerando las posibles relaciones mutuas.

EJECUCIÓN:

En esta fase hay que tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas que presenta Puntonet Cuenca.

RECUPERACIÓN:

Los equipos afectados por los problemas ocasionados que pudiesen haber quedado desactualizados o quemados, deben ser recuperados en este caso pedidos a Quito para tener de respaldo.

EQUIPOS DE BACKUP	
EQUIPOS	EXISTENICA
MKT 433, 2 INTERFACES XR2	OK
MKT 433, 3 INTERFACES XR2	OK
MKT 433, 2 INTERFACES R52H	NO, PEDIDOS A QUITO
MKT 411, 1 INTERFACES R52H	OK
SWITCH	OK
MKT RB750	OK
SECTORIALES	OK
DSLAN CORECESS	OK
PIGTAIL	NO, PEDIDOS A QUITO
FUENTES DE PODER DE 1.6A a 24V	NO, PEDIDOS A QUITO

BASES MKT	
BASE	IP
RAYOLOMA	10.105.60.1
RAYOLOMA	10.105.61.1
HITO CRUZ	10.105.90.1
HITO CRUZ	10.105.91.1
BARABON	10.105.50.1
BARABON	10.105.51.1

NODOS WIFI CUENCA

#	NOMBRE NODO	TECNOLOGIA BACK-HAUL	TECNOLOGIA ACCESO	IP BASE	IP BACK-HULT
1	NODO REMIGIO	CABLE DIRECTO AL SWITCH OFICINA	2 MKT433AH-2 INTERFACES XR2	10.116.11.6 / 10.116.11.7	DIRECTO AL NODO
2	VISTA LINDA	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.12.2	10.104.50.34
3	MIRAFLORES	MKT 411AH-R52H	2 MKT433AH-3 INTERFACES XR2	10.116.16.2 / 10.116.16.4	10.104.90.122
4	ORO VERDE	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.19.2	10.104.50.106
5	HUAYNA CAPAC	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.18.2	10.104.30.26
6	BAÑOS	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.7.2	10.104.91.74
7	CAPULISPAMBA	WIMAX	MKT433AH-3 INTERFACES R52H	10.116.4.2	10.106.60.73
8	CENTRO	MKT 411AH-R52H	2 MKT433AH-3 INTERFACES XR2	10.116.14.2 / 10.116.14.4	10.104.61.10
9	VALLE	WIMAX	MKT411AH-1 INTERFACES R52H	10.116.5.2	10.106.90.170

10	INGENIEROS	MKT 411AH-R52H	MKT433AH-2 INTERFACES R52H	10.116.6.2	10.104.60.26
11	MILENIUM	FIBRA	MKT 3 INTERFACES MINI PCI XR2	10.116.13.2	FIBRA
12	MUTUALISTA AZUAY II	WIMAX	MKT433AH-2 INTERFACES R52H	10.116.3.2	10.106.50.67
13	PUERTAS DEL SOL	FIBRA	MKT 3 INTERFACES MINI PCI XR2	10.116.9.2	FIBRA
14	RIO SOL	MKT 411AH-R52H	MKT 2 INTERFACES MINI PCI XR2	10.116.8.2	10.104.60.18
15	SAN JOSE I	WIMAX	MKT411AH-1 INTERFACES R52H	10.116.1.2	10.106.50.58
16	SAN JOSE II	MKT 411AH-R52H	MKT 2 INTERFACES MINI PCI XR2	10.116.2.2	10.104.90.210
17	TOTORACOCHA	MKT 411AH-R52H	2 MKT433AH-3 INTERFACES XR2	10.116.10.2 / 10.116.10.4	10.104.60.2
18	UNCOVIA	MKT 411AH-R52H	MKT433AH-2 INTERFACES R52H	10.116.20.2	10.104.60.178
19	VISTA LINDA II	MKT 411AH-R52H	MKT433AH-2 INTERFACES XR2	10.116.21.2	10.104.50.178

20	SANTA TERESITA	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.23.2	10.104.51.2
21	COLISEO	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.25.2	10.104.50.154
22	RICAURTE	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.26.2	10.104.91.114
23	AUEROPUERTO	MKT 411AH-R52H	MKT433AH-3 INTERFACES XR2	10.116.22.2	10.104.61.66
24	GUZHO	MKT 411AH-R52H	MKT433AH-2 INTERFACES XR2	10.116.27.2	10.104.50.162

NODOS WIFI CUENCA Contactos.

#	SSID DE LAS BASES	SSID DEL BACK-HAUL	Channel width BASE	CONTACTO	NUMERO
1	PUNTONET_REMIGIO1.3 PUNTONET_REMIGIO1.2 PUNTONET_REMIGIO1.4 PUNTONET_REMIGIO1.1	------	20 MHz	----	----
2	PUNTONET_VISTALINDA1.1 PUNTONET_VISTALINDA2.2 PUNTONET_VISTALINDA2.2	WIFI VISTA LINDA	20 MHz	ALVARO CRESPO SEMINARIO	2888772/2887949/097909565
3	NODO_PTO_MIRAFLORES1 PUNTONET MIRAFLORES 2.1 NODO_PTO_MIRAFLORES2 PUNTONET MIRAFLORES 2.2 NODO_PTO_MIRAFLORES3 PUNTONET MIRAFLORES 2.3	WIFI_MIRAFLORES	10MHz / 20MHz	KLEVER ROMERO SANCHEZ	2829349 / 098899891
4	PUNTONET_OROVERDE1 PUNTONET_OROVERDE2 PUNTONET_OROVERDE3	WIFI ORO VERDE	10MHz	Sr. Araceli de Robayo	98178824
5	PUNTONET_HUANYCAPAC-1 PUNTONET_HUANYCAPAC-2 PUNTONET_HUANYCAPAC- 3	WIFI_HUAY	10MHz	PATRICIO SALINAS POZO	2871942 / 096173535
6	PUNTONET 1 PUNTONET 2 PUNTONET 3	WIFI BANOS	20 MHz	MIGUEL DELGADO ORTIZ	2386885/4024199/092464078
7	PUNTONET PUNTONET2 PUNTONET2	000000010665 ID BASE RAYOLOMA	20 MHz	ROSA FAREZ BUENO	2875366

8	PUNTONET_CENTRO1.2 PUNTONET CENTRO 2.1 PUNTONET_CENTRO1.3 PUNTONET CENTRO 2.2 PUNTONET_CENTRO1.1 PUNTONET CENTRO 2.3	NODO_CENTRO	20MHz / 10MHz	HECTOR BRAVO ZUÑIGA	2848093 / 099675942
9	PUNTONET	000000010698 ID BASE HITOCRUZ	20 MHz	MANUEL AGUIRRE RUEDA	82659625
10	PUNTONET 1 PUNTONET 2	WIFI INGENIEROS	20 MHz	RAUL ORTIZ BRAVO	4085363 / 099903442
11	PUNTONET_MILENIUM_1 PUNTONET_MILENIUM_1 PUNTONET_MILENIUM_2	------	20 MHz	FABIAN SARMIENTO BERMUDEZ	4103658 /2833353 /087874855
12	PUNTONET1 PUNTONET2	000000010652 ID BASE BARABON	20 MHz	ANTONIO PEREZ GONZALES	4082911 / 093324821
13	PUNTONET 3 PUNTONET 1 PUNTONET 2	------	20 MHz	JUAN MARTINEZ MENDUIÑO	2856770/2855069/099854115
14	PUNTONET 2 PUNTONET 1	NODO_RIO_SOL	20 MHz	GENARO PEÑA CORDERO	2802199 / 091884238
15	PUNTONET CUENCA	000000010651 ID BASE BARABON	20 MHz	VERONICA HERMIDA	2894787 / 099600101
16	PUNTONETCUENCA_SAN_JOSE2 PUNTONETSANJOSE2.2	NODO WIFI SAN JOSE II	20 MHz	SANTIAGO PAUTA DELGADO	2377278 / 094139884

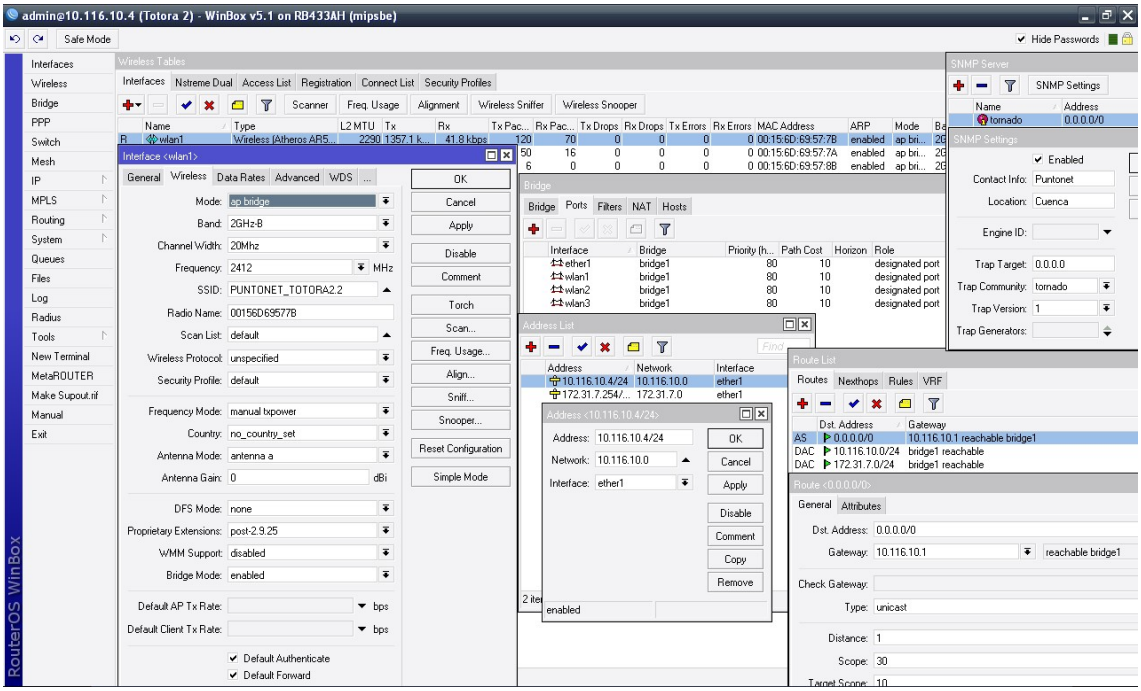
17	PUNTONET_TOTORACHOCHA1.1 PUNTONET_TOTORA2.2 PUNTONET_TOTORACHOCHA1.1 PUNTONET_TOTORA2.2 PUNTONET_TOTORACOCHA1.2 PUNTONET_TOTORA2.1	NODOWIFITOTORA	10MHz 20MHz 20MHz 20MHz 20MHz 10MHz	EDIFICIO ALTO RENDIMIENTO	2811763 / 2814920
18	PUNTONET_UNCOVIA1 PUNTONET_UNCOVIA2	WIFI UNCOVIA	10MHz	Bonilla Roldan Rafael Jacinto	2901119/2862235/094611546
19	PUNTONET_VISTALINDA3.1 PUNTONET_VISTALINDA3.2	WIFI_LINDA2	10MHz	ARQ. VEGA VILLA DIEGO FERNANDO	4090844
20	PUNTONET_TERESITA1 PUNTONET_TERESITA2 PUNTONET_TERESITA3	NODO WIFI SANTA TERESITA	10MHz 20MHz 20MHz	QUILLE MARIA	2868661 / 085758109
21	PUNTONET_COLISEO 1 PUNTONET_COLISEO 2 PUNTONET_COLISEO 3	WIFI_COLISEO	10MHz	FRANCISCO XAVIER PEÑA LEON	092860869/2817645
22	PUNTONET_RICAURTE 1 PUNTONET_RICAURTE 2 PUNTONET_RICAURTE 3	NODO RICAURTE	10MHz	ORTIZ AVILA BRAULIO JOSE	2475422 / 089103077
23	PUNTONET_AEROPUERTO1 PUNTONET_AEROPUERTO2 PUNTONET_AEROPUERTO3	WIFI_TOTORA_II	10MHz	Terán Espinoza Milton Teodoro	2806358/092674009
24	PUNTONET_GUZHO 1 PUNTONET_GUZHO 2	WIFI_GUZHO	10MHz	Freddy Llanos	088153482/4024181

PASOS A SEGUIR AL MOMENTO DE LA CAIDA DE UN NODO.

- Hacer ping al enlace back-hult, en caso que no se llegue hacer ping a la base donde se encuentra enganchado, esta documentación esta en el plan de contingencia corporativo.
- Si se llega con ping al back-hult hacer ping a la base wifi. En caso que no se llegue a la base wifi o al back-hult proceder con lo siguiente.
- Llamar a pedir permisos al dueño de la casa donde está el nodo.
- Llevar los equipos correspondientes necesarios, teniendo presente que pudo haberse quemado la fuente, switch o el equipo al que no se llega.

CONFIGURACIONES:

CONFIGURACIÓN DE UNA BASE MKT



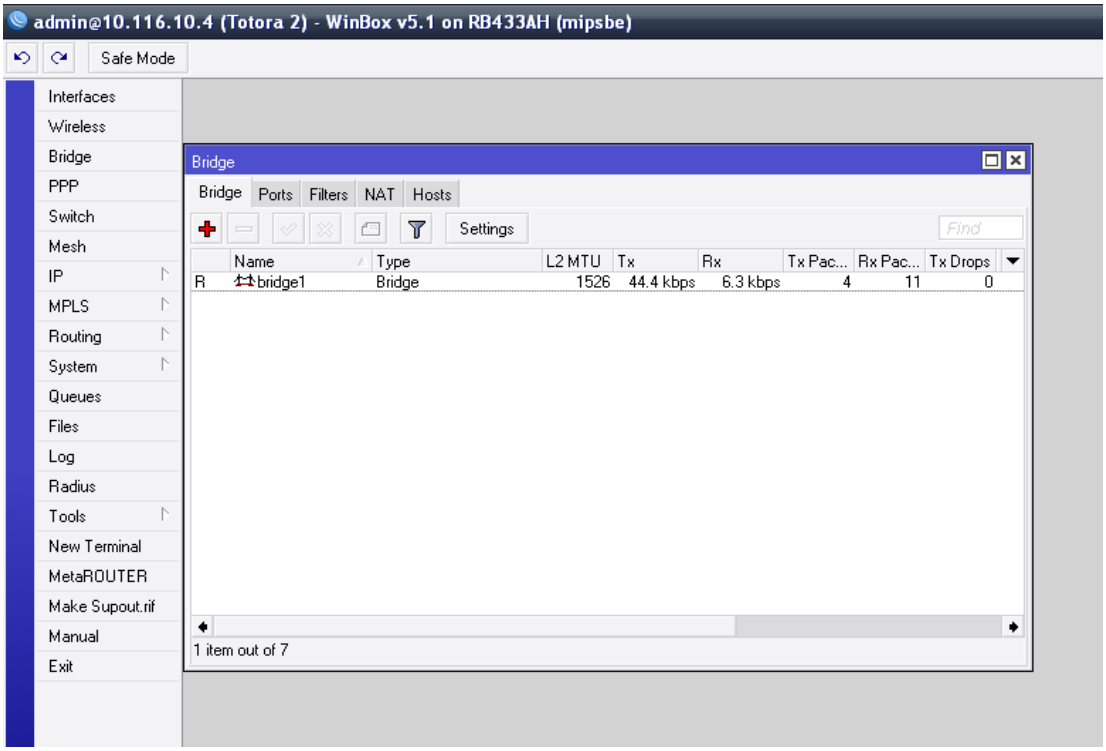
Este incrementa una utilidad por ejemplo un bridge.

Este elimina una utilidad.

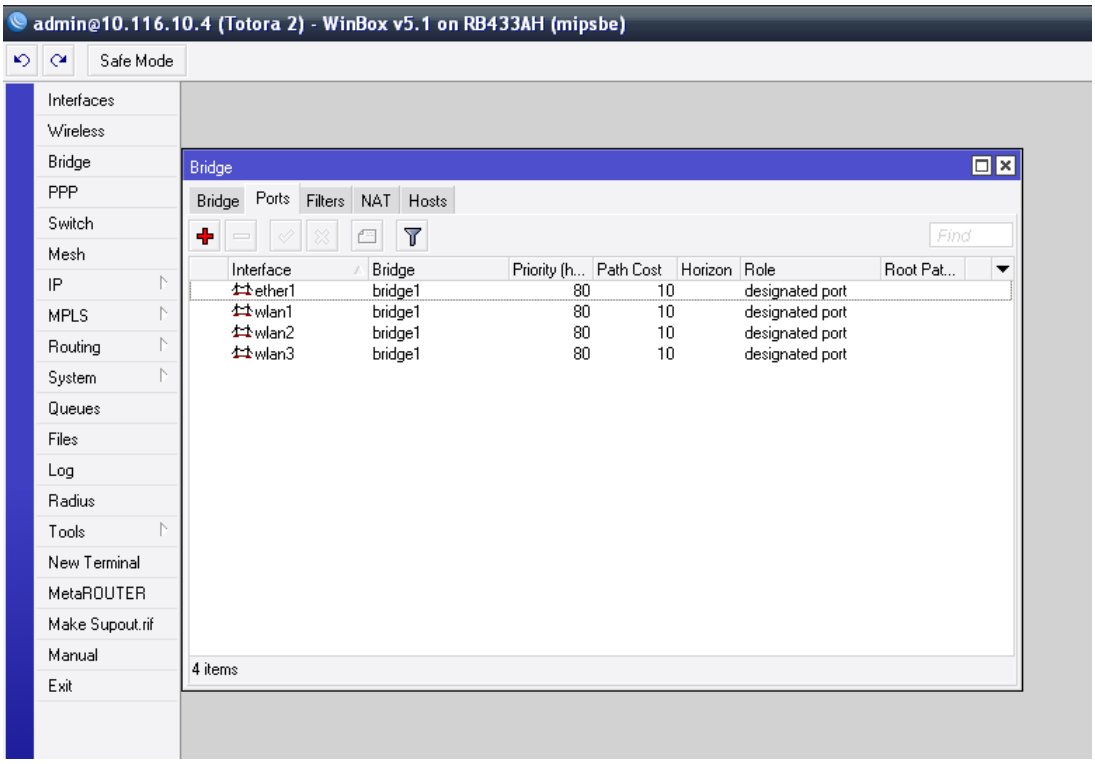
Habilita una utilidad

Deshabilita una utilidad

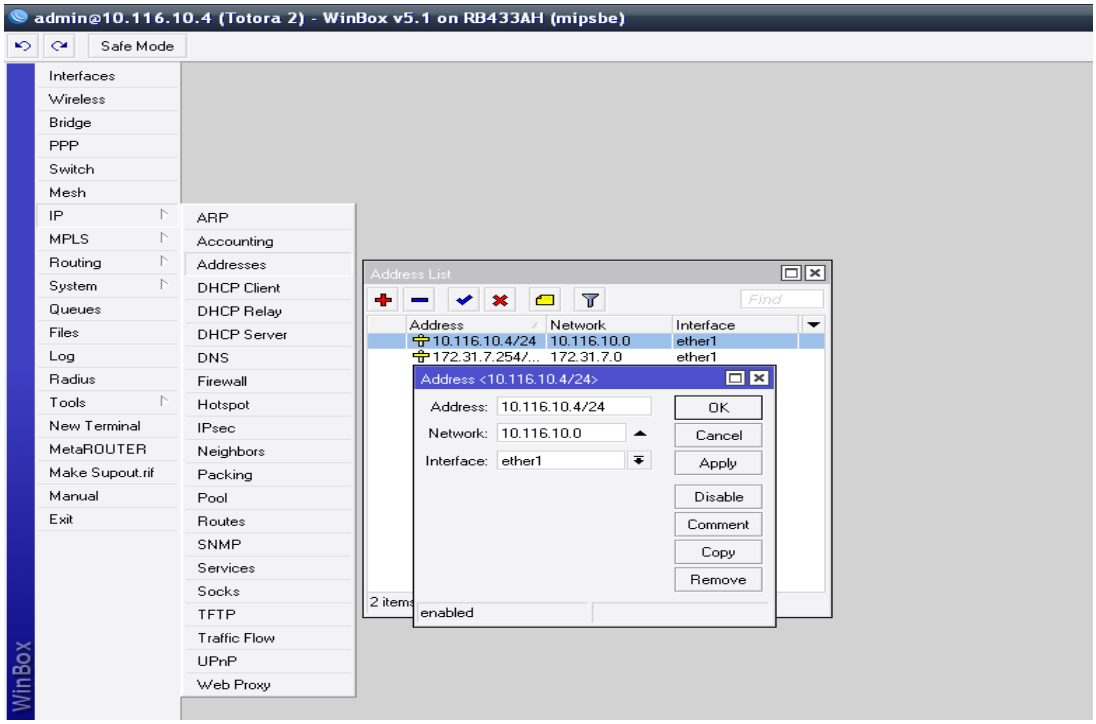
Configuración del Bridge.



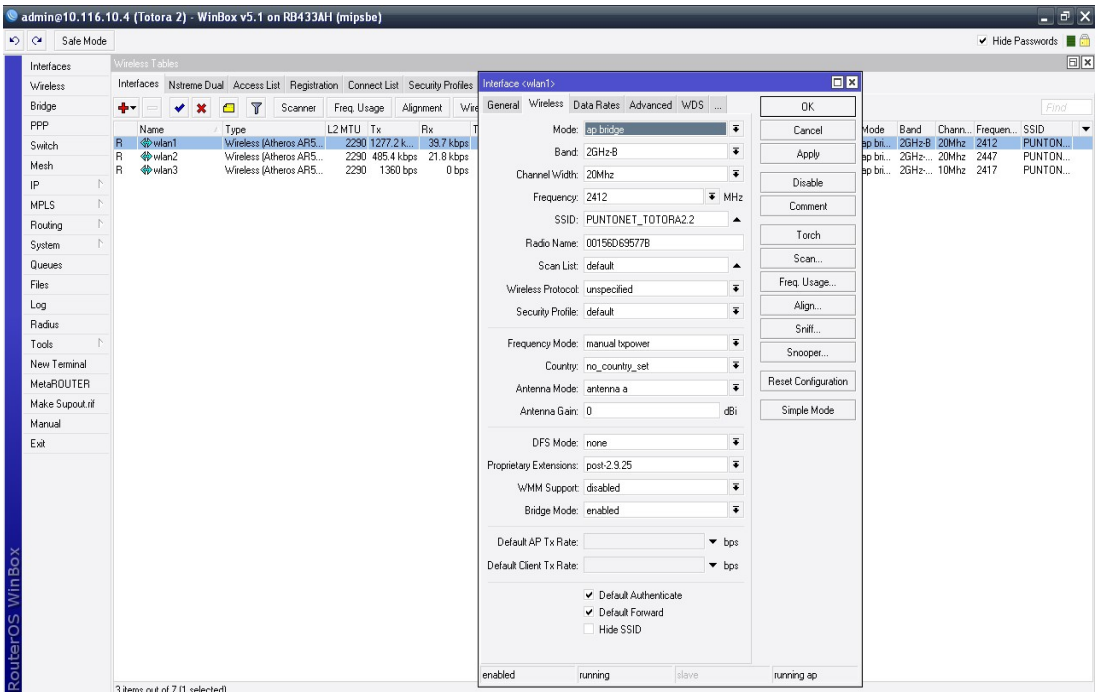
Añadimos a todas la interfaces en el mismo Bridge



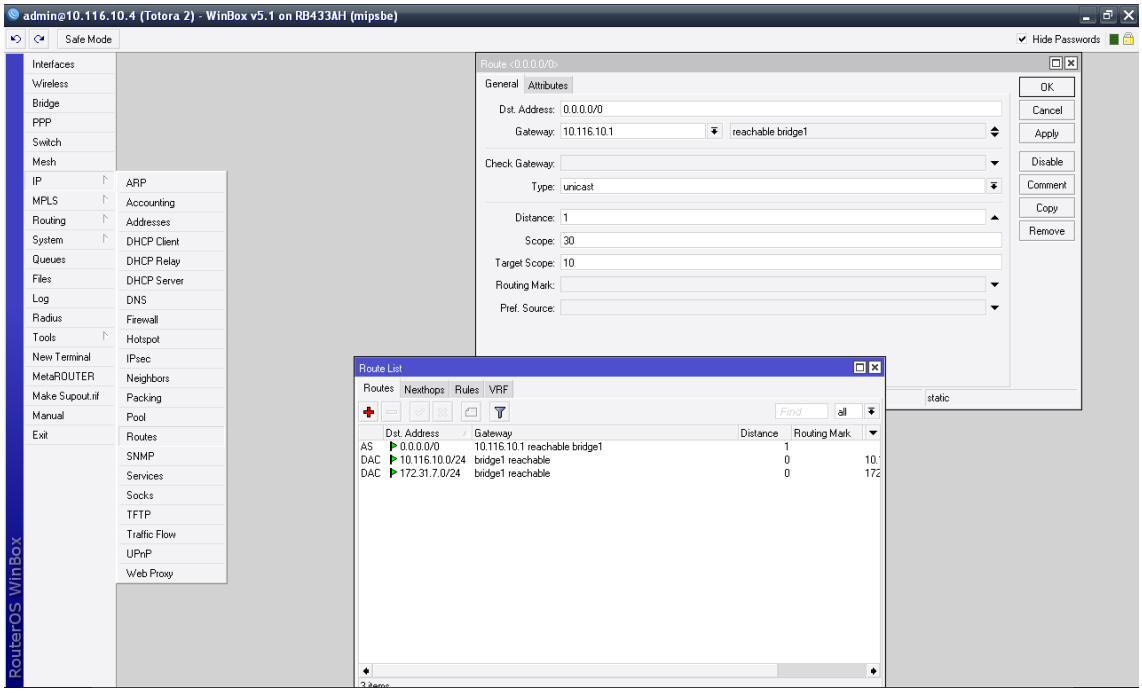
Configuración de las IP's



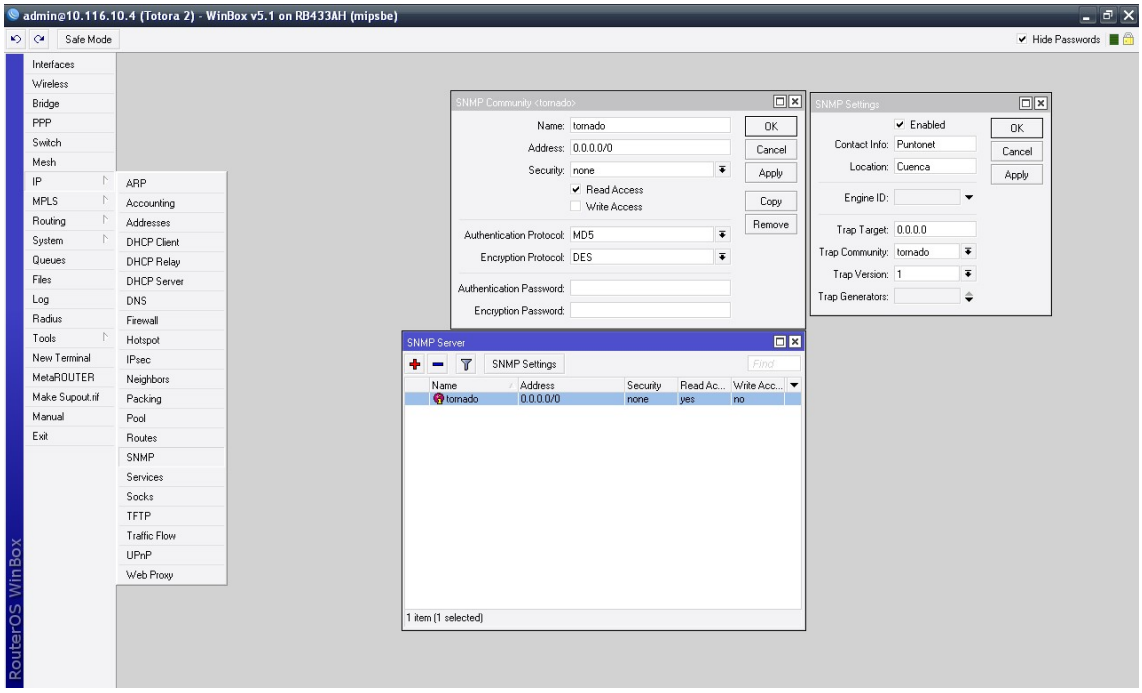
Configuración de la red Inalámbrica.



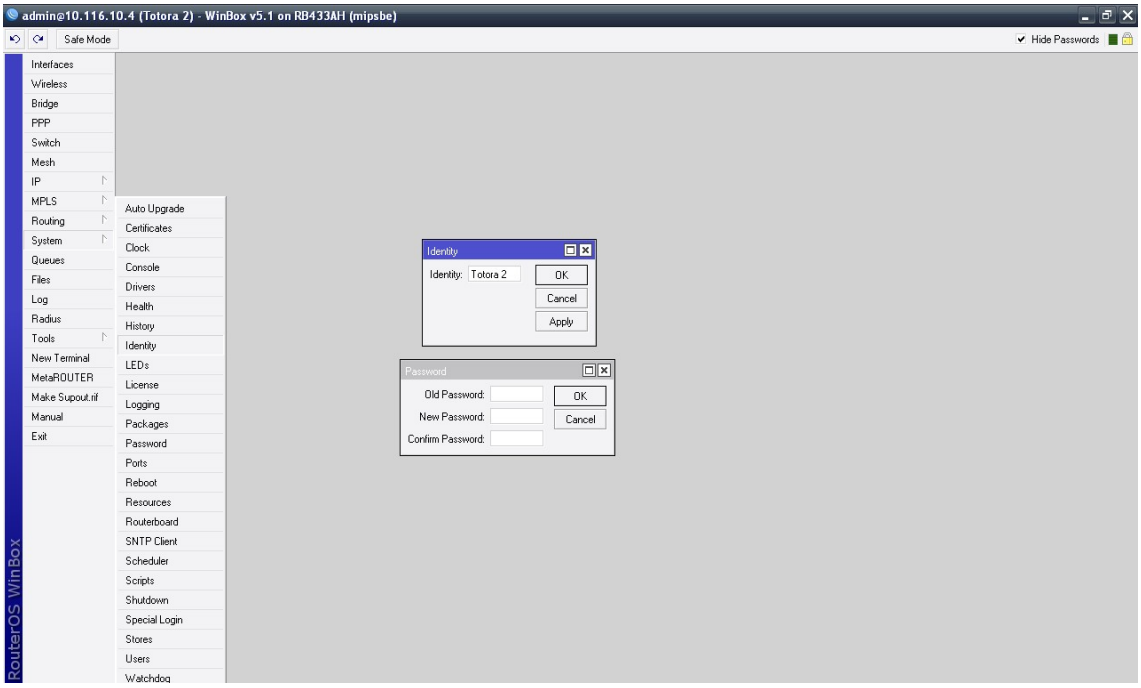
Configuración de la ruta.



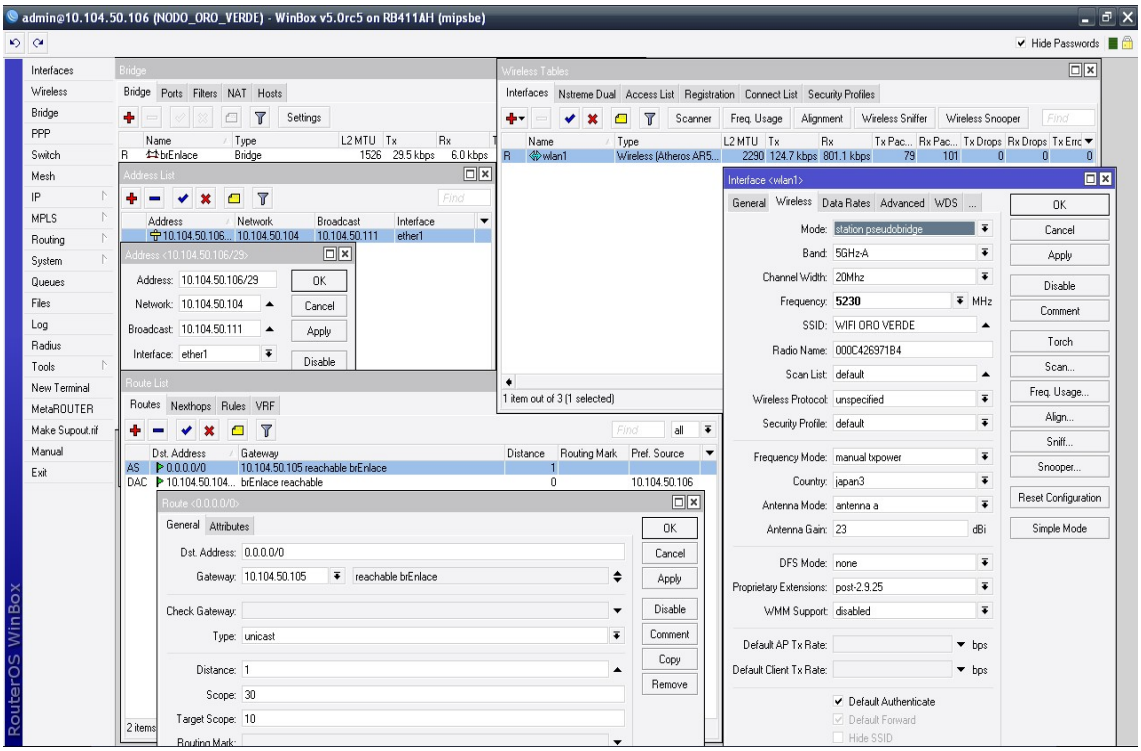
Configuración de la comunidad.



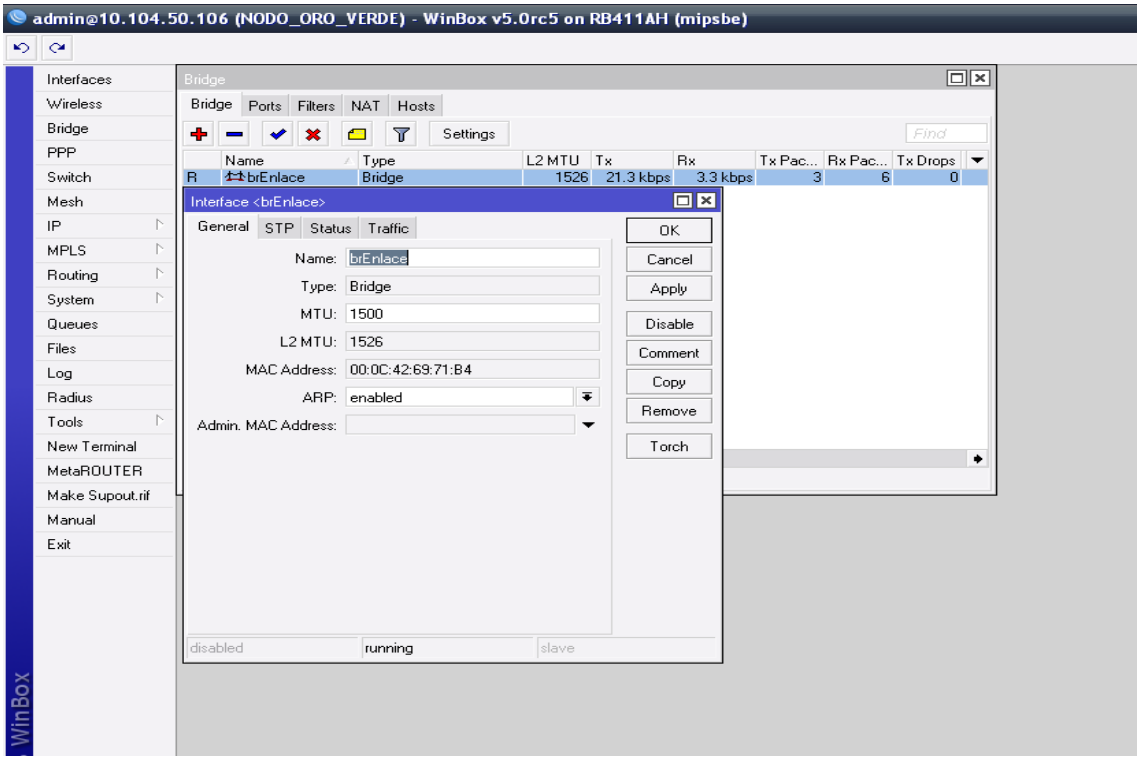
Configuración de la Clave de Acceso al MKT.

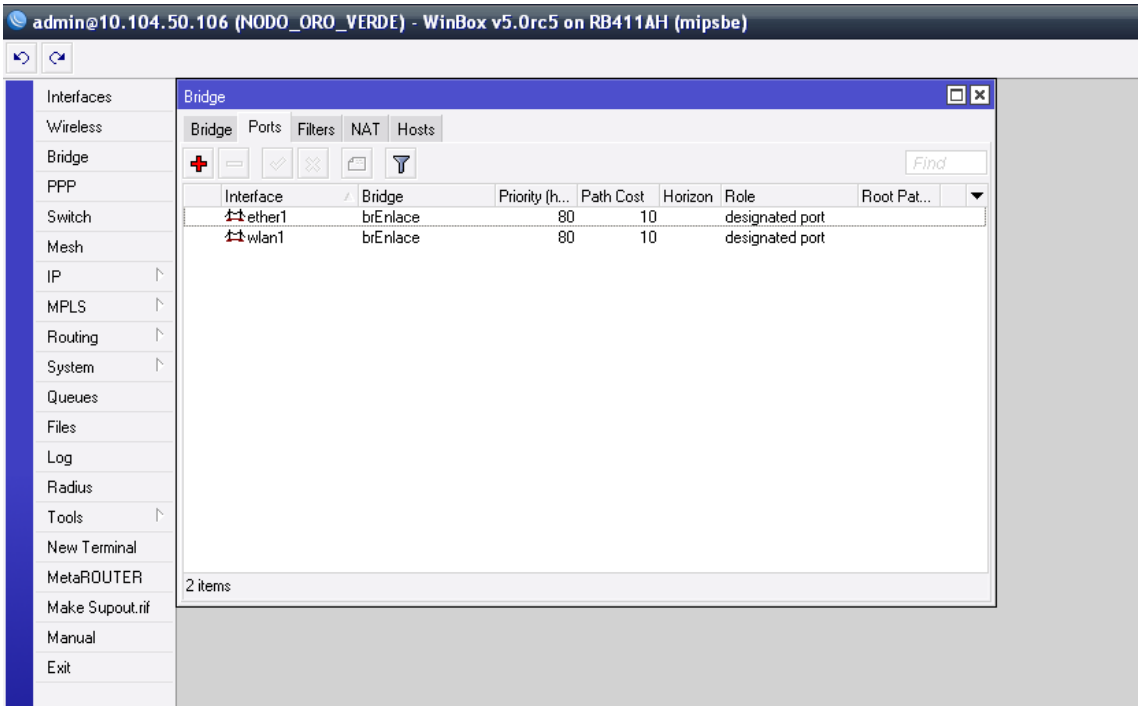


CONFIGURACIÓN BACK-HAUL

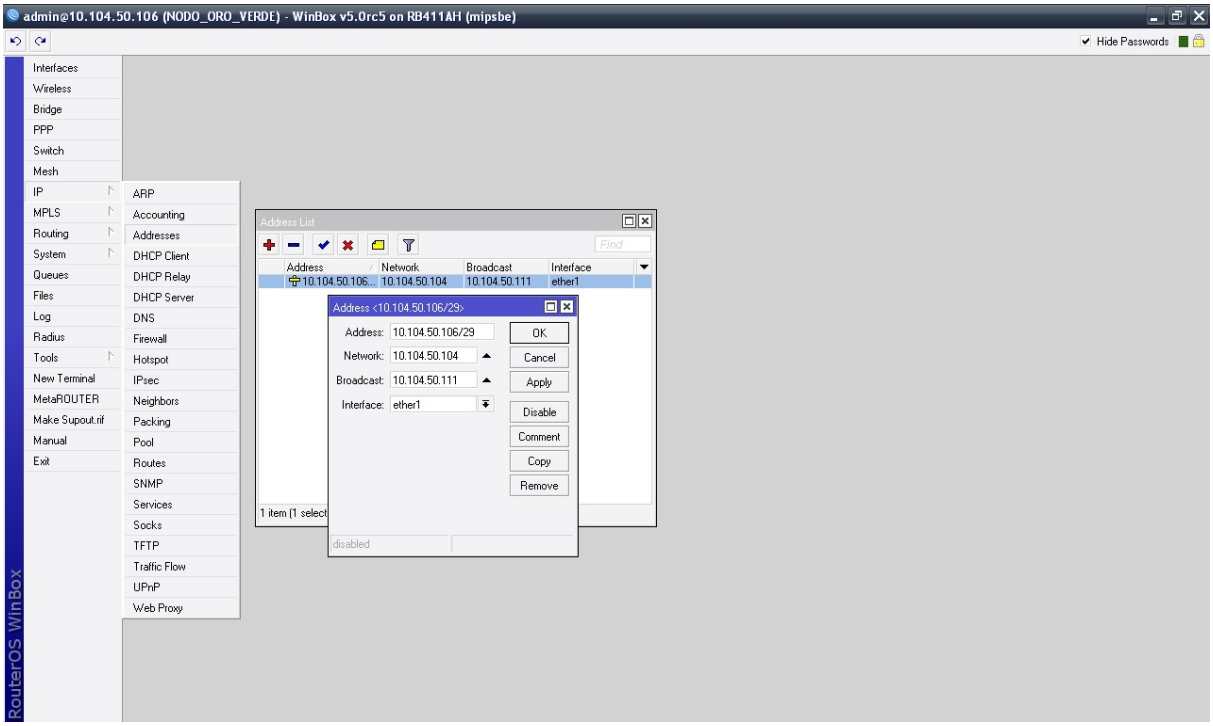


Configuración del Bridge.

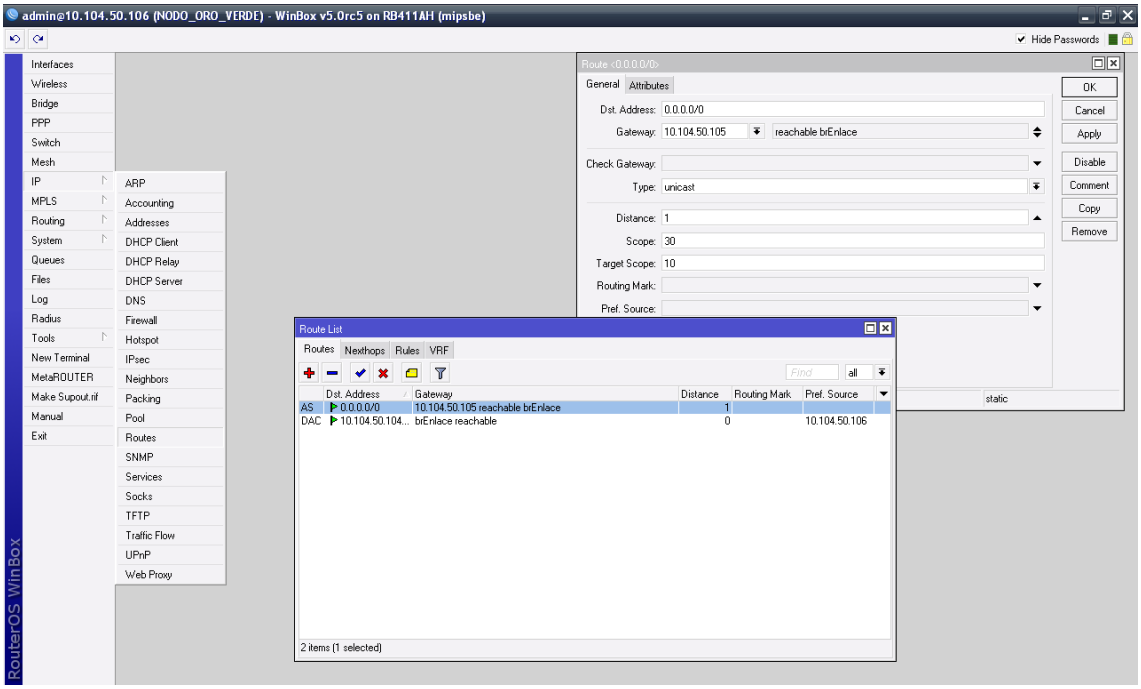




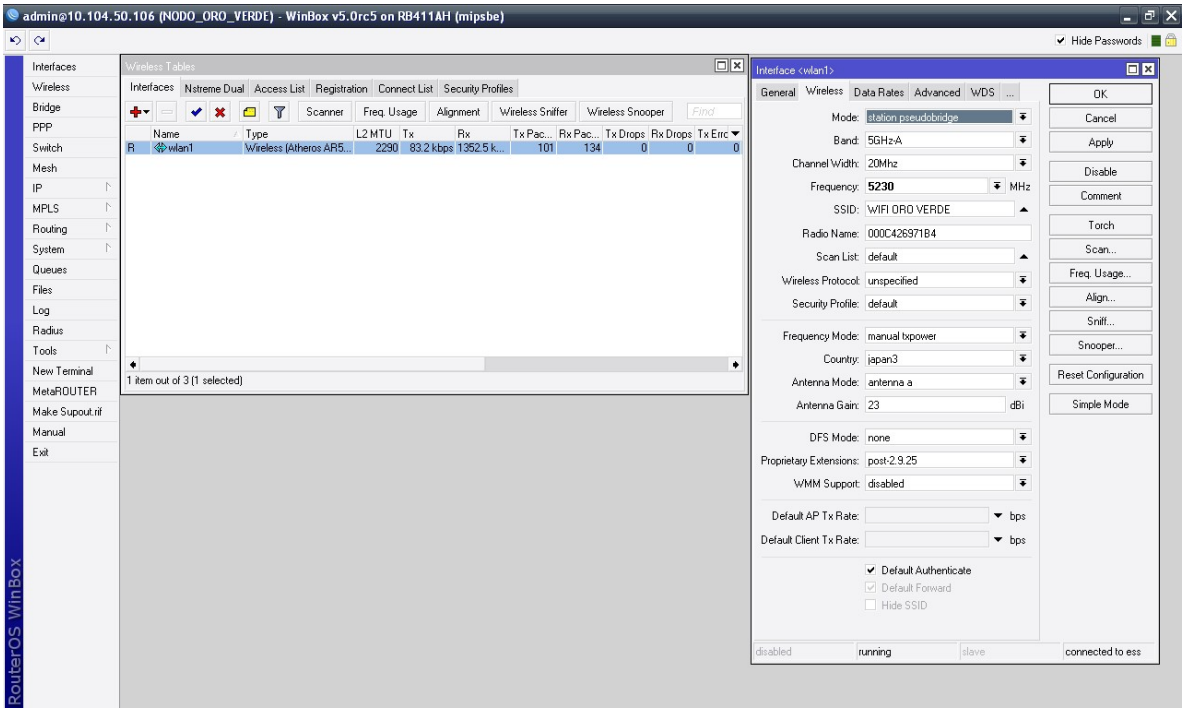
Configuración de las IP’s



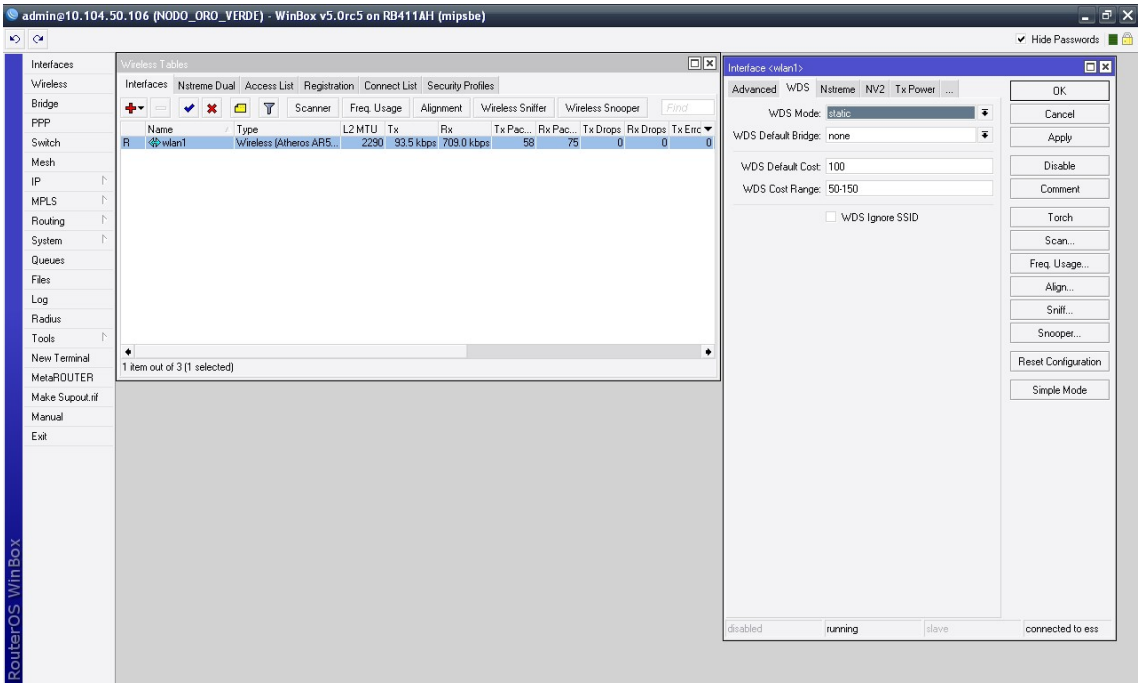
Configuración de la ruta.



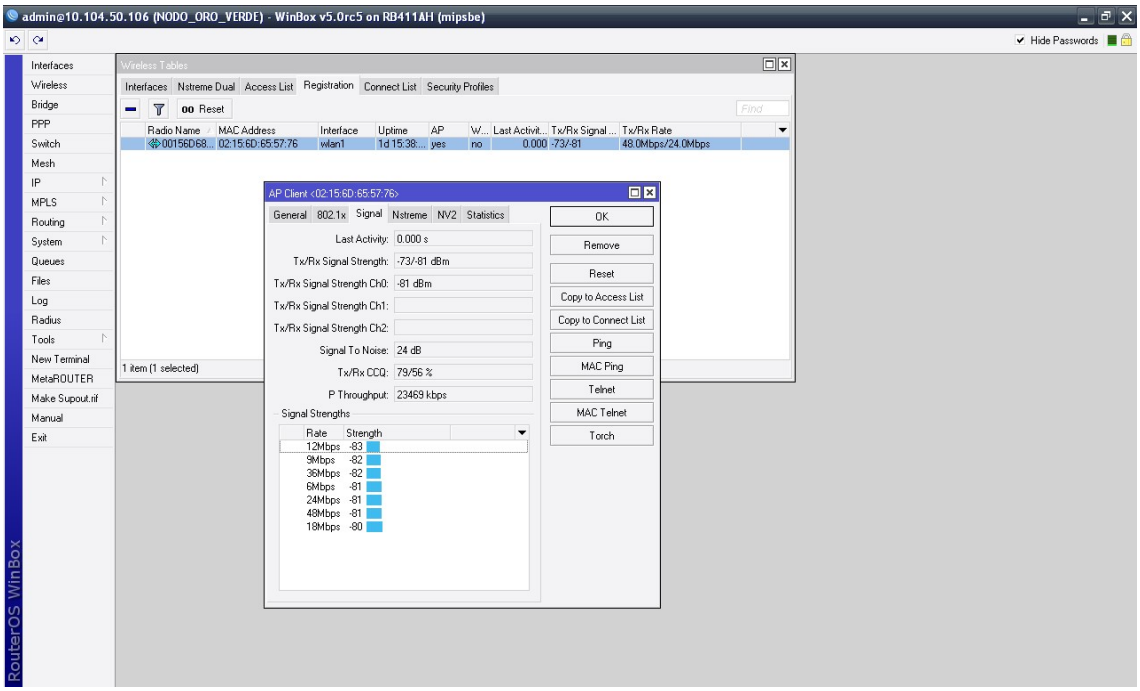
Configuración de la red Inalámbrica.



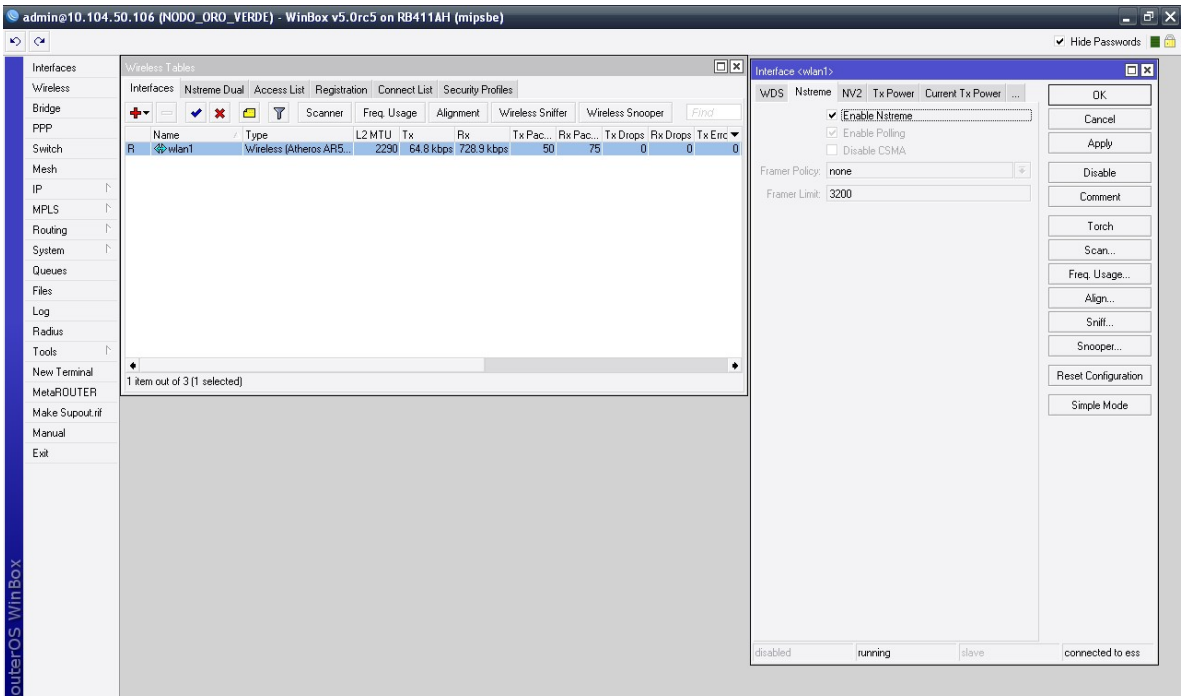
Configuración del WDS



Configuración Nstream



Señal y Throughput.



UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORIZACIÓN DE EMPASTADO

Quito enero 14, 2013
OFI-033-AE-UP-13

Señor
ISRAEL RUBÉN BERMEO CASTILLO
ESTUDIANTE DE LA CARRERA DE SISTEMAS INFORMÁTICOS
UNIVERSIDAD TECNOLÓGICA ISRAEL
Presente.-

De mi consideración:

Una vez revisadas las modificaciones de los informes emitidos, autorizamos al estudiante ISRAEL RUBÉN BERMEO CASTILLO, alumno de la CARRERA DE SISTEMAS INFORMÁTICOS, proceda con la impresión y presentación del empastado para el tema de tesis ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA EL CENTRO DE CÓMPUTO DE UN ISP, para que siga con el proceso de graduación y defensa respectiva.

Cordialmente,

Ing. Miryan Almache
MIEMBRO DEL TRIBUNAL

CC. Secretaría Académica
Archivo Unidad Especial de culminación de estudios y Titulación
/ma