FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

PLAN DE CONTINUIDAD DE NEGOCIO PARA EL DEPARTAMENTO DE IP_MPLS DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT

TRABAJO DE TITULACIÓN PRESENTADO EN CONFORMIDAD A LOS REQUISITOS ESTABLECIDOS PARA OPTAR POR EL TÍTULO DE INGENIERO EN REDES Y TELECOMUNICACIONES

PROFESOR GUÍA
MARCO GALARZA

AUTOR
RODRIGO ALBERTO COBO BENÍTEZ

AÑO
2012

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Marco Antonio Galarza Castillo.
Ingeniero.
0702773250

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Rodrigo Alberto Cobo Benítez

1716385446

DEDICATORIA

Este trabajo está enteramente dedicado a mi pequeño hijo Camilo, como muestra de mi cariño y mi amor.

RESUMEN

Desde los años 70, se ha escuchado acerca de la Continuidad del Negocio, las empresas en el mundo han vivido eventos que han paralizado alguna vez sus operaciones normales, dejando perdidas que no son solo económicas sino también de prestigio, siendo muy pocas empresas las que han desarrollado un plan que les permita volver a su normal operatividad.

En la actualidad, la continuidad del negocio nace con las Tecnologías de la Información (TI), que mediante varias de las disciplinas que la soportan facilitan un debido planeamiento y organización ante un evento, riesgo o desastre que afecte la infraestructura, procesos, activos y provisión de servicios.

Este trabajo muestra un análisis de riesgos que hace una evaluación que facilita el determinar cuáles servicios dentro de la empresa son más relevantes o de mayor prioridad de recuperación que otros, además de una matriz de riesgos en la que se muestra la probabilidad de ocurrencia de los riesgos identificados.

El análisis de impacto al negocio, es el resultado del análisis de riesgos en términos de tiempo de interrupción o paralización de las actividades, que causarían un daño irreversible para la empresa, pero que una vez que ha sido determinado, su resolución es más rápida y eficaz.

Es importante mencionar, que para un Plan de Continuidad como el aquí descrito tenga éxito, es necesario e imperioso desarrollar una cultura organizacional, adecuadas estrategias y la visión del programa de continuidad que se ha abierto, y no confiar solamente en la habilidad para la resolución de problemas.

ABSTRACT

Since three decades ago, the world has heard about Business Continuity, and the companies have lived events that have stopped the normal operations, getting losses that are not only economics also loosing prestige, a few companies have developed or implemented a Plan to help them return to normal operation.

Nowadays, The Business Continuity is born with the Information Technology (IT), through several disciplines that support it and make it easier due to proper organization against events like risks or disasters, affecting the infrastructure, processes or provision of services.

This job shows a Risks Analysis, evaluating and determining which services inside the company are most relevant or which has higher priority than others services, also presents a risks matrix with the probability of occurrence of each identified risk.

The Business Impact Analysis, results of Risk Analysis in terms like, the time of interruption or cessation of activities that would cause irreversible damage to the company, but, once it has been determinate the resolution is faster and effective.

Is very important to mention that, for a Continuity Plan as described here to be successful, is necessary and urgent developing an organizational culture for people, strategies appropriate and vision about the continuity program, and not only trust on the people with abilities to resolve problems.

ÍNDICE.

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

INTRODUCCIÓN

Este proyecto inicia con un diagnóstico que permitirá determinar la situación actual en el Departamento de IP-MPLS de la Corporación Nacional de Telecomunicaciones E.P., se elaborará mediante el diseño de estrategias de recuperación combinando medidas preventivas, que permitan detectar y corregir procesos, minimizando las amenazas, la probabilidad de que ocurra o sus efectos.

Se describirán los procedimientos implementados actualmente, esta información ha sido obtenida de archivos que describen acontecimientos que hasta la fecha han ocurrido en el Departamento de IP-MPLS *(Internet Protocol – Multi-protocol Label Switching)* de la CNT E.P., y que se han constatado en el mencionado departamento.

Se indicará los métodos de las técnicas existentes que señalan los riesgos y el procedimiento que mejor se acomoda a la empresa para su solución. Entonces, se obtendrá la mejor aplicación para el riesgo identificado como potencial daño a los procesos y servicios provistos en la CNT E.P. por el Departamento de IP-MPLS.

También se identificarán las estrategias de recuperación cuantificando los procesos más críticos de operaciones en el Departamento de IP-MPLS de la CNT.

Se presentará un análisis de las aplicaciones que son soportadas por esos procesos, el costo que representa la seguridad de los mismos y el tiempo empleado para su operatividad normal.

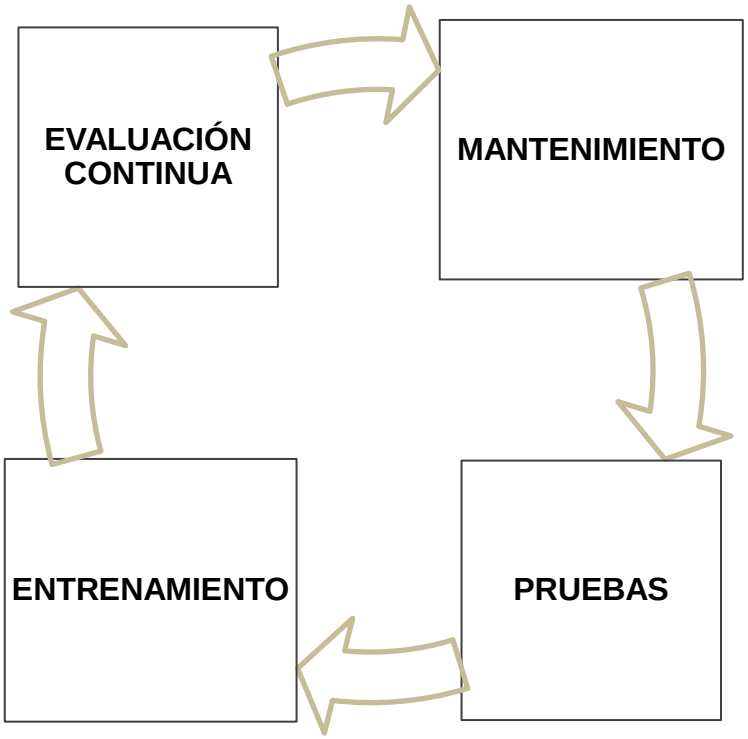
Por otra parte, este proyecto proporcionará mecanismos para restaurar los productos y/o servicios claves a un nivel aceptable y dentro de un marco temporal limitado, realizando un análisis y estudio de los servicios provistos por la CNT en el Departamento de IP-MPLS.

Por lo tanto se dará a conocer la importancia y necesidad de implementar un Plan de Continuidad de Negocio, sus ventajas y desventajas mediante el análisis de impacto del negocio, además de reflejar los resultados para la eficiente y eficaz recuperación de operaciones.

Para conseguir minimizar los efectos de una parálisis en las operaciones se desarrollará un programa de entrenamiento basado en los siguientes aspectos:

Figura 1.

Programa de Entrenamiento para mitigar paralizaciones en las Actividades.



EXPLICACIÓN

“Ecuador ocupó el puesto 108 de 138 naciones incluidas en la nueva edición del Informe Global sobre Tecnología de la Información 2010-2011, el cual fue presentado en Nueva York por el World Economic Forum (WEF), actualmente ocupa el puesto 101 en dicho ranking entre 142 países.

En el periodo de evaluación anterior 2009-2010, cuando se realizó el ranking con 133 países, Ecuador ocupó el puesto 114 y un año antes el lugar 116, el Índice utiliza datos de fuentes públicas y las consecuencias de la Encuesta de Opinión Ejecutiva realizada por el WEF junto con su red de institutos confederados que son los responsables de proveer información, además de coordinar esas encuestas en 8 países de América Latina que son: Honduras, El Salvador, Nicaragua, Costa Rica, Panamá, República Dominicana, Ecuador y Bolivia.

Se debe mencionar que, a nivel mundial, Suecia se mantiene en el primer puesto del Índice, seguido de Singapur, Finlandia, Suiza y Estados Unidos.

En resumen, el informe analiza cuán preparados están los países para utilizar las TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC) de manera eficaz en tres dimensiones: el entorno empresarial, normativo y de infraestructura general; la disponibilidad de los tres actores clave de la sociedad (las personas, las empresas y los gobiernos) para utilizar y aprovechar las TIC y el uso real que se hace de estas.

Ecuador obtuvo las mejores puntuaciones en áreas como la existencia de un mercado competitivo en servicios de Internet y de telefonía, tarifas de telefonía fija y la cantidad de usuarios de telefonía residencial.

Aspectos en que el país debe mejorar son:

- ✓ *Disponibilidad de capital de riesgo necesario y útil para el desarrollo de empresas TIC.*
- ✓ *Calidad del sistema educativo en general dentro de la sociedad y específicamente la calidad de la educación en matemática y ciencias.*
- ✓ *Acceso de las escuelas al Internet, con el uso de redes sociales y capacidad de innovación de las instituciones.*
- ✓ *Eficiencia, eficacia e independencia de un sistema legal para resolver disputas, entre otros.* "http://www. (Forum.)org/)

*L*a Corporación Nacional de Telecomunicaciones CNT E.P., es una entidad pública que proveía en sus inicios telefonía fija como único servicio, actualmente es una empresa que mediante su gran infraestructura facilita servicios de telecomunicaciones a empresas y usuarios.

Es conocido que proveer servicios de telecomunicaciones en cualquier parte del mundo es un campo propicio para tener a la vista escenarios de riesgo a su infraestructura, a todos los clientes suscritos, a sus servicios ya sean de voz, datos y/o video.

Un ejemplo reciente fue el ataque del 11 de septiembre de 2001 en Nueva York al *World Trade Center* (WTC), que tuvo un impacto en las telecomunicaciones sin precedentes, donde los centros de conmutación de AT&T, Sprint y VERIZON fueron destruidos, además VERIZON presentó como principales daños los siguientes:

- ✓ 5 conmutadores de telecomunicaciones.
- ✓ 10 torres del sistema de telefonía celular.
- ✓ 300.000 líneas de voz.

- ✓ 3.6 millones de circuitos ubicados en el área.

He aquí la necesidad de elaborar, desarrollar e implementar un Plan de Continuidad de Negocios para el Departamento de IP-MPLS en la CNT E.P., en el cual se establecerá una guía que señala los métodos, procedimientos y procesos para hacer frente a una contingencia o desastre.

Determinar los métodos, procesos y procedimientos del análisis de la situación actual en el Departamento de IP-MPLS de la CNT E.P., mediante la descripción de operaciones desarrolladas en éste trabajo, con la respectiva evaluación de éstas instrucciones y sus riesgos para establecer puntos específicos de control.

CAPÍTULO I

DETALLE DEL ESTADO DE LAS EMPRESAS EN FORMA GENERAL.

1. ANTECEDENTES.

Toda organización empresarial sin importar el área del negocio en el que actúe busca el éxito y lograr cumplir sus metas con el cliente, que sus productos y servicios tengan un reconocimiento en el mercado al que se dedica, ofreciendo calidad y eficiencia en los mismos, pero ninguna compañía está libre de riesgos como: perder sus productos a consecuencia de un incendio, equipos defectuosos, falta de respaldo de información o paralizar sus operaciones por atentados sobre su infraestructura y hasta errónea manipulación de equipamiento por parte del personal, ante estos eventos las preguntas que surgen en toda organización son:

¿El perfil y rendimiento del negocio resulta afectado?
¿La empresa podrá mantenerse líder y pionera en el mercado frente a este tipo de eventos?
¿Se perdería la confianza y seguimiento en sus servicios por parte de sus clientes?

Estas interrogantes tienen respuesta frente a cualquier desastre natural o humano, del cual sólo dependerá de las proyecciones de la compañía en invertir y aplicar un Plan de Continuidad del Negocio (PCN).

Sin embargo, la realidad es que nos enfrentamos a situaciones en las que las empresas no han planificado una salida inmediata a un desastre o imprevisto empresarial, quedando pendiente por mucho tiempo las soluciones a tomarse en cuenta ante una interrupción de la actividad del negocio.

Se debe indicar que las empresas, sin distinción de la actividad a la que se dedican, en un alto porcentaje no disponen de un Plan de Continuidad de Negocio, al contrario de otras instituciones que se han preocupado por desarrollarlo, pero, nunca lo han probado en su totalidad, y unas pocas se han preocupado de probarlo y ejecutarlo completamente aunque sus resultados no hayan sido los esperados.

Es importante mencionar que todas las empresas que prestan servicios en cualquier campo, más aún en el de telecomunicaciones, deben tener un Plan de Continuidad de Negocio (PCN), el mismo que debe diferenciarse de un Plan de Contingencia (PC), por tal razón se definen a continuación los dos conceptos.

1.1. DEFINICIONES.

En el campo de las empresas de tecnologías y de telecomunicaciones, éstas se deben adaptar y responder tanto a los retos, oportunidades y desastres que pudiesen ocurrir en su contra y en su entorno por diferentes factores tales como: los avances tecnológicos, alta competitividad del mercado, una alta disponibilidad y la confiabilidad de sus servicios, lo que representa para la organización la recuperación de los servicios frente a las amenazas con la implementación de un plan de continuidad.

Aun teniendo vigilancia continua y medidas de protección establecidas, siempre existe el riesgo de que la continuidad del negocio sea interrumpida debido a la presencia de peligros, en consecuencia, estas amenazas crean la pérdida en la estabilidad y confiabilidad de los servicios lo que ocasiona en los clientes un déficit en ingresos por la no comunicación empresarial a la que están expuestos durante estos periodos de paralización en los servicios con su proveedor.

He aquí la necesidad de las empresas en seleccionar la mejor forma para minimizar las amenazas y sus efectos, y al implementar un Plan de Continuidad de Negocio permite a las instituciones la continuidad de sus operaciones de manera eficiente.

1.1.1. PLAN DE CONTINUIDAD DE NEGOCIO PCN.

El Plan de Continuidad de Negocio es un grupo de procedimientos y de acciones propicias que una organización debe acoger en caso de que un determinado tipo de desastre, interrupción o contingencia se materialice e impida su normal funcionamiento.

Estas acciones y/o procedimientos deberán asegurar la recuperación de las operaciones a la mayor brevedad posible, ya que se han determinado como importantes y primordiales para el proceso de proveer servicios y para el negocio.
(www.itcio.es)

Un Plan de Continuidad de Negocio PCN, será detallado y documentado, acogiéndose a las políticas que se manejan dentro de la institución, para que responda ante una emergencia, consiguiendo así reducir el impacto en las operaciones de las entidades en general donde es aplicado. (Martínez, J, 2004)

1.1.2. PLAN DE CONTINGENCIA.

Un Plan de Contingencia PC, es un subconjunto o una porción de un Plan de Continuidad de Negocio PCN, que abarca lo relacionado a cómo reaccionar ante una contingencia que afecte a los servicios provistos por la empresa en cualquiera de sus áreas.

1.1.3. OTROS CONCEPTOS LIGADOS A UN PCN PLAN DE CONTINUIDAD DE NEGOCIO.

Un Plan de Continuidad de Negocio es un concepto que comprende tanto la Planeación para Recuperación de Desastres (PRD), como la Planeación para el Restablecimiento del Negocio (PRN).

1.1.3.1. RECUPERACIÓN DE DESASTRES.

Es la capacidad para responder a una interrupción de los servicios mediante la ejecución de un plan para restituir las funciones importantes y más críticas dentro de la organización.

1.1.3.2. REINTEGRACIÓN DEL NEGOCIO.

Una vez que la crisis ha sido superada, el Restablecimiento del Negocio comprende la normalización de las actividades de la organización.

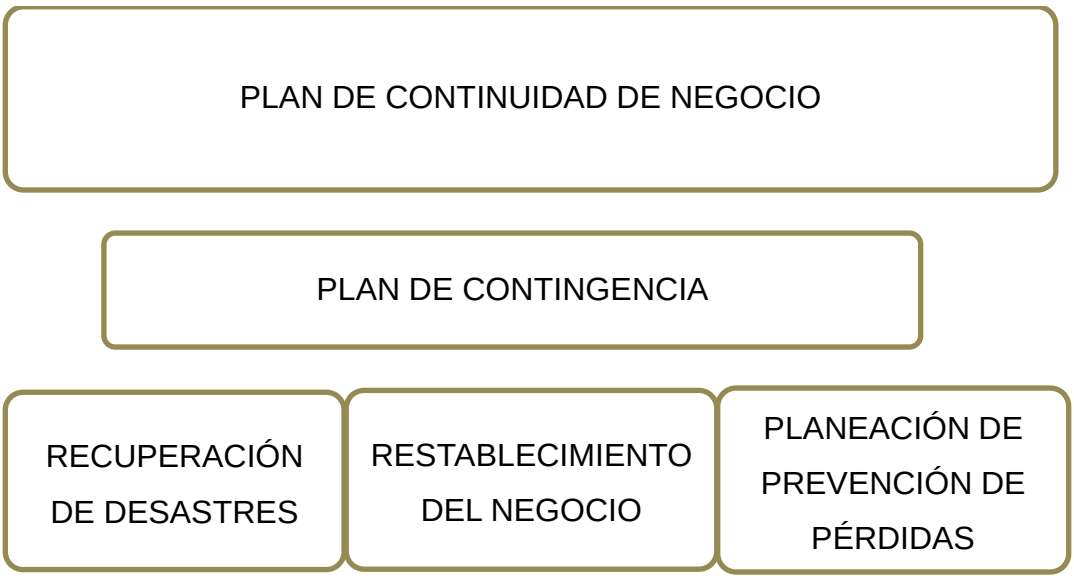
1.1.3.3. PLANEACIÓN DE PREVENCIÓN DE PÉRDIDAS.

Esto involucra que un PCN, debe incluir todas las medidas anticipadas necesarias y de recuperación para cuando se produzca una contingencia que afecte a las actividades de la organización. El PCN es el cómo una organización se prepara para futuros incidentes, que puedan paralizar a la institución y su misión básica a largo plazo, por lo tanto el plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, de acuerdo a las entidades regulatorias,

todo en beneficio de los clientes y de la institución. (Martínez, J, 2004)

Un Plan de Continuidad comprimirá la cantidad de las medidas y la magnitud de las mismas que se toman durante un período en que los errores pueden resultar mayores. (ISEC, Conferencias de Continuidad de Negocio)

Figura 2.
Unidades que conforman el PCN.



1.2. ¿CUÁNDO IMPULSAR EL PLAN DE CONTINUIDAD DE NEGOCIO?

Directamente afín a que cualquier detalle que interrumpa en los procesos de negocio, o que detenga la operación de las empresas, sin importar el área de desempeño, es obligación y competencia de los directores o encargados de las organizaciones decretar la necesidad de la aplicación y seguimiento de un Plan de Continuidad de Negocio que cubra y ofrezca la protección adecuada a las actividades, procesos,

servicios importantes y críticos de las áreas que están bajo su responsabilidad.
(ISEC, Conferencia Continuidad de Negocio)

Es importante indicar que:

Un Plan de Continuidad de Negocio, no se basa expresamente en recuperar los servicios e infraestructuras de Tecnologías de la Información, sino que más bien, se encarga de minimizar sus efectos y la probabilidad de que ocurran o de que se repitan a través de lineamientos que mejoren los ya existentes.
(esa) http://www.esa-security.com

Cuando las organizaciones colocan la investigación o información en soportes que son tratados por las tecnologías implementadas en cada una de las empresas según su área de trabajo, los planes de eventualidades deberían ser de uso común en cada una de ellas.

En definitiva, no son más que medidas preventivas, de buena práctica empresarial para su seguridad, garantizando que la actividad de esa organización está debidamente respaldada y su continuidad garantizada.

La activación de un Plan de Continuidad de Negocio, debería producirse solamente en situaciones de emergencia y cuando las medidas de seguridad hayan fallado.

El Plan de Continuidad de Negocio, servirá para proteger los procesos críticos del negocio en el Departamento de IP_MPLS,

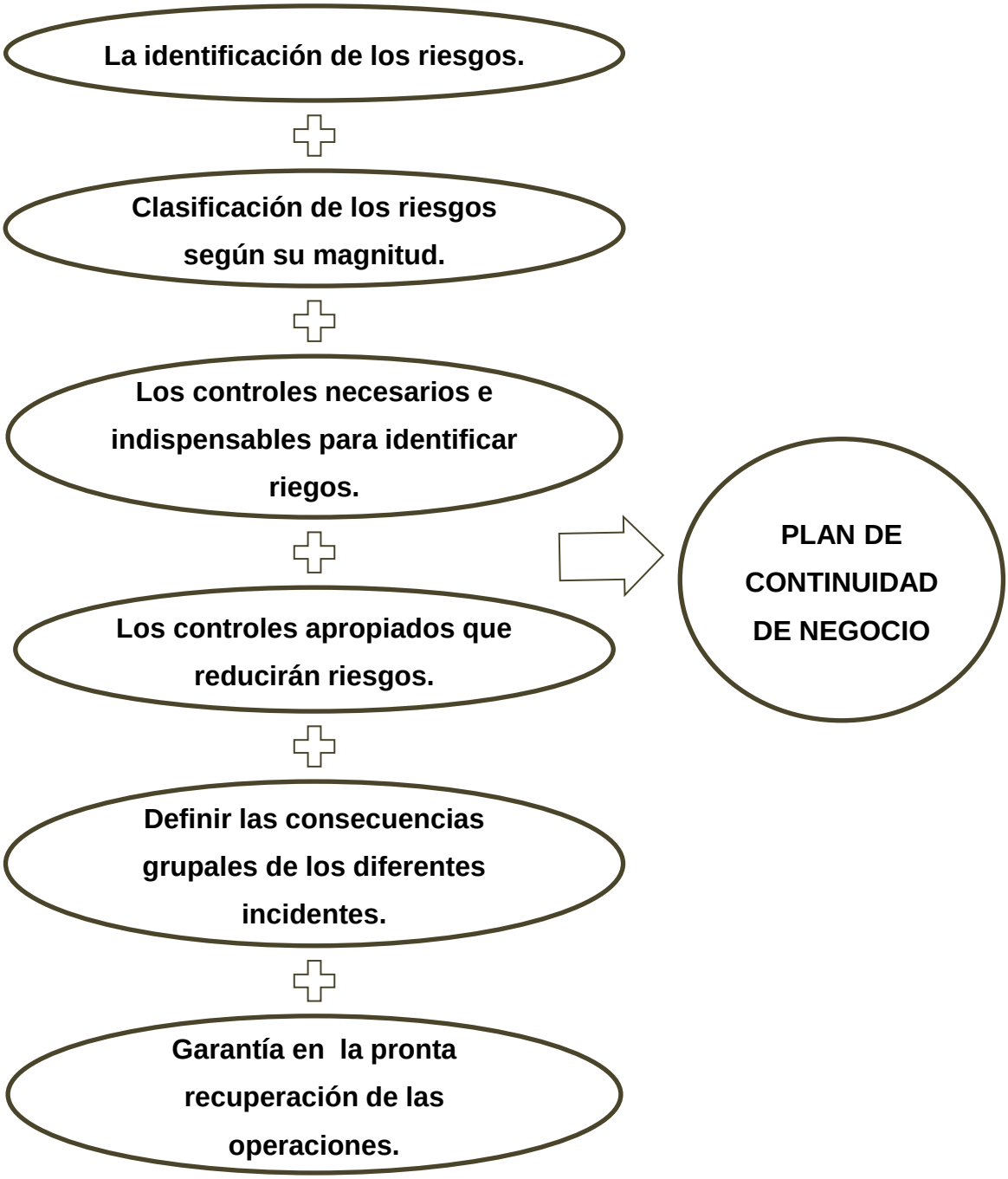
contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan tener tales como pérdidas de tipo financiero, confiabilidad, credibilidad, productividad, etc., debido a la no disponibilidad de los servicios que ésta área provee a los clientes, el Plan de Continuidad del Negocio, busca mitigar el riesgo a dichas fallas o desastres, mediante un plan que guíe y permita la pronta recuperación de sus operaciones en caso de presentarse algún evento que afecte el flujo normal de las actividades de la empresa.

1.3. ¿QUÉ DEBE CONCENTRARSE EN UN PLAN DE CONTINUIDAD DE NEGOCIO?

Un Plan de Continuidad de Negocio deberá incluir:

Figura 3.

Elementos que incluye un PCN.



1.4. RIESGO, INTERRUPCIÓN Y DESASTRES.

A continuación se definen tres de los motivos por los que una empresa como la Corporación Nacional de Telecomunicaciones debe contar con un Plan de Negocio para el Departamento de IP-MPLS, y que están ligados con el tipo de operaciones que realiza la empresa en todas sus áreas de mercado, tanto por las tecnologías, operaciones, negocios y servicios que provee. (Site Security Handbook, 1991)

1.4.1. DEFINICIÓN DE RIESGO.

Un riesgo, representa la eventualidad de que una amenaza se presente y que sus consecuencias para la organización a la que afecta, sea una interrupción o la pérdida en los servicios que provee.

El tener una debilidad no representa un peligro, y las amenazas siendo identificadas pueden ser controladas, pero si se juntan debilidad y amenaza se convierten en un peligro, es decir, se incrementa la posibilidad de que ocurra un desastre.
(Conferencia. Gestión de Riesgos, Mañas, J.)

1.4.2. DEFINICIÓN DE INTERRUPCIÓN.

Es la paralización del flujo y operaciones normales del negocio durante un período de tiempo, provocadas por factores operativos y/o humanos.

1.4.3. DEFINICIÓN DE DESASTRE.

Se relaciona como cualquier evento accidental, malicioso o natural que amenace o rompa con el flujo normal de las operaciones o servicios críticos del negocio, por un tiempo tal que, sea suficiente para afectar financiera, estratégica y operacionalmente a la compañía pudiendo desorganizar la Continuidad del Negocio.

1.5. IDENTIFICACIÓN DE LOS TIPOS DE INCIDENTES Y/O FALLOS.

Además de los imprevistos ambientales que pueden causar daños adversos a la infraestructura de la CNT E.P., tenemos otro tipo de incidentes, como los que se detallan a continuación:

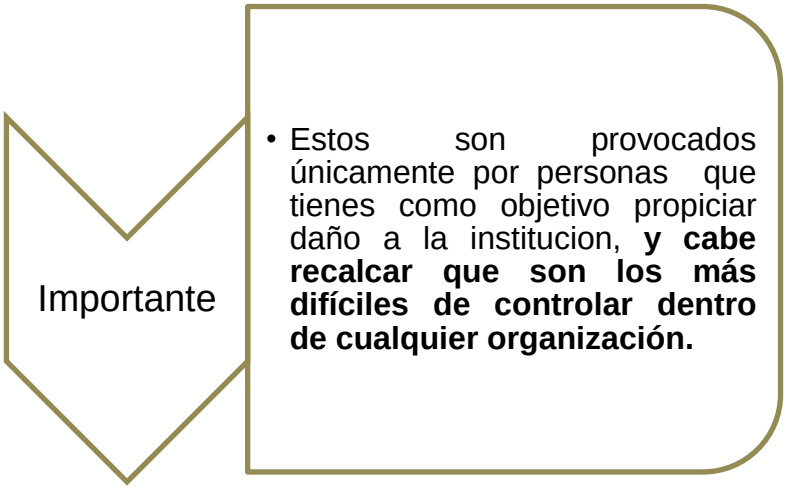
1.5.1. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Con la finalidad de evitar cualquier evento malicioso dentro del campo de los incidentes de seguridad, se deben establecer dentro del Plan de Continuidad de Negocio, los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de los mismos.

Así, las políticas manejadas en lo concerniente a la gestión de incidentes en seguridad de la información están dirigidas a todas las personas que tengan acceso a los sistemas informáticos o a información primordial de la institución, incluso aquellos encargados mediante contratos con empresas proveedoras de equipamientos y/o servicios. (Huerta, A, 2000)

Figura 4.

Difícil control de incidentes, causados por personal.



Así, se pueden mencionar los siguientes:

- ✓ Incidentes de seguridad en los sistemas (políticas ajustadas, definidas o establecidas de manera contraria y/o errónea a las requeridas en la empresa).
- ✓ Delitos informáticos (provocados por Hackers).
- ✓ Introducción de virus o malware (código malicioso en información de usuarios).
- ✓ Venta de la información.
- ✓ Borrado de la información.
- ✓ Destrucción de información.
- ✓ Alteración o manipulación de la información.
- ✓ Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
- ✓ Abuso y/o mal uso de los servicios informáticos internos o externos que requieren autenticación.
- ✓ Intentos recurrentes y no recurrentes de acceso no autorizado.
- ✓ Distribución accidental o premeditada de la información.

- ✓ Fallos en los sistemas de información.
- ✓ Caídas de operación en los sistemas.

(Proctor, PE, 2005, www.nist.org)

1.5.2. INCIDENTES EN LA INFRAESTRUCTURA DE EDIFICIOS O EN LOS SERVICIOS PROVISTOS POR EMPRESAS PÚBLICAS U OTROS.

Los incidentes en la infraestructura podrían ser causados por:

- ✓ Incidentes en el suministro eléctrico.
- ✓ Incidentes en las comunicaciones.
- ✓ Fallos en cableado eléctrico.
- ✓ Sistema de suministro de agua defectuoso.

1.5.3. INCIDENTES EN LOS EQUIPOS O EN LA INFRAESTRUCTURA DE RED.

Una vez que el administrador de la red de datos notifica la necesidad de renovación tecnológica, se definen las acciones a seguir, luego, se establece las acciones para realizar este tipo de actualizaciones, siguiendo las recomendaciones de los fabricantes del hardware y los procedimientos indicados para administrar la realización de dichos cambios. (Site Security Handbook, 1991)

Por lo tanto, los incidentes en los equipos o la infraestructura de red se deben generalmente a:

- ✓ Equipamientos con desperfectos en su fabricación.
- ✓ Falta de mantenimiento periódico.
- ✓ Equipos que no cumplen con las especificaciones requeridas ni entregadas por el fabricante.

- ✓ Incidentes en las fuentes de alimentación a base de baterías.
- ✓ Daños en los equipos de aire acondicionado.
- ✓ Interrupción de los servicios de red y acceso a los sistemas de información.

1.5.4. INCIDENTES EXTERNOS.

Son todos aquellos incidentes provocados por agentes ajenos a la institución pero provocados por cualquiera de las que se mencionan en el siguiente listado.

- ✓ Revoluciones civiles y/o militares
- ✓ Guerras
- ✓ Deslaves
- ✓ Robos
- ✓ Huelgas.
- ✓ Incendios.
- ✓ Inundaciones.
- ✓ Desastres naturales (terremotos, tsunamis, huracanes, ciclones, maremotos, erupciones volcánicas, etc.).
- ✓ Pandemias.
- ✓ Hechos de conmoción nacional.
- ✓ Sabotajes.
- ✓ Actos de terrorismo.
- ✓ Daños premeditados.

(Huerta, 2000)

1.6. ANÁLISIS DEL IMPACTO SOBRE EL NEGOCIO (AIN).

En definitiva, uno de los componentes esenciales de un PCN, es realizar un Análisis del Impacto sobre el Negocio (AIN), siendo ésta la

inicial acción a tomar para el desarrollo de un PCN, ya que mostrará las falencias, debilidades y fallas *operativas por inactividad de la empresa, sus procesos críticos y los requisitos de tiempo de recuperación acordados necesarios*, pero asignando prioridades a las estrategias de recuperación que pudieran ser necesarias durante una interrupción extendida de la actividad en los servicios (varias horas, días o semanas).

1.6.1. REPRESENTACIÓN DEL ANÁLISIS DEL IMPACTO SOBRE EL NEGOCIO.

Se debe considerar principalmente la cantidad de recursos y tiempo empleado para realizar un AIN que dependerá del tamaño y complejidad del área en la que se lo implementará.

El AIN, es una de las fases más importantes del PCN, pues en ésta etapa los riesgos identificados en las operaciones, área o procesos principales de la empresa, serán priorizados y categorizados de acuerdo a su impacto para posteriormente establecer las estrategias de reparación mediante la determinación de los tiempos de recuperación.

En conclusión, el AIN nos permitirá identificar el impacto operativo de cada uno de los riesgos identificados en el Departamento de IP-MPLS de la Corporación Nacional de Telecomunicaciones E.P.

1.6.2. ¿QUÉ ENCIERRA EL ANÁLISIS DE IMPACTO SOBRE EL NEGOCIO?

El análisis del impacto sobre el negocio incluye los siguientes ítems:

1.6.2.1. RIESGO RESIDUAL.

Se describe como el riesgo teórico, es deducido en la elaboración del análisis de riesgos en la etapa del Planeamiento, tomando en cuenta que aun después de aplicar soluciones, éste persiste.
(Conferencia. Gestión de Riesgos. Mañas, J)

Resultando como el ciclo lógico del planeamiento, el siguiente:

Figura 5.
Ciclo lógico para encontrar el Riesgo Residual.

EL PROYECTAR	• Implantacion de los contenidos. • Evaluación del riesgo • Planificación en la relacion del riesgo • Conformidad de riesgo.
EL HACER	• La elaboracion del plan en el proceso del riesgo.
EL CONSIDERAR	• Revisión periodica y continua de los riesgos.
EL PROCEDER.	• Proceso de mejora en la gestión de riesgos y seguridad de la información.

Según la norma ISO 27OO5 en lo concerniente al Riesgo Residual en síntesis dice lo siguiente:

“La fineza para establecer riesgos, incidentes o amenazas, estará ligado a los resultados y a la evaluación de los mismos, considerando que éste permanece o persiste aun después de que las gerencias y encargados del área aplican una respuesta de acción, además realizar una prueba adicional con otro tipo de evaluación para los riesgos con diferentes parámetros, por ejemplo: valoración del riesgo mediante una matriz de riesgos con valoraciones diferentes, aceptación del riesgo con su respectiva escala de riesgo, o criterios de impacto.” (ISO 27005)

Ante esto, las opciones a elegir en la identificación de los riesgos y su respectivo valor residual es:

- ✓ Pasar la responsabilidad a otro: por ejemplo, con la contratación de un seguro, aunque resulte costoso a largo tiempo.
- ✓ Terminar por abandonar la actividad: considerando su alto nivel de riesgo.
- ✓ Reducir el nivel de riesgo, fortaleciendo los controles o con la implantación de nuevos controles.

1.6.2.2. ESTADO MÁXIMO DE INTERRUPCIÓN DE LOS SERVICIOS.

Cuando este tiempo supera lo previsto, las pérdidas sufren un aumento significativo y las funciones no podrían ser reanudadas.

Una vez que está establecido el objetivo y visión del negocio, los procedimientos que lo componen, y la importancia de los procesos de cada uno de ellos, debemos establecer los tiempos de recuperación.

Teniendo en cuenta que el objetivo del Plan es dar continuidad al negocio tras un incidente o contingencia grave con las menores pérdidas operativas funcionales y económicas posibles para la empresa, debe estimarse para cada uno de los procesos que se han considerado críticos, el tiempo a partir del cual las pérdidas económicas afectarían de forma grave a la organización, entonces éste se convierte en el Tiempo Máximo de Recuperación o de Interrupción**.**

Un ejemplo del estado Máximo de Recuperación, es que pueden hallarse procesos en los que el tiempo de reparación es muy pequeño (algunas horas), como la prestación y provisión del servicio de telefonía pública básica, pero distintos procesos, como la facturación a clientes y consumidores en una empresa de servicios como en Hosting, alguna entidad financiera o Bancaria, y en un ISP, pueden tener un periodo de recuperación mayor (nos referimos a varios días o varias semanas según la gravedad del incidente) ya que se inmiscuyen tecnologías y equipamientos de proveedores heterogéneos, dedicando varios servicios sobre una misma red y en un mismo espacio físico, siendo éste el mejor de los casos por la cercanía del equipamiento.

He aquí la valoración importante respecto a seleccionar la estrategia de respaldo adecuada a las necesidades de recuperación de las operaciones en la empresa.

Además estos tiempos deberán estar sujetos a los reglamentos de instituciones estatales regulatorias como el CONSEJO NACIONAL DE TELECOMUNICACIONES (CONATEL) y la SECRETARIA NACIONAL DE TELECOMUNICACIONES (SENATEL).

CONATEL Consejo Nacional de Telecomunicaciones.

Es el organismo encargado de la regulación y administración de las telecomunicaciones en el Ecuador, a través de la implantación de políticas que motiven el acceso de los usuarios a servicios de telecomunicaciones con calidad, y que sus proveedores desarrollen sus actividades en un escenario de leal competencia.
Entre las actividades del CONATEL están:

- ✓ *Velar por el estricto cumplimiento y respeto a los derechos de los usuarios en materia de servicios de telecomunicaciones.*
- ✓ *Consolidar la apertura del mercado de las telecomunicaciones en el país que elimine las distorsiones existentes y que atraiga la inversión.*
- ✓ *Incentivar la participación del sector privado en el desarrollo de infraestructura y prestación de servicios de telecomunicaciones en un marco de seguridad jurídica y de libre y leal competencia.*
- ✓ *Fortalecer la presencia del Ecuador en la esfera subregional, regional y mundial en materia de telecomunicaciones.*
- ✓ *Promover un cambio del marco legal acorde a los avances tecnológicos y de libre mercado.*
- ✓ *Propender a que la sociedad ecuatoriana obtenga el acceso y servicio universal de telecomunicaciones en forma ágil, oportuna, con calidad adecuada y a precios justos.*
- ✓ *Promover el uso de las Tecnologías de Información y Comunicación (TICs) para garantizar el acceso de todos los ecuatorianos a la Sociedad de la Información.*
- ✓ *Fomentar el acceso y uso de Internet, así como sus aplicaciones en el ámbito social como educación y salud.*

SENATEL Secretaria Nacional de Telecomunicaciones.

Es la entidad encargada de la administración y regulación del espectro radioeléctrico en el Ecuador, los servicios de telecomunicaciones, radio y televisión.

Entre las actividades del SENATEL están:

- ✓ *Optimizar el uso de recursos y control de gasto corriente.*
- ✓ *Uso intensivo de medios electrónicos.*
- ✓ *Seguridad, integridad y confidencialidad de la información.*
- ✓ *Fortalecimiento del talento humano.*
- ✓ *Fomentar la permanente formación y capacitación del personal técnico especializado en las tecnologías de nueva generación y regulación aplicables.*
- ✓ *Mantener el sistema de gestión de calidad y mejoramiento continuo en los procesos internos.*

  (www.conatel.gob.ec)

1.6.2.3. DETERMINACIÓN DE PROCESOS CRÍTICOS.

Basada en la importancia misma de los servicios provistos en la empresa, y de los procesos que han de ser clasificados de acuerdo a la disponibilidad, actividad, operatividad, calidad de servicio y demanda por los clientes, ya que estas prestaciones, son las solicitadas por los usuarios y empresas de acuerdo a la actividad de cada uno de ellos. (ISEC. Conferencias de Seguridad de la Información)

1.6.2.4. IMPACTO PARA LA EMPRESA.

Frente a los incidentes detallados anteriormente, tenemos varios factores que afectaran a la imagen, a los procesos, procedimientos habituales de trabajo, que a su vez, conllevan a las consecuencias no deseadas de la corporación, y que se deberán tomar en cuenta como las que se mencionan y figuran como impacto directo sobre la empresa. (ISEC. Conferencias de Seguridad de la Información)

Figura 6.

Elementos que impactan a la Continuidad del Negocio y sus Actividades.

1.6.3. RELACIÓN DE DEPARTAMENTOS Y USUARIOS.

Se puede ligar departamentos y usuarios ya que ocupan el mismo espacio dentro de la organización, por ende, los procesos en cualquier organización están gestionados por usuarios y a su vez en departamentos, dentro del inventario de procesos es necesario conocer el personal involucrado en los mismos.

Como guía, ésta información puede obtenerse en las mismas entrevistas donde se recoge la información de los procesos existentes y de los elementos, es decir, el hardware y software que lo integran. (http://www.ulpgc.es)

1.6.3.1. RELACIÓN DE DEPARTAMENTOS.

Se deberán plantear, identificar y dirigir los departamentos existentes en las instituciones en las que se implemente un Plan de continuidad de Negocio.

1.6.3.2. RELACIÓN DE LOS USUARIOS.

Se deberá organizar cada uno de los nombres de las personas que integran los departamentos y las áreas que intervienen en los procesos internos.

1.6.4. PREPARACIÓN DE LA RELACIÓN DE PROCESOS.

Se deberá establecer los procesos operativos y de negocio que se realizan en la compañía.

Para obtener la información sobre los procesos y las aplicaciones que los gestionan, es esencial la participación de las personas responsables de los mismos dentro de la organización o las

empresas en general, y de aquellos trabajadores que conocen en profundidad los mismos.

Para lograrlo se realizará, entrevistas personales y cuestionarios que nos acercarán a los procesos críticos del negocio en la empresa.
Podemos dividir los procesos en operativos y procesos de soporte. (ISEC. Conferencias de Seguridad de la Información)

1.6.4.1. LOS PROCESOS OPERATIVOS.

Son aquellos que guardan una relación directa con el cliente. Aquí se pueden mencionar la utilización de los servicios provistos por la institución como telefonía, internet, canales de datos, enlaces dedicados sobre diferentes medios de transmisión y tecnologías como: par de cobre, fibra óptica, microondas, enlaces satelitales, etc.

1.6.4.2. LOS PROCESOS DE SOPORTE.

Serían aquellos que facilitan los recursos al cliente, para poder realizar los procesos operativos (recursos humanos, gestión financiera, facturación, almacenaje, atención al cliente, etc.)

1.6.5. PREPARACIÓN DE LA RELACIÓN DE APLICACIONES.

Establecer la reciprocidad de las aplicaciones que soportan los procesos de la empresa, en este punto se debe recolectar el inventario de los recursos tecnológicos que soportan los procesos de la CNT y que básicamente están determinados para cualquier institución en cualquier área de las telecomunicaciones, a fin de

identificar aquellos que den soporte inmediato y directo a los servicios críticos. (ISEC. Conferencias de Seguridad de la Información)

Como se ha mencionado, los recursos tecnológicos sirven para optimizar procesos, tiempos, e incluso recursos humanos, acelerando el trabajo y los tiempos de respuesta que al final siempre afectan positivamente en el rendimiento y en la mayoría de los casos (relación cliente – proveedor de servicios) en la preferencia del consumidor final.
Precisamos a la relación de aplicaciones como el uso profundo de los recursos tecnológicos, para el logro de objetivos dentro de una estructura como la de CNT.

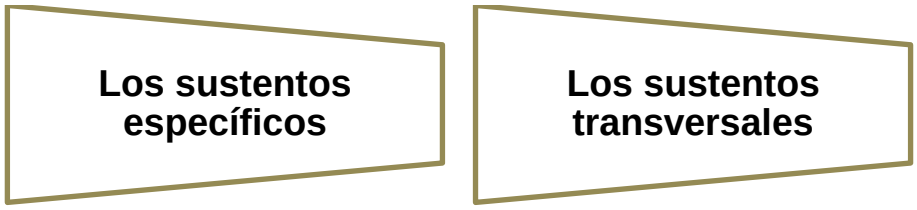
Algunos factores del porqué podemos utilizar los Recursos Tecnológicos se detallan en el siguiente cuadro:

- ✓ Para el cumplimiento y soporte de las normativas en las operaciones de la organización.
- ✓ Para facilitar los servicios con recursos tecnológicos actualizados.
- ✓ Para mejorar los servicios con la tecnología disponible e instalada.
- ✓ Como soporte de operación en los servicios.
- ✓ Para agilizar y mejorar la comunicación del personal.
- ✓ Para la creación de redes de información debida y claramente documentadas.
- ✓ Rapidez y facilidad que brindan.
- ✓ Para dar agilidad a los procesos.

1.6.5.1. SUSTENTOS TECNOLÓGICOS.

Los tipos de sustentos que se analizan son:

Figura 7.
Sustentos Tecnológicos.



11.6.5..1. LOS SUSTENTOS ESPECÍFICOS.

Los sustentos específicos incluyen los siguientes:
(ISEC. Conferencias de Seguridad de la Información)
Concerniente a herramientas, equipos, instrumentos, materiales, máquinas, dispositivos y software específicos necesarios para lograr el propósito técnico establecido, tomando como mas importantes los mencionados a continuación:

HARDWARE.

Identificando cada uno de los elementos de hardware que soportan los Sistemas de Información de la organización (como son: documentos, manuales, procedimientos, personas, hardware, software, bases de datos).
Entre los dispositivos: Routers, switches, laptops, PC de escritorio, bridges, módems, Access point, centrales, impresoras, centros de gestión, etc. (Huerta, 2000)

SOFTWARE.

Recogiendo todos aquellos componentes de software, incluido todos los asociados al sistema operativo, indispensables para el funcionamiento y optimización del Sistema de Información de la empresa. (Windows, Linux, Unix, etc.). (Huerta, 2000)

SOFTWARE Y SU SET APLICACIONES.

Inventariando las aplicaciones de gestión que son utilizadas en la compañía. Estas plataformas son necesarias y provistas para el funcionamiento de las tecnologías disponibles en la organización y por cada proveedor.
(ISEC. Conferencias de Seguridad de la Información)

INSTALACIONES FÍSICAS.

Considerando aquellos elementos o componentes que sin disponer de una tecnología requieren de una plataforma para su funcionamiento, ésta, está enfocada propiamente al tratamiento de la información donde si son requeridos para garantizar la operatividad del servicio.

Dentro de la infraestructura física consideramos:
El espacio físico para el uso y el almacenamiento de los recursos: laboratorios, centrales telefónicas, nodos, (COMAGs) Centros de Operación, Mantenimiento, Administración y Gestión, departamento comercial, bodegas, etc.

11.6.5..2. LOS SUSTENTOS TRANSVERSALES.

Estos sustentos son de tipo imperceptible, pudiendo ser identificados y catalogados como el capital humano y de estructura departamental o de manera simple como información o conocimiento.

De manera que, el sustento transversal es aplicable para el mejoramiento de los procedimientos que se aprovechan sobre un sistema establecido como: cadena de valor empresarial, unidad estratégica de negocios, y demás componentes.

Para citar los sustentos transversales podemos nombrar:

- ✓ Manejo de los procesos, por conocimiento del personal.
- ✓ Los procesos y métodos han sido documentados o codificados.
- ✓ Personal que introduce en procesos técnicos, documentándolos y registrándolos dentro en un historial de control.
- ✓ Estructura organizacional asociada a la actividad técnica.
- ✓ Áreas, personal, proveedores y usuarios con los que se tiene dependencia operativa.
- ✓ Información necesaria para los procesos técnicos de la organización.

1.6.6. ANÁLISIS OPERATIVO.

En el análisis operativo, se procederá a medir los impactos negativos resultantes de la ocurrencia de un evento que pudiera

llegar a interrumpir el proceso de operaciones en las diversas áreas que se encuentran involucradas con su departamento de IP_MPLS en la CNT.

La ponderación considerada para el análisis operativo de la compañía, estará basado directamente al grado de la magnitud del daño que afectaría en la proyección como por ejemplo: caída de los sistemas de operación, eventos de conmoción nacional, hechos vandálicos en contra de la infraestructura de la organización, etc., tomando en consideración las pérdidas operacionales y funcionales.

De este análisis nacen interrogantes como por ejemplo:

- ✓ ¿Cuáles son los *recursos* afines con los procesos críticos del negocio?, y el más importante,
- ✓ ¿Cuál es el período *de recuperación crítico* para los recursos de información en el cual se debe establecer el procesamiento del negocio, antes de que se produzcan pérdidas totales de los servicios provistos o la pérdida de clientes?

Se puede entender que los accidentes afectan en ocasiones muy seriamente y de forma diferente a cada sección de la empresa dependiendo de su área de actividad sin importar el tamaño que esta tuviere.

Otros efectos provenidos de un desastre, interrupción o paralización de las actividades y servicios provistos por la organización, que pueden causar un gran impacto son la pérdida de reputación frente a los clientes y la pérdida de ventaja competitiva con otras compañías.

1.6.7. ANÁLISIS DE RIESGOS.

Para el análisis de inseguridades se debe identificar y analizar los incomparables detalles o factores de riesgo que fortuitamente podrán aparecer afectando a las actividades que se desea proteger.

La estimación de riesgos, siempre contempla que algo o alguien puede fallar, y a continuación estimar las consecuencias que resultarían para la institución frente a estos hechos, es decir, es el proceso que permite el evaluar los riegos y su impacto.

Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles, de ésta forma, se pueden priorizar los problemas y su consecuencia potencial desarrollando un plan adecuado.

Por lo tanto, la dirección de los riesgos es la facilidad de aprovechar el análisis de riesgo para trazar estrategias óptimas que admitan la reducción significativa o la mitigación de los mismos.

CAPÍTULO II

2. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL EN LA CNT E.P. Y SU DEPARTAMENTO DE IP_MPLS.

(*Internet Protocol – Multi-protocol Label Switching*)

Mensualmente en la Corporación Nacional de Telecomunicaciones CNT E.P., se instalan mediante órdenes de trabajo generadas por el área de ingeniería, SWITCH IP en localidades que no cuentan con equipamiento IP, para la entrega de servicios masivos y corporativos a los usuarios.

Mediante el Plan de Ampliación de la red del departamento de IP_MPLS en la Corporación Nacional de Telecomunicaciones, se ha contemplado equipamiento en las capitales de provincias, sin embargo existe requerimiento de localidades intermedias en las cuales se cuenta con infraestructura de fibra óptica, pero aún no se dispone del equipamiento IP.

Se ha realizado también, un análisis comercial encontrando que existe la demanda de infraestructura IP insatisfecha en varias localidades a nivel nacional.

Se identificaron los sitios que cuentan con infraestructura de fibra óptica como parte del Proyecto de la Red Nacional de Transmisión y de las facilidades para la instalación de SWITCH IP o reemplazo de los equipos existentes para mejorar capacidades y la provisión de nuevos servicios.

Ante ésta situación se han identificado las siguientes causas y efectos en el desarrollo del negocio en la CNT E.P., ya que la demanda por los servicios que provee es mayor al crecimiento de la capacidad para ofertarlos que actualmente posee.

Las causas detectadas son las siguientes:

- ✓ Las localidades intermedias no han sido consideradas en la ampliación de la red IP.
- ✓ La información de la demanda de los servicios prestados por la CNT, está desactualizada.
- ✓ Proyectos de reemplazo de equipamiento IP de baja capacidad han sido programados a mediano y largo plazo.
- ✓ No se ha realizado un análisis de mercado del sector corporativo.
- ✓ La saturación de equipos existentes en varias localidades.

Los efectos de la problemática son:

- ✓ Demora en la atención de órdenes de trabajo.
- ✓ Demanda Insatisfecha de servicios IP en varias localidades del país.
- ✓ Bajo posicionamiento de la empresa CNT E.P en zonas no atendidas.
- ✓ Pérdida de clientes que optan por otros proveedores.

2.1. ANTECEDENTES:

TECNOLOGÍA, PROCESOS, PERSONAL, ACTIVIDADES.

2.1.1. TECNOLOGÍA.

Las diferentes redes que maneja la Corporación Nacional de Telecomunicaciones que funcionan actualmente dentro de su infraestructura tecnológica son:

- ✓ **BACKBONE ATM NORTEL.**
  (Inicio Operación NOV_2001).

  Se encuentra operativa desde hace 10 años, ésta red era el Backbone de la CNT, soportaba todo el tráfico de esos años. Se conserva en operación por que aún existen usuarios y empresas que mantienen sus troncales ATM (*Asynchronous Transfer Mode, que es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda capacidad de transmisión para servicios y aplicaciones;* que ofrece un servicio orientado a conexión gracias a los VP (*Virtual Paths*) y los VC (*Virtual Circuits*)) y se niegan a migrar debido a la fiabilidad que les ha brindado esta red durante todos estos años.

  Sin embargo, entre varias de las restricciones de esta red son:

  - ✓ el limitado Ancho de Banda.
  - ✓ su alto costo.
  - ✓ y el mantenimiento requerido de sus componentes.

  Ante esta situación, ya existe un acuerdo para migrar a la red IP en Julio del 2012.

- ✓ **AAA-BRAS HUAWEI.**
  (Inicio Operación DIC_2003).

  Actualmente lo que es la red BRAS está constituida por los servidores que asignan las Direcciones IP a los usuarios finales, y están unidos a una plataforma inteligente llamada

AAA (plataforma convergente en la que se produce la autenticación).

El BRAS de la Corporación Nacional de Telecomunicaciones, es el espacio de interconexión con el tráfico de información para los usuarios, suministrando al mismo tiempo la capacidad de integrar protocolos como IP[1], ATM[2] o PPP[3], además, brinda la facilidad en la administración de políticas de QoS[4] (Calidad de Servicio) entre la red de accesos (fibra óptica, cobre o Inalámbrico WIMAX[5]) y la PSN (*PUBLIC SWITCHED NETWORK* - Red Pública Conmutada)

AAA (*Authentication, Authorization and Accounting*), Red de servicios de seguridad que proporcionan el marco básico para establecer control de acceso en un router o un servidor de acceso. Es flexible, escalable y soporta múltiples métodos de autenticación

---

[1] IP.- INTERNET PROTOCOL. Aunque es un protocolo que no garantiza la entrega de paquetes es uno de los más importantes, es un protocolo no orientado a conexión de nivel 3, cuenta con un direccionamiento de 4 bytes.

[2] ATM.- ASYNCHRONOUS TRANSFER MODE.- es una tecnología de conmutación de paquetes donde dichos paquetes de información son trasportadas sin la necesidad de un orden específico.

[3] PPP.- POINT TO POINT PROTOCOL.- es un protocolo que admite métodos de autenticación con la ventaja del cifrado de la información. Normalmente sus procesos son automatizados.

[4] QoS.- QUALITY of SERVICE.- es la capacidad de las redes para brindar prioridad a aplicaciones, usuarios, datos, con el fin de garantizar la satisfacción de los usuarios de red en el uso de sus recursos.

[5] WIMAX. - Worldwide Interoperability for Microwave Access – Interoperabilidad Mundial para Acceso por Microondas. Creado por Intel y Alvarion, para permitir el acceso a internet inalámbrico a varios kilómetros de distancia.

Es importante mencionar que ésta plataforma tiene su respectivo Backup operativo.

- ✓ **BACKBONE MPLS FASE1.**
  (Inicio Operación ENE_2009).

La Corporación Nacional de Telecomunicaciones mediante un proyecto visionario, integró a su red un total de 38 equipos MPLS, con la finalidad de mejorar el servicio a los usuarios dando inicio al Backbone MPLS.

MPLS (MULTI-PROTOCOL LABEL SWITCHING, Conmutación Multi-Protocolo mediante Etiquetas), es un mecanismo de transporte de datos estándar creado por la IETF[6] y definido en el RFC[7] 3031. Opera entre las capas de red y la de enlace de datos del modelo OSI[8] (Estándar donde se definen los diferentes estratos existentes de los protocolos utilizados en redes).

Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes.

Es utilizado para la transmisión de tráfico de voz y de paquetes IP.

---

[6] IETF.- INTERNET ENGINEERING TASK FORCE, siendo el instituto que define los estándares de la red en áreas como transporte, seguridad, enrutamiento, entre otros, es el ente regulador de los estándares de internet.

[7] RFC.- REQUEST FOR COMMENTS, se basa principalmente en el intercambio de etiquetas, permitiendo garantizar el QoS sobre IP, además hace posible la implementación de la ingeniería de tráfico.

[8] OSI. - OPEN SYSTEM INTERCONNECTION, está compuesta por 7 niveles o capas, es la norma que rige para los protocolos de comunicación desde 1984. Asegura que los estándares de compatibilidad e interoperabilidad entre tecnologías sean acogidos por los fabricantes que las producen.

- ✓ **AAA-BRAS ERICCSON.**
  (Inicio Operación FEB_2009).

  La red Ericsson, posee una tecnología confiable y eficiente, pero la primordial limitante de conservar operativa esta plataforma tecnológica, es el factor costo-mantenimiento. Actualmente tiene unos pocos clientes conectados. Cabe señalar que está en proceso de ser suprimida y migrada a tecnología IP.

- ✓ **BACKBONE MPLS FASE2.**
  (Inicio Ejecución NOV_2009).

  Al empezar con esta red fue diseñada con 3 dispositivos los cuales estaban conectados a nivel internacional. Pero ya estaba diseñada su ampliación en lo que se llamó Backbone MPLS FASE 2.

  La Fase 2, es la ampliación de la red de BORDES DE INTERNET que consta de LER[9] (*Label Edge Router*), estos tienen la habilidad de encaminar paquetes en redes externas a MPLS. Las etiquetas asignadas por el LSR[10] (*Label Switching Router*), son distribuidas por el LDP[11] (*Label Distribution Protocol*), mediante el protocolo LDP los ruteadores de etiquetas (LSR) intercambian información para luego integrar un grupo de equipos internos y externos, lo que ha hecho de ésta red, una de las más grandes y eficientes actualmente dentro de la Infraestructura de la CNT.

---

[9] LER.- Es un ruteador de borde, que sirve de interface entre la red MPLS y otras redes clasificando el trafico que ingresa al dominio.

[10] LSR.- Es un router (normalmente configurado como núcleo) que efectúa conmutación basado únicamente en el intercambio de etiquetas.

[11] LDP.- es el protocolo empleado para la repartición de las etiquetas MPLS entre los dispositivos y componentes de la RED.

- ✓ **FASE 3 MPLS.**
  (Ejecución 2010).

Siendo esta una ampliación de los BRAS, cabe señalar que gran parte de la infraestructura de esta fase, estará dedicada para ampliación de la capacidad del servicio en la provincia del Guayas.

Todas estas plataformas que se han detallado se encuentran formando una red convergente dentro de la CNT, el DWDM, red de transporte de la información es una técnica de transmisión de señales a través de fibra óptica usando la banda C a 1550 nanómetros de longitud de onda, son las encargadas de proveer servicios a los clientes corporativos, masivos o de IP fijos.

Distribución

En síntesis: los usuarios ingresan a la plataforma mediante la red de cobre hacia el ATM, a través de los DSLAMs[12] (estos ya casi en desuso), DSLAMs IP o AMGs[13] (tienen voz y/o datos) y WIMAX, luego se transmiten mediante DWDM[14] con una capacidad de 10 Gbps. con posibilidad de ser enviados a largas distancias.

Toda la información es soportada por las plataformas MPLS y ATM, las cuales convergen al BRAS, éste último es quien asigna y agrega su respectivo ancho de banda a cada usuario,

---

[12] DSLAMs (*DIGITAL SUSCRIBER LINE ACCES MULTIPLEXER*), dispositivo colocado en las centrales telefónicas de la CNT, y que tiene como función realizar el enlace múltiple de las conexiones DSL de los usuarios en una portadora de alta velocidad como ATM.

[13] AMG (*ACCES MEDIA GATEWAY*), concentradores de líneas telefónicas con capacidad de incluir servicio de datos a los usuarios mediante fibra óptica.

[14] DWDM (*DENSE WAVELENGTH DIVISION MULTIPLEXING*), tecnología de transporte de información capaz de enviar varias señales en una sola fibra óptica. Permite la comunicación *FULL DUPLEX.*

los autentica para fines de facturación, y les asigna un perfil de navegación de acuerdo al plan contratado. (Los BRAS-AAA Ericsson y Huawei se conectan a las redes IP_MPLS y ATM respectivamente).

Figura 8.

Conexión usuarios corporativos y masivos.

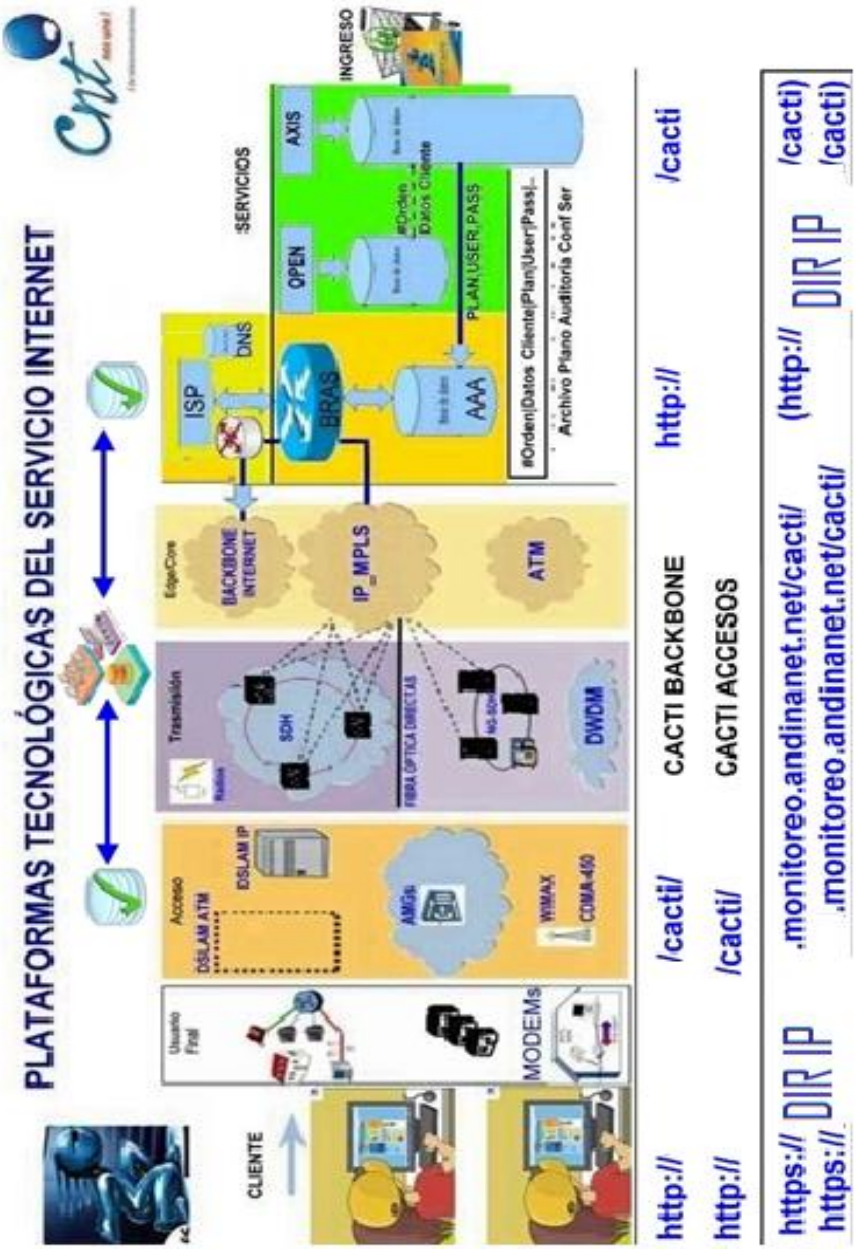


Figura tomada de los manuales informativos y esquemas de red de la CNT.

También tiene su integración a los servicios de como se factura mediante las bases de datos que contienen a los clientes por medio de las plataformas respectivas OPEN FLEXIS y AXIS[15].

2.1.2. PROCESOS.

La carga de cada actividad ha sido dimensionada de acuerdo a parámetros de requerimientos diarios o semanales, el tiempo que toma atenderlos, actividades que son ocasionales y en otros casos se ha usado la cantidad de horas que se estima se requieren, ya que para ellas no existen datos estadísticos ni indicadores mensuales.

Realizado el análisis de carga de trabajo para cada plataforma, de acuerdo a las actividades de aprovisionamiento, atención a problemas de clientes, atención a problemas de red, mantención de red y atención a las órdenes de trabajo solicitadas por el área de ingeniería y otras actividades de más alto nivel, cada una de éstas actividades se han agrupado en tres niveles de operación dentro del Departamento IP-MPLS en la CNT.

- ✓ **Nivel 1.**

  Se agruparon todas las actividades concernidas a la atención de clientes, para la solución de problemas a nivel de usuario.

- ✓ **Nivel 2.**

  Relacionado con todas las actividades que tienen concordancia con el soporte de la red como sus fallas y

[15] OPEN FLEXIS y AXIS (Plataformas que contienen la base de datos de los registros de red, permite almacenar los datos técnicos de red y referencias de los clientes incluidos sus registros para facturación)

atención de órdenes de trabajo generados por el área de ingeniería.

- ✓ **Nivel 3.**

  Contiene todas las actividades que están relacionadas a la red, como su crecimiento, resolución de fallas mayores, contacto con áreas de marketing y relación con proveedores.

La imagen d. muestra el nivel Jerárquico del departamento IP-MPLS

Figura 9.

Esquema de soporte jerárquico Gestión ATM.

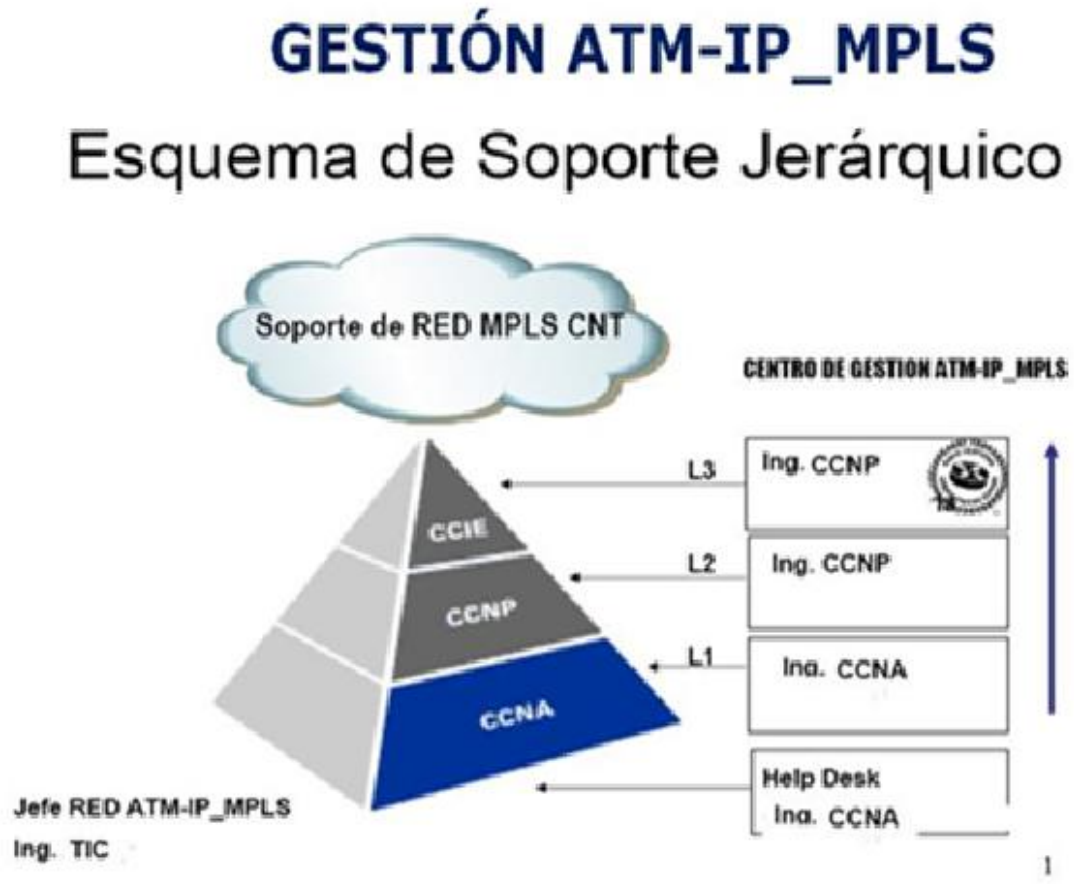


Figura tomada de los manuales informativos y esquemas de red de la CNT.

La conexión de DWDM en la que ingresa el trafico MPLS, se realiza mediante una interfaz entre router conectados sobre la infraestructura de red, se muestra en la imagen e.

Figura 10.

Conexión DWDM. Transporte del tráfico MPLS.

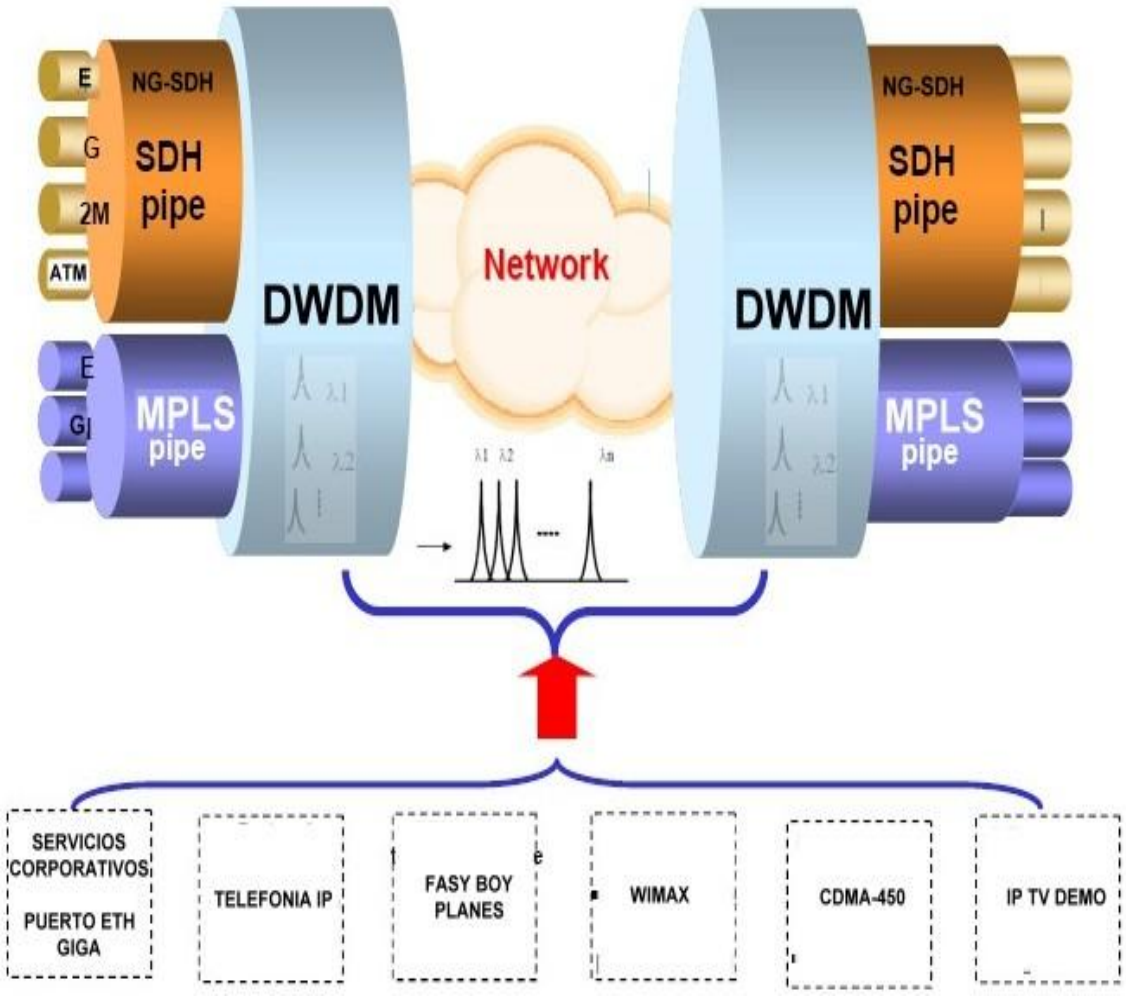


Figura tomada de los manuales informativos y esquemas de red de la CNT.

2.1.3. PERSONAL.

Como una porción de los servicios que presta la Corporación Nacional de Telecomunicaciones, se dispone de un centro de Administración de asistencia al cliente a nivel nacional denominado Call Center, en el cual se reciben los reportes de fallas de la red de datos (internet), y se constatan los datos del cliente, obteniéndose indicaciones de la falla por parte de los usuarios que presentan un problema con sus servicio, realizándose las pruebas de primer nivel correspondientes.

Luego se establece comunicación inmediata con el NOC *(Network Operation Center*), a fin de efectuar la revisión extremo a extremo sobre la Red y determinar la causa real del problema. El Call Center y el NOC funcionan las veinticuatro (24) horas, siete (7) días de la semana, los trescientos sesenta y cinco (365) días del año.

Dada la situación, de existir daños masivos en servicios de la CNT, el administrador a cargo de la plataforma deberá elaborar un informe acerca del daño en un tiempo estimado de entrega de hasta 72 horas, si cuenta con toda la información del hecho. Si requiere información de otro país o Carrier (empresa portadora de servicios), deberá incluir el tiempo que estos empleen para responder.

Es así como, el personal del departamento IP-MPLS y las tareas encomendadas están distribuidas y conformadas de acuerdo a las tablas 1 y 2.

Tabla 1.

Personal responsable del área de IP_MPLS.

<table>
<tr><th></th><th></th><th></th><th colspan="3">TÉCNICO</th></tr>
<tr><th>RESPONSABLE</th><th>BACKBONE</th><th>RESPONSABLE RED</th><th>NIVEL 3</th><th>NIVEL 2</th><th>NIVEL 1</th></tr>
<tr><td rowspan="8">RESP. IP MPLS</td><td rowspan="2">MPLS</td><td rowspan="2">TEC.1</td><td>T N 3.1</td><td rowspan="2">2 personas rotación mensual</td><td rowspan="8">2 TÉCNICOS</td></tr>
<tr><td>T N 3.2</td></tr>
<tr><td rowspan="2">ATM</td><td rowspan="2">TEC. 2</td><td>T N 3.3</td><td rowspan="2">3 personas rotación mensual</td></tr>
<tr><td>T N 3.4</td></tr>
<tr><td rowspan="2">METRO MPLS</td><td rowspan="2">TEC. 3</td><td>T N 3.5</td><td rowspan="2">3 personas rotación mensual</td></tr>
<tr><td>T N 3.6</td></tr>
<tr><td rowspan="2">BORDERS</td><td rowspan="2">TEC. 4</td><td>T N 3.7</td><td rowspan="2">2 personas rotación mensual</td></tr>
<tr><td>T N 3.8</td></tr>
</table>

2.1.4. ACTIVIDADES.

Las actividades están clasificadas de acuerdo al nivel de servicio que presta el personal del departamento IP-MPLS así:

Tabla 2.

Actividades del departamento de IP_MPLS.

NIVEL 1 _ CALL CENTER Son todas aquellas actividades que conciernen con la atención a clientes.
Tareas A:
Configuración, levantamiento y revisión de interfaces.
Atención de llamadas telefónicas hacia la PBX del Área.
Solicitud de correo y verificación de alarmas.
Atención a los OPE GESTION ATM Y OPE BACKBONE IP.
Configuración de servicios masivos y corporativos.
Verificación de pendientes.
Configuración de usuario y contraseña en AAA.
Levantamiento de VLANS
Verificación de Pendientes
Configuración de user y password en AAA
Contraordenes Retiros de infraestructuras (.10) Traslados, upgrades, downgrade, cambios (.16)
Atención solución y cierre de Trouble Tickets según prioridad.
Identificación de incidentes en la red y aplicación de procedimientos.
Administración de incidentes utilizando herramientas básicas y documentación de los mismos.

Uso de herramientas de administración para monitoreo de status de red.
Interpretación de alarmas y determinación de su severidad para inicio de troubleshooting en un primer nivel.
Monitoreo y gestión de la red mediante herramientas tales como ANA, CACTI, NAGIOS.
Reconexión de usuarios masivos con el AAA.
Registro de incidentes.
Troubleshooting nets IP/MPLS, BRAS, ITELLIN, METROS_OPE, ATM
Soporte a XDSL, Call Center y NOC cuando existen desbordes de XDSL, incluso se atiende a técnicos.
Requerimientos de cableado
NIVEL 2 _ DEPARTAMENTO MULTISERVICIOS Relacionado con todas las actividades que tienen concordancia con el soporte de la red, sus fallas, coordinación y atención.
Coordinación y atención de OTs dentro del área asignada.
Atención de órdenes de trabajo de sus zonas.
Planificar y participar en migraciones.
Configuración, levantamiento y revisión de interfaces.
Planificar y participar en mantenimientos programados.
Generar MOPs y comunicados de mantenimiento.
Actualizar los diagramas de red.

Inventarios, etiquetamiento de equipos.
Operar y mantener las plataformas asignadas.
Apertura de tickets a proveedores.
Interconexión de redes.
Instalaciones y requerimientos de cableado estructurado.
Instalación de nodos.
Reparación de equipos.
Back up de configuración de las diversas plataformas.
Generación de nuevos scripts.
Procesos de administración de inventario de la red.
Operación de mantenimientos físicos y lógicos.
Administración de Syslog, ACS.
Atención de problemas dentro y fuera de la ciudad que ocasionan interrupción en el servicio de red y accesos a los sistemas de información.
Uso de scripts. UNIX cron job command para crear retinas automáticas de mantenimientos de la red.
Administración de las políticas de seguridad. (FW, administración de usuarios, antivirus, cumplimiento de privacidad, acceso remoto, registro de vrf y túneles.)
Atención al teléfono celular del NOC y Stand by.
Migraciones masivas de troncales.

Configuración y levantamiento de nuevos servicios.
Operar y mantener los sistemas de monitoreo gestores.
Administración de servidores gestores.
Soporte en trabajos nivel 1.
NIVEL 3 _ DEPARTAMENTO DE BACKBONE ATM/MPLS Contiene actividades que están relacionadas con su crecimiento, optimización, resolución de fallas mayores y contacto con otras aéreas.
Optimización de la red.
Planificación anticipada.
Proyectos de reemplazo de equipamiento IP.
Coordinación y atención OTs dentro del área asignada.
Planificación y participación de migraciones de mayor impacto.
Definir políticas de seguridad en cada plataforma.
Implementar nuevos proyectos.
Aplicación de procesos de administración de problemas según ITIL.
Planificar y participar en mantenimientos programados.
Ser líder y responsable de una plataforma.
Identificación de posibles riesgos y amenazas.
Stand by.
Integración de las plataformas.

Configuración y levantamiento de nuevos servicios.
Operar y mantener las plataformas INTERNET, MPLS, BRAS Y GESTORES.
Cambios de sistemas operativos (IOS, PTR, VRP)
Definición de servicios.
Migración masiva de troncales.
Soporte en trabajos de nivel 2.
Troubleshooting de las plataformas.
Análisis de la arquitectura de las plataformas.

2.2. RECURSOS DEL DEPARTAMENTO DE IP_MPLS EN LA CNT.

2.2.1. INFRAESTRUCTURA DE RED DE TRANSPORTE.

La configuración física de la red MPLS y conexiones de sus componentes se muestran a continuación:

- ✓ Sus diferentes niveles de conectividad:

  Acceso, Distribución y Core.

- ✓ Los equipos instalados:

  Servidores, routers, switches, DSLAMS, AMG, Centrales Telefónicas, los enlaces con sus

respectivas capacidades y el medio de transmisión que se ha utilizado en la implementación.

- ✓ La ubicación según cada uno de los centros poblados o ciudades.

La infraestructura de red que la CNT posee y que el Área de IP-MPLS administra esta detallada de acuerdo al diseño al que fue elaborado.

Se muestra la estructura y su configuración de red en cada uno de ellos, todos estos monitoreados y gestionados desde la ciudad de Quito.

Figura 11.

Esquema de red de la Plataforma de Accesos WIMAX.

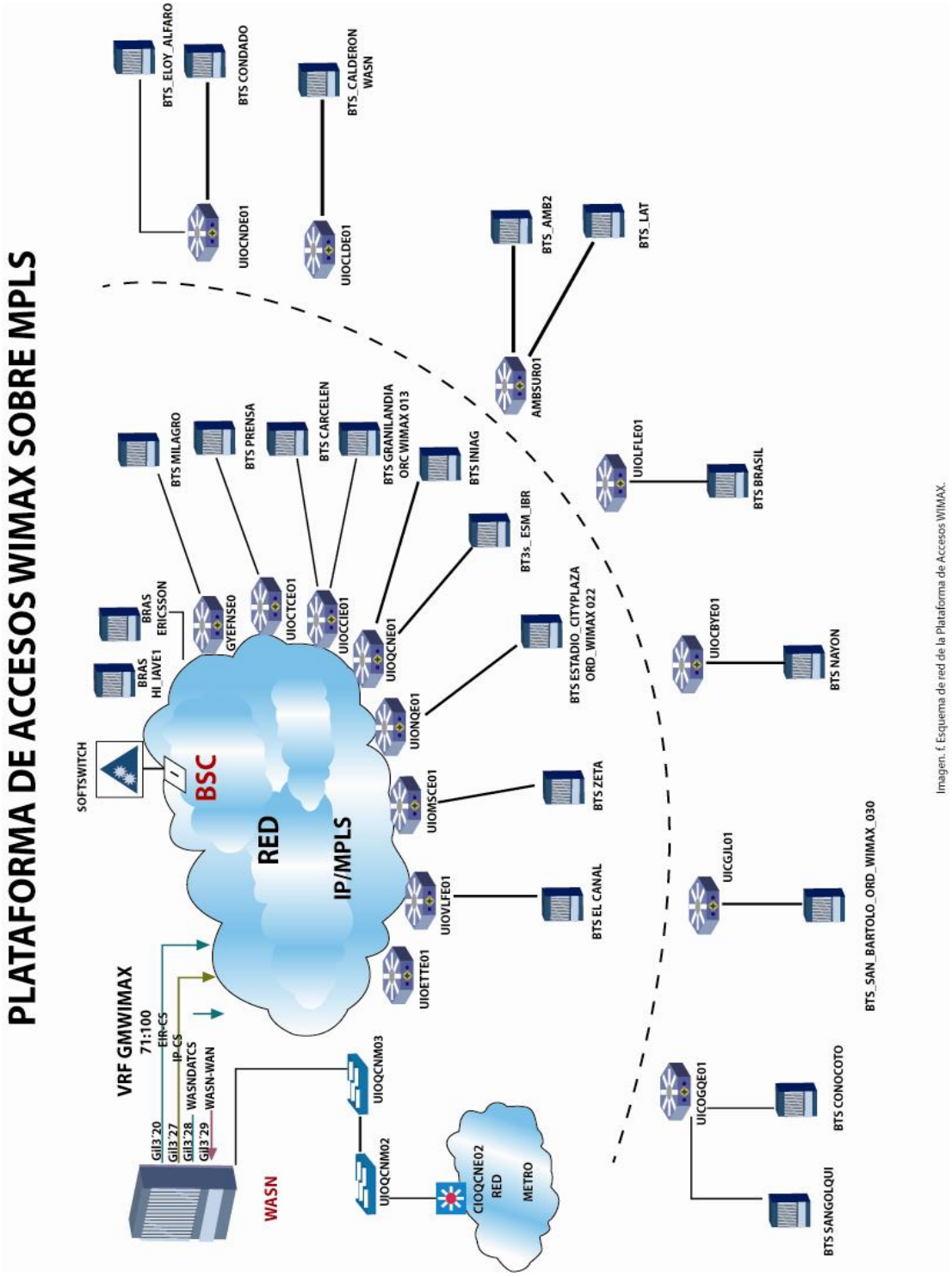


Imagen. f. Esquema de red de la Plataforma de Accesos WIMAX.

Figura tomada de los manuales informativos y esquemas de red de la CNT.

Figura 12.

Esquema de red de la Plataforma de Accesos hacia AMGs.

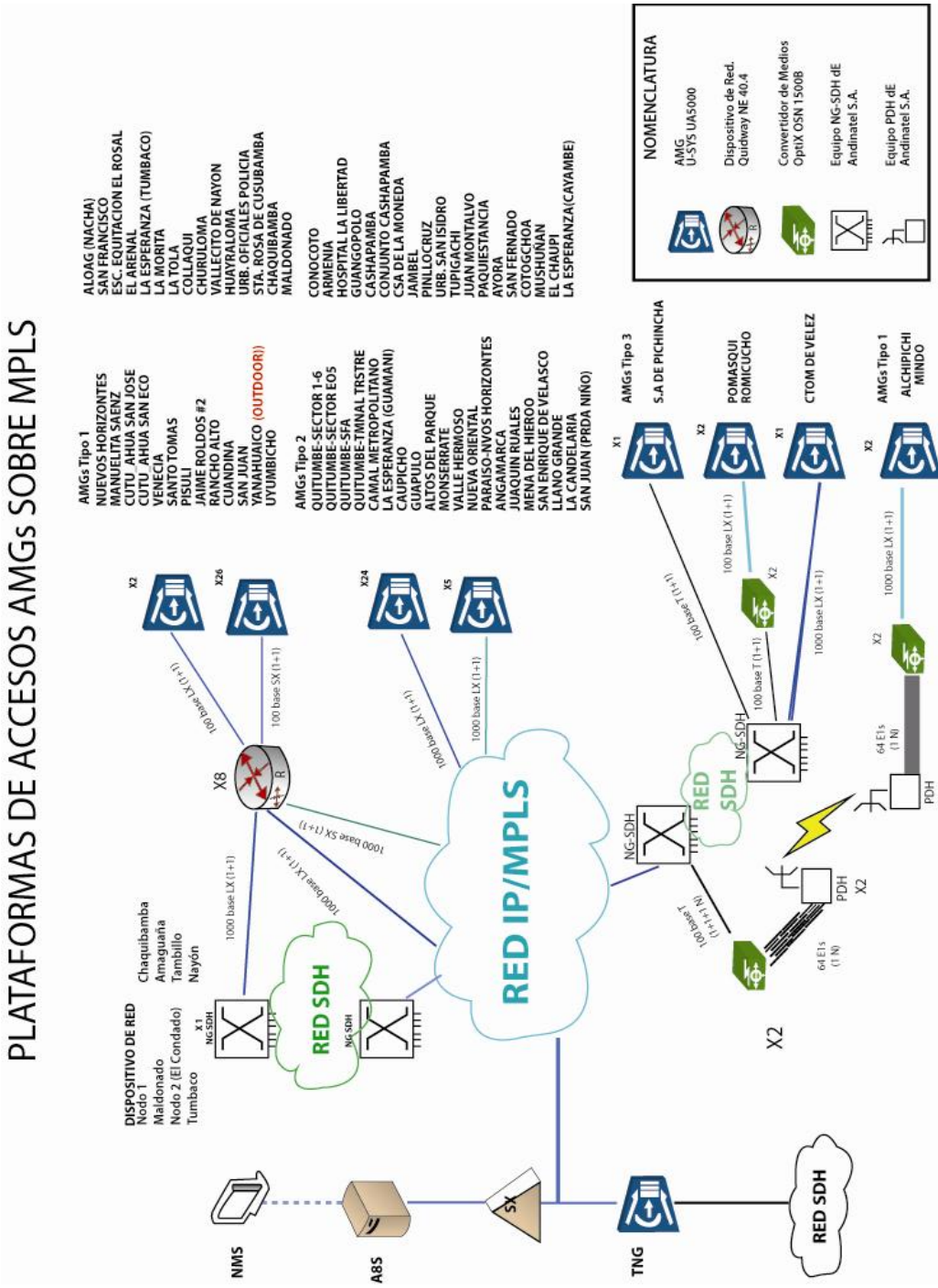


Imagen. g. Esquema de red Plataforma de Accesos hacia AMGs.

Figura tomada de los manuales informativos y esquemas de red de la CNT.

Figura 13.

Esquema de Red IP.

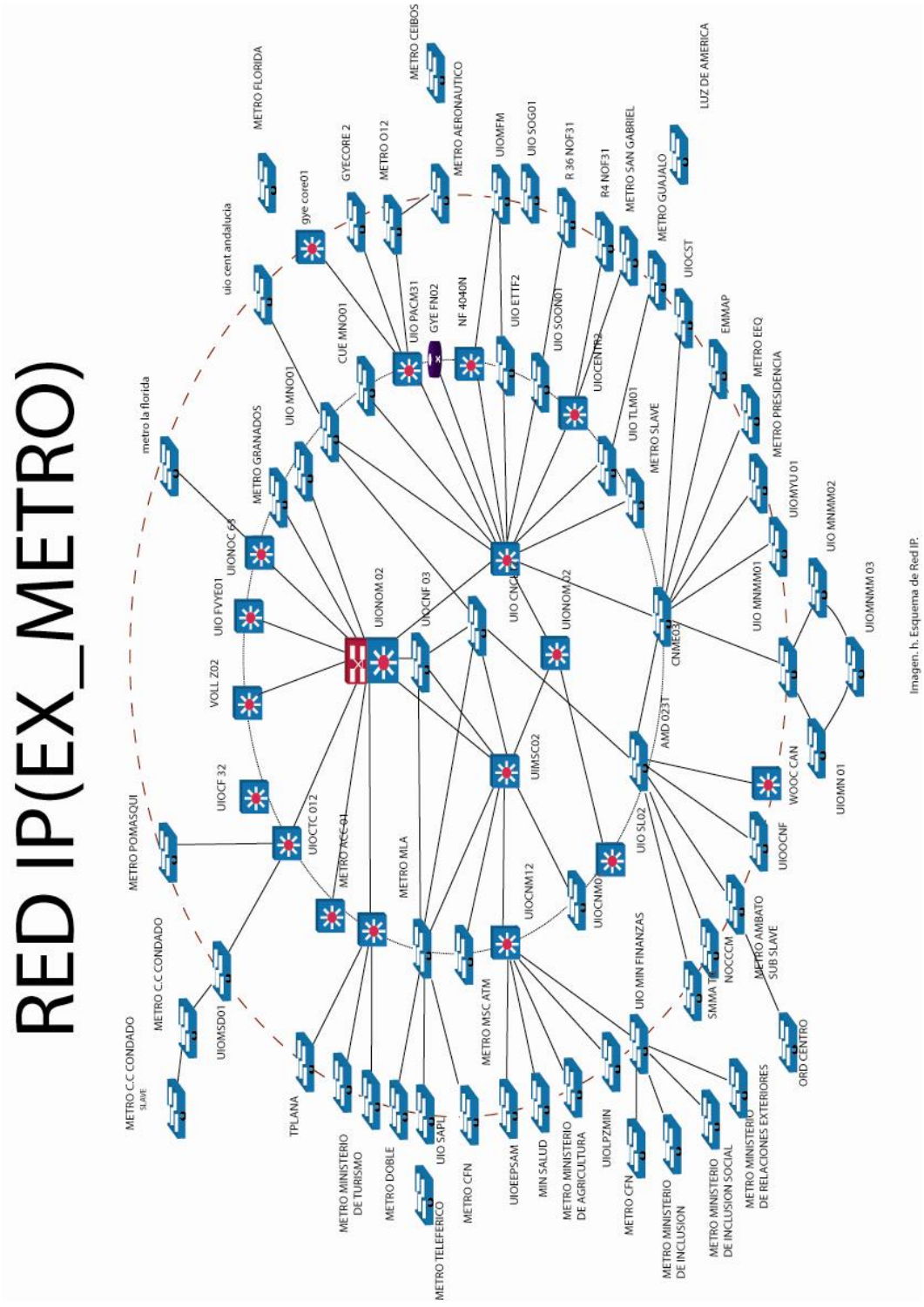


Figura tomada de los manuales informativos y esquemas de red de la CNT.

Figura 14.

Esquema de capas Backbone IP_MPLS.

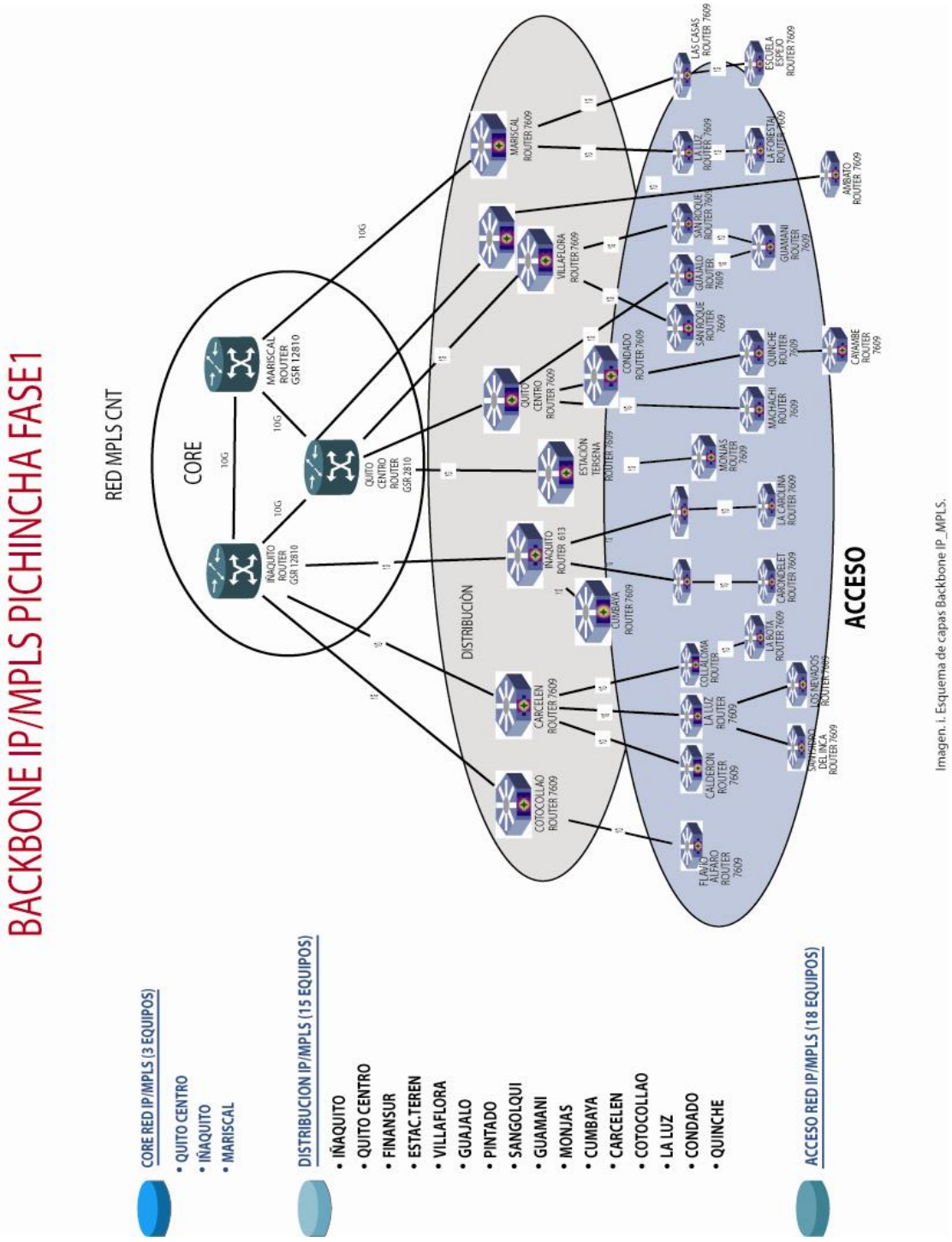


Imagen. I. Esquema de capas Backbone IP_MPLS.

Figura tomada de los manuales informativos y esquemas de red de la CNT.

Figura 15.

Red de transporte nacional de FO CNT.

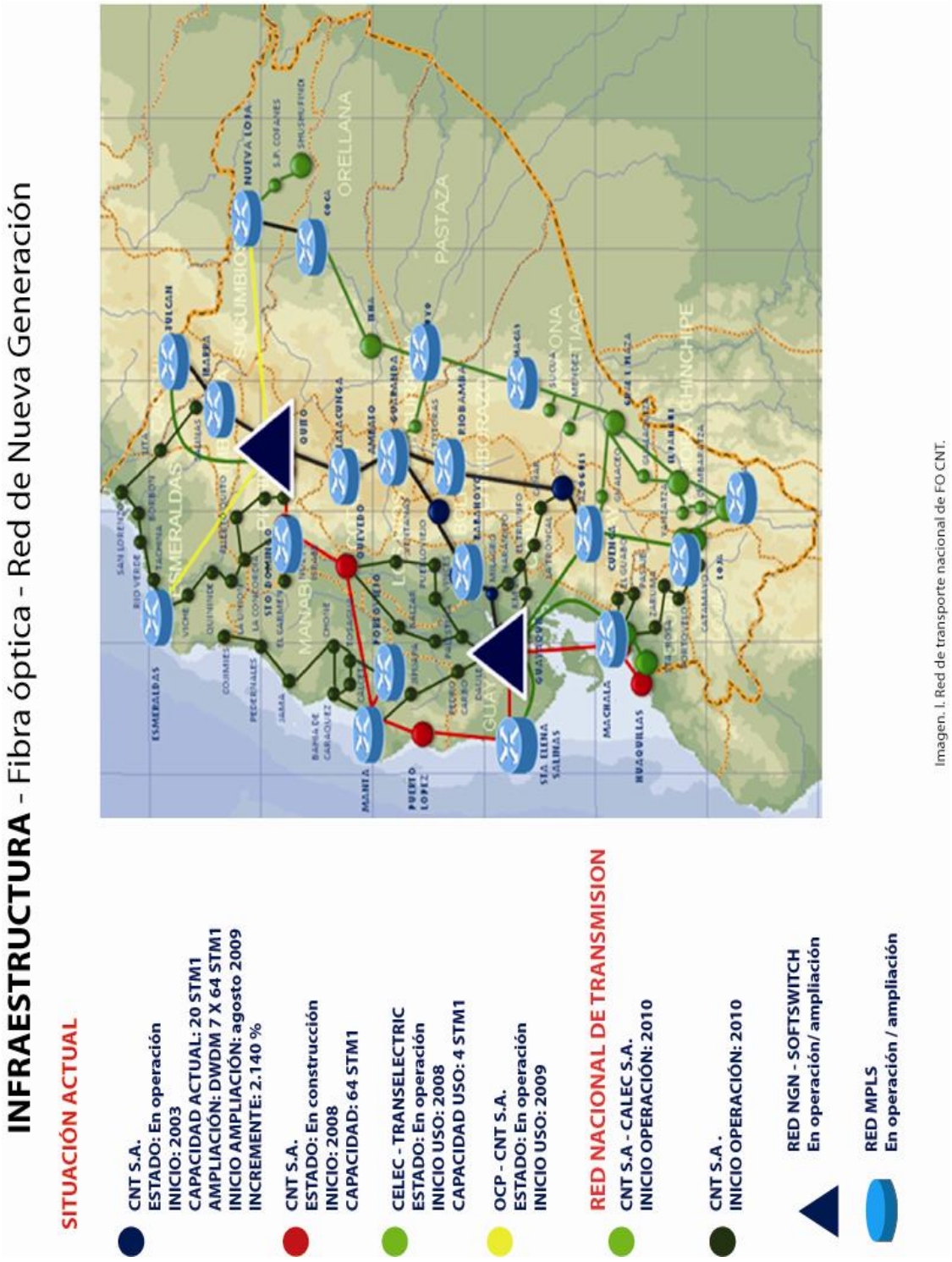


Imagen. I. Red de transporte nacional de FO CNT.

Figura tomada de los manuales informativos y esquemas de red de la CNT.

Figura 16.

Esquema de salida de datos internacional CNT.

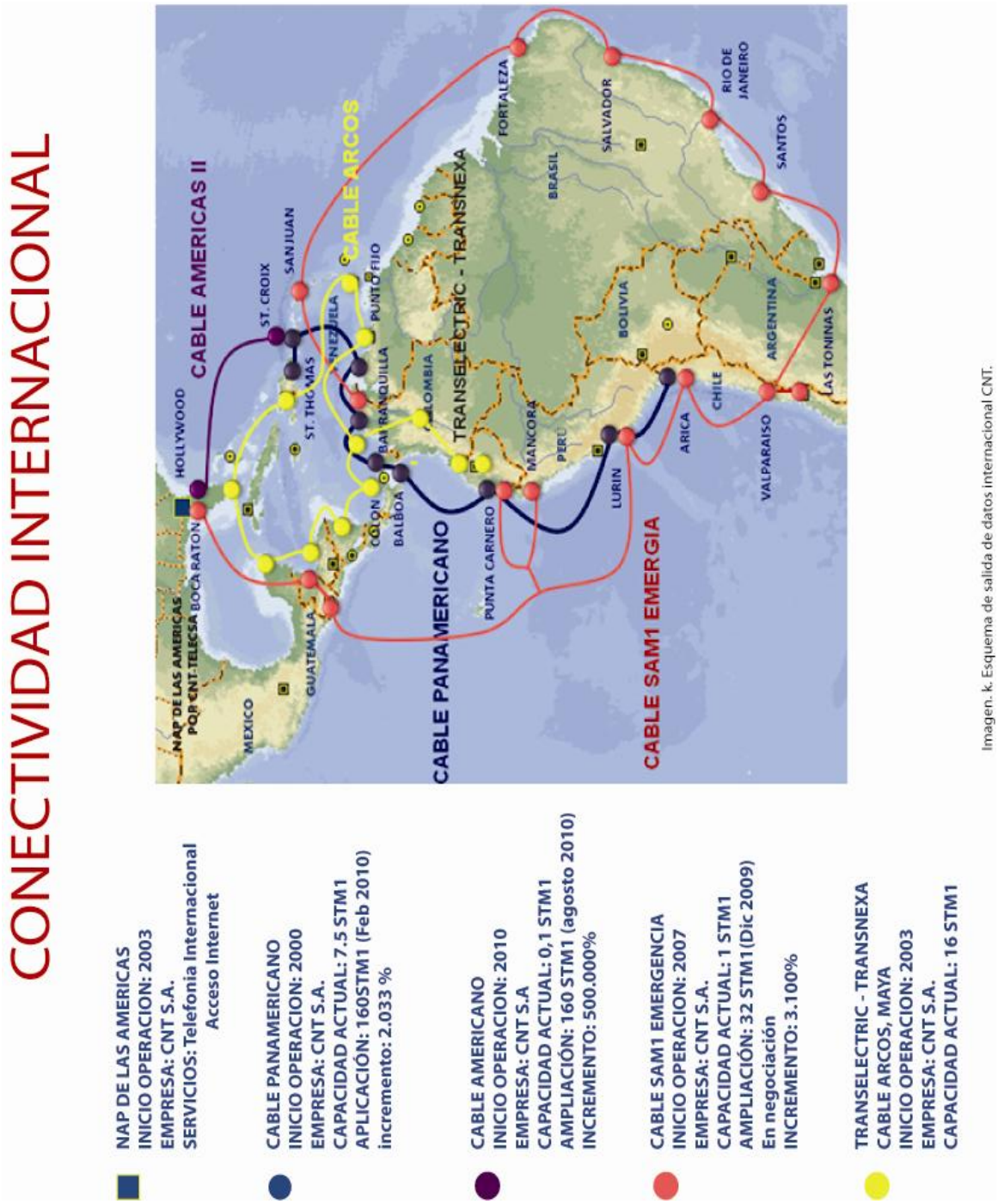


Imagen. k. Esquema de salida de datos internacional CNT.

Figura tomada de los manuales informativos y esquemas de red de la CNT.

Para una red multiservicios como la que posee la Corporación Nacional de Telecomunicaciones, es imprescindible tener enlaces de gran capacidad para soportar los servicios de voz, datos y video debido al crecimiento de las redes de acceso y sus usuarios.

Esta red ha sido diseñada y basada totalmente en anillos para brindar protección en la red, confiabilidad de los sistemas de telecomunicaciones y disponibilidad de los servicios.

Detalles técnicos de la longitud instalada de la red de Fibra Óptica DWDM de la CNT E.P.

FIBRA ÓPTICA CNT
RED EXISTENTE (2006): 1.413 Km
NUEVA RED ADICIONAL (2010): 5.357 Km
TOTAL NACIONAL al 2010: 6780 Km
INCREMENTO: 380 %

2.2.2. HERRAMIENTAS UTILIZADAS.

Para todos los departamentos de la CNT, existen instrumentos de gestión que facilitan los procesos y agilizan las operaciones propias de cada uno de ellos, es así como, entre las herramientas de soporte para la verificación del estado de interfaces, activación de dispositivos, solución de problemas de red, monitoreo, informe de soporte, inventario de equipos y configuraciones utilizadas por el departamento de IP-MPLS en la corporación Nacional de Telecomunicaciones E.P., se enlistan a continuación los siguientes:

- ✓ **DEPARTAMENTO MULTISERVICIOS, DEPARTAMENTO DE BACKBONE ATM/MPLS.**

  Son los equipos de trabajo organizados dentro de la CNT que resuelven los problemas de RED IP/MPLS, cada uno de ellos en los 3 niveles de servicio ya establecidos.

- ✓ **CACTI-CISCO-ANA.**

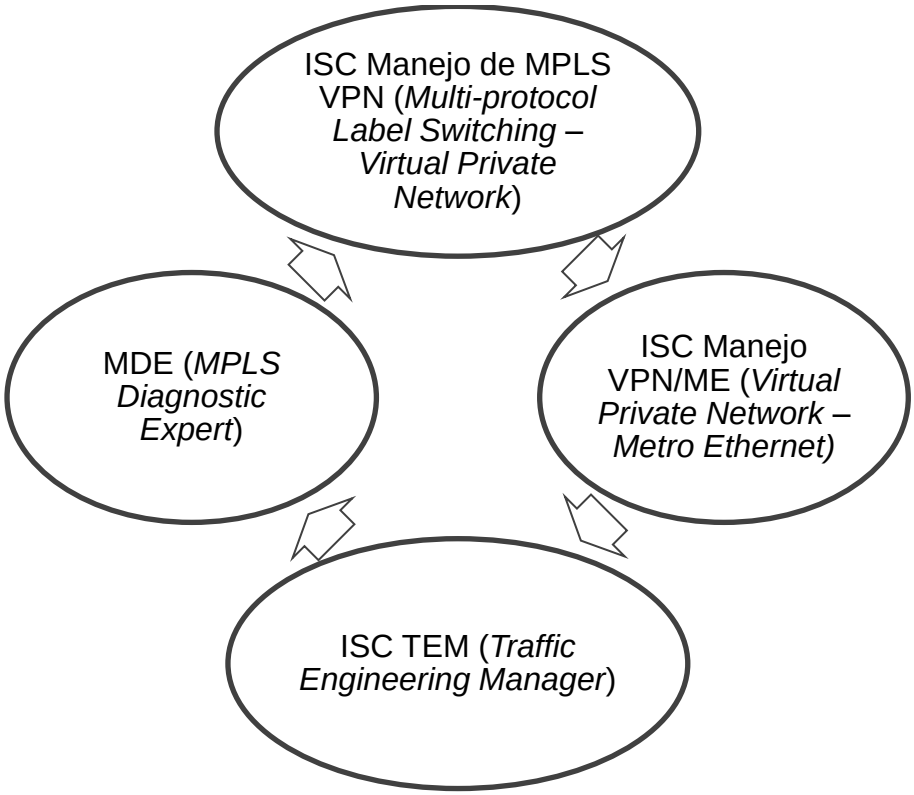
  Herramienta propietaria de CISCO Systems Inc. que realiza operaciones para el monitoreo del servicio masivo, ANA Manage, proporciona las funciones principales de administración, se enlistan las siguientes:

  - ✓ Verifica saturación de interfaces.
  - ✓ Visualización de los segmentos de la base de datos.
  - ✓ La administración de eventos en la red.
  - ✓ La configuración de los grupos protectores de la red.
  - ✓ Gestión de configuración de informe.
  - ✓ La gestión de la seguridad parámetros.
  - ✓ Ámbitos de gestión y las cuentas de usuario.
  - ✓ Gestión de enlaces estáticos.
  - ✓ Administra la capacidad de ancho de banda en la red.

- ✓ **ISC (*IP SOLUTION CENTER*).**

  El ISC, es un instrumento de gestión del cual es propietario CISCO Systems Inc., y es una familia de aplicaciones inteligentes para gestionar la red que ayuda a reducir la administración en general, los costos de tareas proporcionando la gestión de recursos automatizado, basado en el perfil de las capacidades de suministro.

Está dividido en 4 aplicaciones:



- ✓ **OPEN FLEXXIS.**

  Es una plataforma encargada del sistema de facturación en la CNT E.P. en esta base de datos se encuentran todos los números telefónicos y números de servicio de datos con sus respectivos datos de red física y lógica.

- ✓ **MANAGED ENGINE PLUS SERVICE DESK.**

  Es una herramienta de administración para Service Desk, que reemplazará a las hojas de cálculo de Excel.

- ✓ **EMAIL.**

  Usado para la notificación de operaciones, administración de órdenes, problemas y de negocios.

- ✓ **Plataforma AXIS.**

  Es el sistema de facturación de ancho de banda de cada cliente, también asigna el usuario y contraseña.

2.2.3. PROCESAMIENTO DE LA INFORMACIÓN.

La información que maneja el departamento de IP_MPLS en la Corporación Nacional de Telecomunicaciones, tiene que ver específicamente con la configuración del servicio de datos de los clientes, es decir, aspectos como ancho de banda de operación de cada cliente, modo de operación, VLAN a la que pertenece el cliente, nombre del usuario, contraseña, número de servicio al que está ligado, numero de splitter (número telefónico) entre otros, en caso de un ISP (*INTERNET SERVICE PROVIDER*) también está asociado a una VLAN, además de la Categoría de servicio que tiene el ISP con la CNT, la categoría de productos de Internet se encuentra dividida en tres líneas de servicio, las cuales son:

- ✓ Servicios de Internet para Usuarios Finales (SVAF), Servicios de Internet para Usuarios Finales dividido en 8 tipos de productos.
- ✓ Servicios de Internet para Distribuidores (SVAD) y Servicios de Valor Agregado; estas líneas a su vez tienen productos asociados que se han estandarizado de acuerdo a lo siguiente: SVAF: SVAD: Servicios de Internet para Distribuidores dividido en 7 tipos de productos.

- ✓ Servicios de Valor Agregado dividido en 5 tipos de productos.

A continuación la tabla 3, se exponen algunos parámetros que pueden ser tratados desde el centro de gestión y sus respectivos valores (los valores cambian constantemente en el tiempo, no son fijos y dependerá de factores como: estado de la red, distancia del usuario a la central telefónica, bucle del par telefónico, ancho de banda solicitado, relación señal a ruido, atenuación propia del medio físico de conexión del usuario, inducción sobre la red, humedad, etc.).

Tabla 3.

Parámetros a considerar en el servicio de datos ADSL.

ADSL	Descripción
ADSL State[16]	Show Time
Data Path	Interleaved
Operation Mode	G. dmt. bis plus
Max. Bandwidth Down/Up(kbps)	20660 / 1167
Bandwidth Down/Up(kbps)	744 / 306
SNR[17] Margin Down/Up(dB)	37.4 / 31.8
Attenuation Down/Up(dB)	24.3 / 13.0
Power Down/Up(dBm)	1.6 / 11.3
CRC[18] Down/Up	0/ 2

[16] ADSL State Asymmetric Digital Subscriber Line. Estado de la digitalización del par de cobre telefónico, capacidad de transporte de datos a través del par telefónico.

[17] SNR.- SIGNAL NOISE REFERENCE. Margen existente entre la potencia de la señal generada como información y la potencia del ruido que la corrompe.

FEC[19] Down/Up	95/ 1
HEC[20] Down/Up	0/ 0
System Up Time	10:47:55
DSL[21] Up Time	6:11:49
PPP[22] Up Time	6:11:48

(Student Guide; Cisco Systems Learning; 2010)

2.2.4. PÓLITICAS DE SEGURIDAD DEL DEPARTAMENTO IP-MPLS.

La RFC 1244 (***R**equest **F**or **C**omments*) expresa que en una Política de Seguridad de gran nivel, envuelve la seguridad de los medios informáticos, y que comparte las bases para definir y delimitar compromisos para las diversas acciones técnicas organizativas que se requerirán con el fin de mejorar la seguridad.

La Gestión de las políticas de seguridad se las ha definido como el conjunto de acciones y procesos destinados a ofrecer al departamento de IP_MPLS, la seguridad que requiere, relacionando directamente a los servicios que provee y a los usuarios, formando la comunidad tecnológica existente dentro de la CNT E.P.

---

[18] CRC.- CYCLIC REDUNDANDY CHECK. Técnica de cifrado por medio de bloques de manera recursiva, el tamaño de los bloques pudiendo estar formados de 2 o 4 bytes.

[19] FEC.- FORWARDING EQUIVALENCE CLASS. Es el tipo de clase en el que todo el tráfico con similar requerimiento es agrupado.

[20] HEC.-HEADER ERROR CHECK. Es el último campo del la celda de de la trama ATM que consiste en un CRC de 8 bits.

[21] DSL.-DIGITAL SUSCRIBER LINE. Es una tecnología que brinda la posibilidad de un ancho de banda superior al Dial UP, a través del par telefónico convencional.

[22] PPP.- POINT TO POINT PROTOCOL, protocolo que admite métodos de autenticación con la ventaja del cifrado de la información.

Todas estas precauciones con el afán de minimizar la ocurrencia de incidentes de seguridad que afecten real o potencialmente sus servicios.

Algunas de las herramientas de seguridad implementadas en el Departamento de IP_MPLS están relacionadas con:

- ✓ Firewall
- ✓ Administración de cuentas de usuarios
- ✓ Antivirus
- ✓ Acceso remoto
- ✓ Redes Virtuales Privadas "VPNs"
- ✓ Tecnologías de monitoreo

Es destacable mencionar que las políticas no son y no deben tratarse como una simple descripción técnica de mecanismos o procedimientos para controlar y brindar seguridad, sino más bien adoptarlas como una descripción de lo que deseamos proteger y el porqué de nuestro objetivo al implementarlas.

Cada una de las herramientas detalladas en el listado anterior, en general cumplen con características como las siguientes:

- ✓ La Integridad.
- ✓ Disponibilidad.
- ✓ Privacidad.
- ✓ Control.
- ✓ Autenticidad.

Además, las políticas implementadas tienen como alcance:

Cubrir todos los aspectos relacionados con la misma política.

Adecuarse a las necesidades y recursos.

Son atemporales, es decir, el tiempo en el que se aplican no influye en su actividad y vigencia.

Limitar maniobras donde se conocen las opciones ante eventos repetidos.

Definir criterios usuales para ser acogidos en distintas funciones y actividades.

2.2.5. IDENTIFICACIÓN DE LOS PROBLEMAS.

Los incidentes de seguridad informática tales como: configuraciones erróneas, equipos defectuosos, conexiones inapropiadas, etc., dentro del departamento de IP-MPLS, se pueden definir como la violación o amenaza inminente a su infraestructura o el quebrantamiento de una política de seguridad de la información implícita o explícita dentro del mismo.

También es un incidente de seguridad un evento que compromete la seguridad de un sistema como por ejemplo la confidencialidad, la integridad y la disponibilidad.

Entre los posibles ejemplos o amenazas determinados como ejemplos de incidentes de seguridad en el departamento de IP-MPLS podemos enumerar:

- ✓ Accesos no autorizados
- ✓ Robo de contraseñas
- ✓ Robo de información
- ✓ Denegación de servicios
- ✓ Ataques informáticos externos

2.2.6. FACTORES QUE DESENCADENAN UNA CRISIS O AMENAZA.

Si en una empresa no existe un Plan de Continuidad de Negocio, no se podrá conocer si se encuentra expuesta a una crisis, y peor aún saber la magnitud de la misma.

Una crisis o amenaza inminente, estará caracterizada por la falta de tiempo para su resolución ante las variables desconocidas de la amenaza y la falta de conformación de un equipo entrenado que será el encargado de tomar las decisiones necesarias.

Entre los factores desencadenantes de una crisis se mencionan los siguientes:

- ✓ Situaciones que inician como pequeños incidentes.
- ✓ Una mala evaluación de los incidentes.
- ✓ Falta de preparación ante una amenaza.
- ✓ Desconocimientos de las causas.
- ✓ Falta de registros.
- ✓ Falta de cultura organizacional.

2.2.7. RIESGOS Y VULNERABILIDADES.

Entre los tipos de riesgos y vulnerabilidades encontrados en el departamento de IP-MPLS están los que se detallan a continuación:

2.2.7.1. FÍSICOS.

Relacionados directamente con la inspección de los elementos eléctricos, mecánicos y estructurales de las instalaciones existentes en el departamento de IP_MPLS.

2.2.7.2. LÓGICOS.

Concerniente a la inspección de las reglas de negocio y de Tecnologías de la Información ajustadas y empleadas para administrar el departamento de IP_MPLS.

2.2.7.3. SEGURIDAD.

Inspección de la seguridad lógica de sus datos e información, así como de la seguridad física de las instalaciones, además un análisis en la inspección de riesgos relacionados con la seguridad nacional en caso de que fuera quebrantada.

2.2.7.4. SEGURIDAD LABORAL.

La inspección periódica de aspectos relacionados con la protección del personal, ante la manipulación de equipamientos eléctricos, suministros de emergencia, formación y tratamiento de lesiones.

2.2.7.5. IDENTIFICACIÓN DE SUCESOS O AMENAZAS.

Hace referencia a los incidentes que pudieran afectar a la continuidad de las operaciones de negocio o a la imagen y reputación de la marca CNT, así como la probabilidad de que sucedan.

2.2.7.6. PLANIFICACIÓN ANTICIPADA.

Carece del establecimiento y análisis detallado de planes de actuación que permitan la mitigación de los riesgos ya identificados.

Se incluyen el estudio y la determinación del impacto sobre la empresa de nuevas iniciativas de negocio o nuevas tecnologías, éstas implementadas para el mejoramiento de servicios y sus procesos.

2.2.7.7. EFECTOS.

La necesidad de detallar consecuencias de la recuperación de las actividades y sus procesos frente a las medidas adoptadas ante una paralización de actividades, o, a un cambio en el departamento de IP-MPLS.

CAPÍTULO III

3. ESTRUCTURA DEL PLAN DE CONTINUIDAD DE NEGOCIO PARA LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES E.P. DEPARTAMENTO IP_MPLS.

Dentro del capítulo uno de este trabajo, ya se han definido los principales conceptos que intervienen en el Plan de Continuidad de Negocio, y se ha llegado a la conclusión de que no se trata solamente en recuperar y devolver los servicios provistos por la empresa hacia sus usuarios, tampoco es solamente de rescatar la infraestructura y a las tecnologías de información, sino por el contrario, el objetivo está en lograr que las consecuencias que puedan ocurrir ante un incidente de cualquier índole, sean minimizados y su probabilidad de que ocurran también.

A continuación se muestra un resumen de la infraestructura tecnológica de la Corporación Nacional de Telecomunicaciones

"BackBone

- ✓ *CNT es propietario de la red de fibra óptica más grande a nivel nacional, con más de 10.000 Km de fibra óptica instalada en todo el territorio ecuatoriano.*
- ✓ *La fibra óptica de mayor calidad del Ecuador.*
- ✓ *Su fibra monomodo y anillada, permite mayor calidad en la transmisión de datos y garantiza una alta disponibilidad en la red*
- ✓ *Su fibra óptica incluye triple protección en el cable, chaquetas de seguridad, material anti-roedores y con alma de acero.*
- ✓ *Tiene una implementación a través de canalización subterránea, brindando mayor seguridad para garantizar el servicio.*
- ✓ *Posee una implementación y operación conforme a estándares internacionales, tales como el 568B.3.1.*

RED DE TRANSPORTE

Dispone de tecnología de última generación con IP/MPLS TE y DWDM. La red nacional IP/MPLS TE de CNT es una red de última tecnología, una de las mejores a nivel de toda Sudamérica, implementada en su totalidad con tecnología CISCO, que se encuentra a la vanguardia de innovación, utilizada en los países más desarrollados, lo cual da garantía de calidad de servicio.

Capacidad en la red de Transporte de hasta 192 Lambdas
Interfaces de conexión con capacidades de hasta 10 Gbps.

RED DE ACCESO

Mediante la aplicación de las tecnologías, se encuentra en capacidad de brindar todas las soluciones de telecomunicaciones que los clientes requieren, posibilitando alcanzar alta capacidad, e incrementando la eficiencia de su empresa ya que permite configurar las opciones de acuerdo a las necesidades específicas que tenga cada empresa.

Dispone de las tecnologías de acceso fija más avanzadas del Ecuador, para llegar con la mejor velocidad de Internet a las empresas clientes del servicio como:

ADSL2+, GPON, G.SHDSL y WIMAX.

CONECTIVIDAD INTERNACIONAL

CNT posee una red de nivel 2, por lo tanto la mejor conectividad internacional del país con una capacidad de transporte de datos internacional de 192 STM-1.

CNT posee actualmente 5 salidas para conexión internacional:

- ✓ *Tres cables submarinos (Cable Panamericano, Emergía y Américas 2).*
- ✓ *Dos cables terrestres (Telecom y Transnexa)* ***".***
  (http://www.cnt.com.ec)

Sabiendo de antemano que, es imposible el no tener riegos o incidentes de cualquier tipo ante la inmensa infraestructura tecnológica que posee la CNT E.P., frente a esta premisa, se puede acoger entonces, que el departamento de IP_MPLS estará seguro, si los incidentes y sus riesgos son limitados mediante la implementación del Plan de Continuidad de Negocio.

Se analizará, ahora que se conoce la infraestructura de la CNT, los posibles incidentes a los que está expuesto el departamento de IP_MPLS dentro de la CNT E.P., y el impacto de estos al negocio (AIN Análisis del Impacto sobre el Negocio).

Por tal razón, se ampliarán 5 temas determinantes para la estructuración del plan de continuidad:

LA EVALUACIÓN DE RIESGOS.

Debido a las cambiantes condiciones y nuevas plataformas tecnológicas que se hallan implementadas y disponibles en la CNT E.P., la posibilidad de la ocurrencia de un incidente, o la aparición de nuevas amenazas para los sistemas de información, han hecho más probable los riesgos dentro de la infraestructura.

Es por estos riesgos, que cada incidente ocurrido deberá ser valorado o tener una clasificación y posterior seguimiento de acuerdo a varios parámetros como los señalados a continuación:

- ✓ De acuerdo a la frecuencia de ocurrencia de cada incidente.
- ✓ Alcance del riesgo que presenta.
- ✓ Nivel de riesgo del incidente.
- ✓ Elementos del incidente.
- ✓ Consecuencia provocada por el incidente.
  (www.ezone.net)

Con dicha valoración, se podrá obtener un mayor provecho del plan de continuidad de negocio aquí guiado y desarrollado, debe considerarse como un instrumento organizacional acerca del valor de la información, procedimientos y servicios que la CNT provee a sus usuarios dentro y fuera de sus instalaciones.

Todo con el único objetivo de mantener competitiva y en continuo servicio a la CNT, pero requiere de un alto compromiso con la organización para el determinar fallas y debilidades en su estudio, se requiere la firmeza para la renovación, todo en función de mejorar el ambiente en los procesos hasta ahora implementados.

3.1. ANÁLISIS DE RIESGOS

3.1.1. LA IDENTIFICACIÓN DE LOS ACTIVOS.

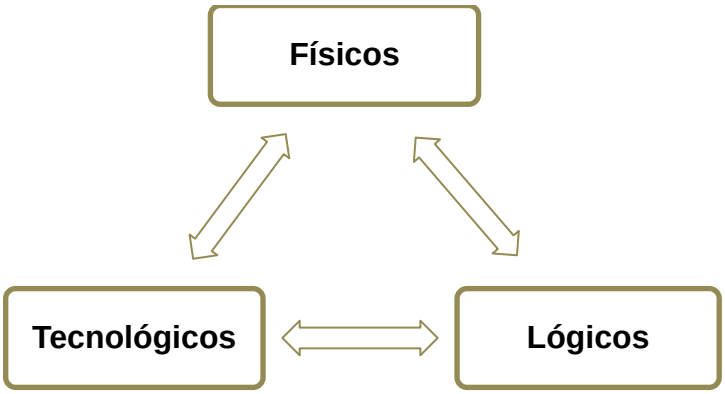
Para la identificación de los riesgos en el departamento de IP_MPLS, se ha realizado un estudio detenido de los incidentes a los que esta propenso y que requieren de una apropiada gestión para su resolución brindando así, la seguridad en la información y seguridad tecnológica requerida.

Esto solo es una muestra que indica lo comunes que son los problemas de seguridad en las empresas, frente a esto, el riesgo de que un incidente tome forma y se produzca, se deberá a factores como la debilidad o la falta de requisitos en el medio de operación en el que las amenazas se hallan latentes, sin que exista la predisposición de corregirlos.

Estos activos y sus incidentes están ligados entre sí.

Figura 17.

Tipos de Activos que son afectados por los riesgos.



3.1.2. AMENAZA LATENTE EN ACTIVOS.

Los sistemas de información, servicios o infraestructura, locaciones físicas y los procesos que la soportan, son el principal activo dentro de la CNT en especial dentro del departamento IP_MPLS.

CLASIFICACIÓN DE ACTIVOS.

La clasificación de los activos, permite inventariarlos asegurando una protección sobre ellos más efectiva.

- ✓ **ACTIVOS DE SERVICIOS.**

  Se pueden mencionar servicios como las comunicaciones y los dirigidos a usuarios.

- ✓ **ACTIVOS INSTANGIBLES.**

  La imagen o marca empresarial, institucional y organizacional.

- ✓ **ACTIVOS PERSONAL.**

  Envuelve al personal miembro del área, sus conocimientos, experiencia y habilidades de trabajo y desempeño.

- ✓ **ACTIVOS INFORMACIÓN.**

  Encierra los procedimientos establecidos, operativos, soporte, configuraciones, información de sistemas, bases de datos, archivos entre otros.

- ✓ **ACTIVOS SOFTWARE.**

  Se pueden mencionar programas desarrollados, software de aplicaciones, software de sistemas, software de monitoreo, etc.

- ✓ **ACTIVOS FISICOS.**

  Entre estos se Incluyen medios de almacenamiento (USBs, discos duros, CDs), equipos de comunicación personal, dispositivos de red y otros equipos técnicos o tecnológicos.

Estos activos deberán ser protegidos debido a que son el medio a través del cual se facilita a los clientes alcanzar sus objetivos empresariales y personales, sin la inversión, propiedad de costos o asumiendo los riesgos de lo que representa la implementación de estos recursos y todas las actividades que están asociadas a ellos, lo que se procura ofrecer es asegurar la información de la que hace uso el área de MPLS.

Es importante referirse a que un servicio contrasta de un bien físico por ser intangible, además el bien físico se desgasta y se consume, el servicio se evalúa por el nivel de confianza del cliente, esto ha originado tener ciertos cuidados adicionales sobre la organización física de la CNT E.P.

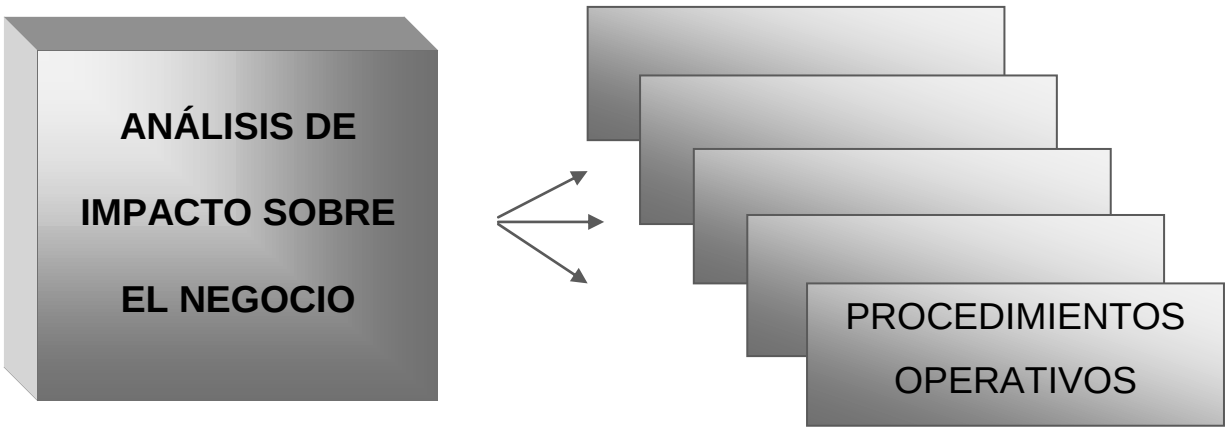
3.2. ANÁLISIS DE IMPACTO AL NEGOCIO.

El involucramiento e información del personal acerca de la realización de un análisis de impacto sobre el negocio es importante y deberá ser considerado, registrado y actualizado en cuanto a todos los cambios en la organización, brindando así el adecuado soporte para una inmediata tipificación del o los incidentes y amenazas ocurridos en el área, para su posterior solución.

Se tomarán en cuenta las condiciones necesarias para lograr la realización del Análisis de Impacto sobre el Negocio (AIN), es decir, considerar un plan de trabajo en el que dentro de su cronograma se revisen aspectos mediante una adecuada y sistemática técnica de recolección de datos que conlleve a la solución inmediata del incidente. (www.ezone.net)

Figura 18.

Procedimientos operativos sobre el AIN.



Aspectos y elementos dentro del Análisis de Impacto sobre el Negocio, como los enlistados a continuación en la tabla 4.

Tabla 4.

Factores de Análisis de Impacto al Negocio.

Análisis de Impacto sobre el Negocio	**Ítems**
✓ Recopilación de datos	✓ Entender la jerarquía de una estructura de acuerdo a un formato básico. ✓ Develar información que se está buscando. ✓ Elaborar una lista de elementos y consultar la lista de los registros obtenido con incidentes o amenazas anteriores. ✓ Plan de seguimiento si el análisis

	inicial demuestra una necesidad de reseñas o búsqueda adicional.
✓ Evaluar los efectos de las paralización de operaciones y los impactos de las mismas	✓ Pérdida de activos. ✓ Personal Clave. ✓ Los activos físicos. ✓ Los activos de información. ✓ La interrupción de la continuidad de los servicios y operaciones. ✓ Legales o reglamento. ✓ Percepción pública de credibilidad en servicios de la CNT.
✓ Determinación de pérdidas.	✓ Pérdida de ingresos. ✓ Pérdida de clientes. ✓ Sanciones responsabilidades legales. ✓ Recurso humano. ✓ Gastos adicionales. ✓ Mayor trabajo.
✓ Definir datos críticos y sus funciones.	✓ Definición de lo esencial para el área de IP_MPLS. ✓ Desorganización, perdida información, seguridad, inactividad de equipamiento y personal. ✓ Tiempos de recuperación: críticos y menores. ✓ Identificación de datos más relevantes para asegurar la continuidad de operaciones. ✓ Existencia de equipos de apoyo.

	✓ Identificación de aéreas afectadas por su relación con el departamento de IP_MPLS.
✓ Determinación de tiempo y recursos	✓ Criterios de criticidad de las operaciones. ✓ Requisitos mínimos de recursos. ✓ Priorización de funciones paralelas e independientes. ✓ Orden de recuperación. ✓ Evaluación de pérdidas sin perjuicio ante incidentes o amenazas. ✓ Evaluación de pérdidas y su perjuicio ante incidentes o amenazas.
✓ Procesos de solución	✓ Tiempos de reemplazo de equipos. ✓ Puesta en marcha y operación de equipos. ✓ Personal. ✓ Evaluación de pérdidas y su perjuicio ante incidentes o amenazas. ✓ Priorizar elementos críticos para la mitigación del impacto.

3.2.1. CATEGORIZACIÓN DE RIEGOS

CLASIFICACIÓN DE LOS RIESGOS SEGÚN SU MAGNITUD.

Una clasificación de los riesgos proporcionará un amplio rango de ideas y planes de seguridad en contra de cualquier amenaza

riesgo o incidente dentro del área de IP_MPLS, que asegurarán la continuidad de negocio minimizando daños posibles.

Esta clasificación se mantendrá como resultado de haber gestionado controles como prácticas, políticas, medios, procesos y estructuras organizativas siendo algunas de ellas ya existentes dentro de los registros de la CNT, que fomentarán las buenas prácticas de los procesos de solución en cada situación.

3.2.2. IDENTIFICACIÓN DE LOS RIESGOS.

Establecidos, monitoreados y revisados los riegos de incidentes dentro del departamento de IP_MPLS quedarán tipificados de la siguiente manera como:

3.2.2.1. IDENTIFICACIÓN DE LOS RIESGOS FÍSICOS.

Los riesgos de acontecimientos físicos identificados en el Departamento de IP_MPLS tienen un grado de ocurrencia igual que todos los tipos de incidentes analizados, lo que no podemos conocer es cuando sucederán.

- ✓ **Incidentes en el suministro eléctrico.**

  Un incidente de este tipo no está dentro de los que la CNT puede controlar, pero al hacer uso de éste servicio, se encuentra en la necesidad de contrarrestarlo.

  Para ello, la CNT en todas sus áreas (tanto técnicas como administrativas) mantiene y dispone de los respectivos respaldos, con fuentes de energía alternativa, minimizando así el riesgo de una paralización en sus servicios y operaciones por incidentes de este tipo.

- ✓ **Incidentes en las comunicaciones.**

  En el desarrollo de un incidente y/o durante los procedimientos diarios y normales de un día de trabajo, las técnicas de comunicaciones (telefonía, celular, email) y su contenido se alteran de acuerdo al volumen de cada una ellas, por ende una falla en los sistemas de comunicación internos o externos puede derivar en una paralización de las operaciones.

  Por lo tanto resulta esencial que las comunicaciones se mantengan en funcionamiento constante para mantener el servicio y la operatividad del personal.

- ✓ **Fallos en cableado eléctrico.**

  Se originan por fallas eléctricas que no han sido detectadas a tiempo provocando incendios o corto circuitos, debido a que se ven ocasionalmente, ya que no es una tendencia y tampoco forma parte de las estadísticas.

  En las instalaciones eléctricas de la CNT, se han preocupado del buen estado y una adecuada conexión a tierra en todas sus áreas, evitando de esta manera que equipamiento de altas prestaciones sufra electrificaciones, por lo tanto, el cable a tierra derivará cualquier ráfaga hacia el suelo, imposibilitando además las descargas eléctricas en las personas que operan estos dispositivos.

- ✓ **Tuberías de agua defectuosas.**

  En la actualidad, el clima ha provocado desperfectos en cañerías causando emergencias y contratiempos, ya que

varias de estas instalaciones de agua atraviesan cuartos de pruebas, laboratorios, salas de computo, etc., y un buen modo de evitar estos inconvenientes es aislar las tuberías.

Una solución sencilla y económica es la utilización de coquillas, unos cilindros rígidos que se adquieren en cualquier tienda de bricolaje. Éstos evitaran el filtrado del agua hacia y en lugares donde se encuentran equipos de alta tecnología y que además son proveedores de servicios.

- ✓ **Instalación de equipamiento sobre paredes viejas o húmedas.**

La formación de condensaciones de agua sobre superficies tiene distintas causas: tuberías en mal estado, humedad y temperatura, esto conduce a un aumento de la resistencia a la transferencia de calor y en consecuencia, a un descenso de la temperatura de las superficies.
La condensación de agua no sólo empeora el clima en la sala de equipos, sino que ocasiona daños en las superficies de paredes, techos y muebles.

La mayoría de racks, equipamiento y cableado están sujetos a paredes, lo cual ocasionaría un conato de riesgo si la humedad debilita muros que sumado al peso de los equipos provocaría la caída de los mismos, convirtiéndose en un hecho que paralizaría las parte de las operaciones del Departamento de IP_MPLS en la CNT.

- ✓ **Incidentes ocasionados accidentalmente por el personal de limpieza.**

  Otro posible incidente físico que pudiera acontecer dentro de cualquiera de las instalaciones de la CNT y de cualquier empresa, es que el personal de limpieza o mantenimiento de una manera no intencional, quizá descuidada, derrame o vierta líquido o sustancias que ocasionen graves incidentes a los dispositivos o equipamiento

- ✓ **Daños en los equipos de aire acondicionado.**

  El cuerpo humano mantiene una temperatura constante de 37°C. Cuando el ser humano es expuesto a temperaturas altas se origina una gran transpiración, si por el contrario, tenemos bajas temperaturas la deshidratación se da en la respiración, lo que quiere decir que es mucho más severa, por tanto: el área de trabajo debe tener un sistema de aire acondicionado apropiado y funcionado, además provisto de ventanas adecuadas que complementen la idoneidad del ambiente en los cuartos de equipos como servidores, distribuidores, centrales y salas de operaciones del personal técnico.

- ✓ **Incidentes causados por desastres naturales. (Terremotos, temblores, maremotos, tsunamis, erupciones volcánicas, huracanes, inundaciones, derrumbes, etc.).**

  Esta clase incidentes es imposible de anticipar, por tal razón la continuidad comercial y la planificación para emergencias están adquiriendo una nueva importancia, requieren de un plan para contrarrestar su impacto. Por la importancia de los servicios que provee y la gran cantidad de clientes que posee

la CNT y su área de IP_MPLS, puede beneficiarse al tener listo un equipo de iniciativas ya planificadas en caso de este tipo de desastres, que sería resuelto rápidamente en coordinación con la policía nacional y bomberos evitando así interrupciones prolongadas de los servicios.

- ✓ **Incidentes causados por el hombre.**
  (Huelgas de personal, terrorismo, sublevación policial o militar, paralizaciones en carreteras, guerras, robos, etc.).

  Un claro ejemplo reciente en el Ecuador, fue la intrusión de actores políticos y personal desconocido a las instalaciones de Ecuador TV y de los policías sublevados el 30 de septiembre de 2010 con el planeamiento de la destrucción premeditada de las antenas del mencionado canal y evitar así la continuidad de sus transmisiones. Ante esta situación, la infraestructura del departamento de IP_MPLS y la CNT, no está lejos de ser un objetivo de sabotaje por el gran conjunto de infraestructura e información que soporta y la enorme cantidad de usuarios que hacen uso de sus servicios.

  Ante esta amenaza convertida ya en latente y muy probable, se deberá conformar un segundo centro de gestión con su respectivo personal que permita realizar, maniobrar, dirigir, modificar y devolver la continuidad de las operaciones que resulten afectadas después de la materialización de la misma, logrando así que las operaciones se mantengan en funcionamiento.

- **POLÍTICAS DE SEGURIDAD.**

La primera característica que deben tener las políticas de seguridad en el departamento de IP_MPLS, es contemplar apropiados controles para reducir riegos.

Deberá ser parte de un conjunto de herramientas para la concientización del personal dentro y fuera de la CNT, con el objetivo de mantener minimizadas las amenazas y los incidentes de infraestructura e información interna.

La implementación de políticas seguras, permite la anticipación de medidas para la detección y detención de agresiones que pueden complicar, eliminar, modificar la integridad de la información.

Ya se ha mencionado que uno de los problemas de seguridad son los usuarios, ya que son el eslabón más débil en las redes de telecomunicaciones, son ellos quienes disponen y manipulan la información, por lo tanto: la seguridad comienza y termina con los usuarios de la red.

Los componentes importantes de las políticas internas están dadas por:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Cumplimiento de las políticas.

Se puede concluir que toda la información es importante, por ende se debe tener varios niveles de seguridad y precauciones con la

información que ingresa a la red, como pueden ser archivos en emails.

El disponer de un firewall, antivirus o de un servidor web actualizado, no garantiza un red segura al 100 por ciento.

Las políticas de seguridad deberán enfocarse en tres áreas:

- ✓ Área tecnológica.
- ✓ Área de personal.
- ✓ Área de la autenticación, autorización y auditoria.

Evitando que esta ultima (la autenticación, autorización y auditoria), sea vista como una dificultad para los usuarios cuando estos manejan la información, sino mas bien como una mejora continua en su seguridad que controlará de mejor manera el acceso de los usuarios a cada uno de los recursos de la infraestructura del departamento de IP_MPLS.

3.2.2.2. IDENTIFICACIÓN DE LOS RIESGOS LÓGICOS.

Los riesgos de incidentes lógicos son imperceptibles para el común de las personas, pero para una infraestructura como la que posee una institución como la CNT y su departamento de IP_MPLS, se ha convertido en una prioridad la seguridad a este nivel.

*Mediante un estudio titulado **Trust, Security & Passwords**, realizado y enfocado a profesionales dedicados a la Administración de infraestructura de red y de seguridad informática por Cyber-Ark, arrojo los resultados siguientes:*

El 88% de los responsables o administradores de informática, admiten que se llevarían información valiosa y sensible de sus empresas, como por ejemplo: información financiera y todas las contraseñas que pudieran conseguir, las claves de los directivos y usuarios, información de las bases de datos importantes de sus clientes, si fueran despedidos inmediatamente.

En el mismo estudio indica que, más de un tercio de las empresas creen que el espionaje industrial y el robo de datos son crecientes incluyendo información que llega a competidores o en el peor de los casos a criminales cibernéticos vía correo y memorias USB. Y una cuarta parte admite de los entrevistados creen que sufren de sabotajes internos.
(www.itworld.com)

Esto conlleva a concluir que, el gran problema de la seguridad en la CNT y su departamento de IPMPLS, así como de todas las empresas, son sus usuarios internos, ya que son estos quienes manipulan y conocen de la información.

El soporte de este estudio permitirá desarrollar los siguientes puntos a ser evaluados.

- ✓ **Por omisión y/o error.**

  Para evitar un incidente tan elemental como el de omisión y/o error, el personal deberá dejar el razonamiento o la idea de:
  Lo que no está expresamente prohibido, resulta estar permitido.

  Esta forma de pensar puede traer consecuencias nefastas para el departamento IP_MPLS y la CNT, es decir no se debe esperar encontrar un letrero en cada uno de los lugares de

trabajo, que prohíba o limite una acción como por ejemplo “no ingerir alimentos mientras trabaja” (siendo esta acción, pudiera convertirse en accidente, si llegase a suceder sobre un servidor o un router, dejando consecuencias graves a la infraestructura tecnológica), para hacer conciencia de que eso no está permitido.

- ✓ **Incidentes de seguridad en los sistemas.**
  (Políticas ajustadas de manera contraria y/o errónea a las requeridas en la empresa).

  La posibilidad que brinda el comunicarse a través de redes informáticas, han abierto también, el deseo de aprovecharse de infraestructuras privadas o públicas con el único fin de causar daño, trayendo al mismo tiempo nuevas amenazas para los sistemas de información existentes.
  El departamento de IP_MPLS, actualmente mantiene un plan de políticas de seguridad, sus políticas se han basado a nivel de usuarios y de gestión.

  Entonces se puede decir que desarrollar un sistema de seguridad significa la planeación, organización y control de las actividades, con el objetivo de garantizar la integridad lógica y física de los recursos informáticos, comunicaciones y servicios, además de los activos de la empresa.

  Las políticas aplicadas no funcionan solas, forman solamente una precaución para la confianza del área de IP_MPLS, responderán a la visión del área y a su personal lo que requiere de un esfuerzo conjunto de sus integrantes por gestionar los recursos de seguridad, siendo estos los factores que facilitan

la formación y materialización de los compromisos empresariales.

- ✓ **Delitos informáticos.**
  (Provocados por Hackers).

  Considerando el valor de los bienes intangibles de la informática, los servicios, la infraestructura, especialmente la alteración de datos de computadora y las plataformas tecnológicas dentro del área de IP_MPLS, se deberá tener un especial cuidado con el acceso que se podría efectuar a menudo desde un lugar externo, situado en la red de telecomunicaciones, el Hacker una vez dentro de la red, aprovechará la falta de control existente en la red para obtener acceso y así descubrir posibles deficiencias en las políticas de seguridad implementadas hasta hoy para la protección de los procedimientos del sistema.

  Una vez conocidos los defectos de seguridad en la red, continuamente el intruso informático se autenticará como un usuario común pero legítimo del sistema; esto es una de las consecuencias que atraen en su mayoría los sistemas donde sus usuarios emplean contraseñas comunes y sencillas o contraseñas de mantenimiento que se mantienen dentro del propio sistema, dando así arranque al continuo deterioro informático de la red.

  Es importante indicar que también los usuarios comunes de internet, cometen infracciones al enviar programas piratas, archivos infectados o realizar intromisiones en los sistemas gubernamentales o más comúnmente en programas y plataformas de entidades bancarias.

Entre los tantos conceptos y criterios acerca de los delitos informáticos, podemos concluir en componentes comunes: el computador como medio o como el fin de la infracción; y por otro lado, el uso de la informática (ciencia que estudia la información cualquiera que fuere su soporte físico) para el cometimiento de hechos catalogados como criminales.
(MERLAT, 1999)

- ✓ **Entrada de virus o malware.**
  (Código malicioso en información de usuarios).

La importancia de llevar un control y limitación en la información que ingresa vía correo electrónico hacia los usuarios de la intranet evitaría la intrusión indeseada de software y programas maliciosos a la red de telecomunicaciones en el área de IP_MPLS de la CNT, ya que son elementos informáticos, que tienen tendencia a multiplicarse y a desarrollarse dentro del sistema al que acceden, se infectan de un sistema a otro, presentan varios grados de malignidad y son casualmente, incapaces de ser destruidos con el uso de ciertos antivirus, pero otros son capaces de desarrollar bastante tenacidad a estos.

- ✓ **Pérdida de información.**

Es muy probable que personal de MPLS, por motivos de trabajo haya almacenado información en un pen drive, memoria USB o en un disco duro portátil, y que la mencionada información sea extraviada.

Dependerá de la cantidad de información y del destino de esa información una vez que su recuperación ya ha sido considerada nula y las intenciones de quien la encuentre, para ocasionar un daño a la red de telecomunicaciones de la CNT.

- ✓ **Robo de información.**

Este incidente solo podrá ocurrir con personal que trabaja en el departamento de MPLS, ya que son los únicos con acceso directo a computadores en los que se almacena importante información sobre configuraciones, estructura de red, estado de interfaces, puertos habilitados, direcciones de red y de equipamientos, dispositivos, etc.

Lo difícil sería identificar quien fue el causante del robo de información. Es por eso que, se requerirá de personal completamente comprometido con el área, y sienta responsabilidad empresarial.

- ✓ **Venta de la información.**

La venta de información como tal, ocurrirá cuando el personal miembro del área MPLS, se sienta inconforme con el puesto que ocupa, para perjuicio de otros, o perjuicio empresarial, y al no existir una política que prohíba sacar con la debida responsabilidad información vital del área MPLS, también será difícil el conocer que propósito fue el extraer la información.

- ✓ **Borrado de la información.**

  Se entenderá como la pérdida de información involuntaria, siendo fácil de solucionar si se dispone de una fuente o de un apropiado respaldo.

- ✓ **Alteración o manipulación de la información.**

  La manipulación de la información puede darse de dos maneras:
  Planificada.- es aquella en la que existe un objetivo de mejoramiento, actualización, estudio o necesidad primordial en cuanto al alcance de la información.

  No planificada.- tiene que ver con aquellos actos que solo pueden ser causados con el fin de dañar los procedimientos establecidos dentro del área.

  Siendo esta última el motivo de origen de un incidente del que no se podría conocer sus razones ni su alcance inmediato.

- ✓ **Accesos no autorizados sin perjuicios visibles a componentes tecnológicos.**

  Esta dentro de lo que se conoce como amenaza informática, siendo potencialmente un peligro para la seguridad de la infraestructura de la red MPLS.

  Se caracteriza por no existir inmediatamente un daño, se cree que el primer ingreso es de mera exploración a la red, sin embargo, sus consecuencias no demoran en tomar forma y presentarse dejando secuelas irreparables.

(Canosa, 2011), (SIC., 2005)

Un incidente de información está determinado por una serie de eventos no deseados que tienen una alta posibilidad de causar paralización a las operaciones y servicios que provee la CNT a través del departamento de IP_MPLS.
Aquí tenemos los siguientes.

AMENAZAS INFORMÁTICAS.
(ABOSO, 2006)

- ✓ **Packet sniffers.**

Todos los tipos de servicio de red para usuarios internos y externos que hacen uso de PING, HTTP, SMTP, POP3, FTP, etc., habilitando puertos que en el sistema se requiere mantener protegidos para evitar incidentes de ataques informáticos probables en la red.

La implementación de Packet sniffers se realiza para comprobar cada evento en la red y puede ser utilizado con fines maliciosos.

- ✓ **Man in the middle.**

El principal indicio de que la red está siendo agredida por este tipo de ataque, es cuando la velocidad de la conexión se ve afectada ya que la mayoría son para la red local la información debe viajar por varios puntos o nodos, convirtiéndose en motivo de alarma para su posterior revisión, descarte y/o solución.

Incidentes a nivel de software, base de datos o programas, se pueden considerar varios tipos de este tipo, por ejemplo:

- ✓ **SQL Injection**.

  Sucede cuando se inserta un código SQL malicioso dentro de otro código SQL con el fin de destruir su buen y normal funcionamiento.

- ✓ **Key Loggers.**

  Es un malware del tipo daemon, encargado de registrar la pulsación sobre el dispositivo de entrada (el teclado) almacenándolas en un archivo y enviándolas por la red hacia el internet.

- ✓ **Hacking Wireless**.

  Las redes inalámbricas operan en sus respectivas frecuencias de operación, si éstas redes no poseen ningún tipo de encriptación las tramas que circulan por la red podrán ser extraídas, obteniendo de esta manera la información o la posibilidad de conectarse a los recursos compartidos.
  Además la intrusión de virus, gusanos, troyanos, etc.

- ✓ **Cracker y Hackers.**

  Este tipo de incidentes es provocado por individuos capaces de realizar ingeniería social (quiere decir obtención de información a través de usuarios verdaderos).

  Desde cualquier punto los hackers ingresan a la red de telecomunicaciones aprovechando la falta de definición en la seguridad, simulando ser usuarios propios o empleando contraseñas que están dentro del sistema.
  (Huerta, 2000)

- ✓ **Rootkits.**

  Evaden el hecho de que un proceso malicioso pueda ser identificado o visible en el listado de procesos de los sistemas infectados o que sus archivos sean visibles en el explorador de archivos.
  Formado por un conjunto de herramientas que esconden a programas, archivos, procesos, directorios y puertos, lo que permitirá a los intrusos el acceso a los sistemas remotamente para sustraer la información, atacar y manipular equipamiento o dispositivos.

- ✓ **Buffer overflow.**

  Provocado por un error de software, con y sin la ejecución de shellcode, al copiar datos en una área física del equipo que no es capaz de contenerlos.

- ✓ **Exploits.**

  Este tipo de amenaza incluye en su estructura un shellcode, para ejecutar una secuencia de comandos preestablecidos.
  Los exploits están caracterizados por realizar un ataque a los sistemas operativos según la vulnerabilidad que muestren, así:

  Vulnerabilidades de Inyección SQL, desbordamiento de buffer, error de formato de cadena, inyección de caracteres, denegación del servicio, ventanas engañosas o Window Spoofing, estas vulnerabilidades son agredidas con el único fin de destruir o inhabilitar el sistema.
  (FERNADEZ, 1988)

3.2.2.3. IDENTIFICACIÓN DE LOS RIESGOS TECNOLÓGICOS.

En cualquier momento de vida de un sistema de información tecnológico existen ciertos eventos que pueden desencadenar situaciones conflictivas que requieren cambios u otros tipos de intervención.

Para lo cual la parte tecnológica dentro de la CNT, se ha convertido en un valor económico de primera magnitud, y en su principal patrimonio, su utilización ha sido creciente en casi todos los ámbitos de las actividades de empresas nacionales y extranjeras así como de todos sus usuarios en el Ecuador, esto ha hecho que la confianza de sus beneficiarios sea un factor de desarrollo en el negocio de datos y del departamento de IP_MPLS.

Figura 19.

Relación de infraestructura tecnológica.

Figura tomada de los manuales informativos y esquemas de red de la CNT.

- ✓ **Fallos en los sistemas de información.**

  En general, la integración de hombre máquina para la resolución de este tipo de fallos requiere de una recolección de información y la posibilidad de su aplicación en todo su entorno, ante la dependencia entre sus activos, como puede ser la información y recursos relacionados que son necesarios para que la CNT, funcione correctamente.

- ✓ **Equipamientos con desperfectos en su fabricación.**

  Los incidentes de este tipo se han de solucionar mediante el uso de garantía de los equipos que presenten problemas de funcionamiento y que ocasionan molestias a usuarios y personal técnico.

  Es imprescindible, contar con un proceso de adquisición debidamente elaborado asegurando el funcionamiento mediante el uso de un periodo de pruebas para los dispositivos y equipos.

- ✓ **Falta de mantenimiento periódico.**

  No ha existido equipamiento, plataforma, o sistema tecnológico que no requiera de mantenimiento periódico (limpieza, cambio de partes, actualización, etc.)

  Este mantenimiento por lo general es ofrecido por los proveedores, lo cual no limita al personal propio de la CNT a preocuparse por mantener los equipos, plataformas y dispositivos en perfectas condiciones.

- ✓ **Equipos que no cumplen con las especificaciones requeridas por la CNT, ni entregadas por el fabricante.**

  Se puede presentar la situación en que los equipos contratados no cumplan con requerimientos que el área MPLS solicita para mejorar el servicio a los usuarios, debiéndose considerar al momento de la adquisición un periodo de pruebas con el afán de disminuir la ocurrencia de estos eventos poco profesionales por parte del proveedor de los mismos.

- ✓ **Incidentes en las fuentes de alimentación a base de baterías.**

  El pretender minimizar este tipo de incidentes, lleva consigo la labor de mantener un registro actualizado sobre la vida útil del sistema de energía alternativo existente en el área MPLS, es decir, tener constancia exacta de las fechas de instalación, periodos de mantenimiento, registros reales de operación, etc., que ayudarán a mejorar los sistemas y a no interrumpir los servicios.

- ✓ **Interrupción de los servicios de red y acceso a los sistemas de información.**

  Debido principalmente a la falta de comunicación se puede presentar un incidente de este tipo, ya que la interrupción de cualquier servicio interno (coreo electrónico, páginas o anuncios vía web, servicio telefónico) debe ser planificada y tener la respectiva anticipación para el conocimiento de todos los usuarios.

La renovación tecnológica también puede convertirse en un incidente de interrupción de servicios, acceso a la red y a los sistemas de información, los responsables de la realización de los trabajos definirán las acciones a seguir, mediante la designación de un equipo responsable para seguridad de la información.

- ✓ **MANTENIMIENTO DE SISTEMAS.**

Conocer los sistemas que posee el área de IP_MPLS permitirá ofrecerles un mejor mantenimiento que ayudará a contemplar todos los aspectos necesarios para su buena planificación e implantación.

El poder identificar las exigencias que los sistemas requieren deberá ser capacidad de cada miembro del departamento, incluyendo las políticas como se indico en el punto anterior.

El componente tecnológico es un elemento de la plataforma que abarca entre otros los siguientes:

- ✓ Equipos activos de red: switches, rotures, puntos de acceso inalámbrico (Access point).
- ✓ Sistemas operativos y de Información.
- ✓ Servidores / PCS / Impresoras / Red de datos
- ✓ Internet/ Intranet.
- ✓ Correo electrónico (Microsoft Exchange)

- ✓ **Sistema operativo.**

El sistema operativo es un conjunto de secuencias y programas que llevan el buen funcionamiento y mayor

provecho de un computador, que es el encargado de controlar electrónicamente las unidades periféricas, la memoria y los dispositivos conectados.

- ✓ **Sistema de información.**

Con su utilización se logran significativos adelantos, ya que mecanizan, automatizan y simplifican los procesos operativos, facilitando a la plataforma de información conectada la toma de decisiones logrando ventajas profesionales.

- ✓ **Prohibición o Denegación de servicio.**

Sus siglas DoS/DDoS, este tipo de amenazas a la red provoca que un recurso sea difícil para usuarios legítimos, provocando perdida de conectividad y exceso en el procesamiento de recursos en el sistema de la víctima.

3.3. SELECCIÓN DE ESTRATEGIAS.

IDENTIFICACIÓN DE VULNERABILIDADES.

Una vulnerabilidad es una abertura o falencia, virtualmente causada por una falla en diseño o un error de una aplicación, permitiendo que un invasor de la red tenga la posibilidad de provocar daño a la infraestructura.

El objetivo es causar molestias en el servicio, aplicaciones y clientes, ante el incremento constante de amenazas informáticas, las vulnerabilidades también crecen al mismo ritmo y no deben ser consideradas como simples errores u omisiones por parte del personal que administra la red pero que en ocasiones puede tener desconocimiento de las buenas prácticas de seguridad.

Descubrir un ataque informático hoy en día, es muy complicado, puesto que, puede ser realizado desde cualquier parte del mundo e incluso de varios sitios a la vez.

A las vulnerabilidades se las puede clasificar mediante varios criterios o niveles como:

- ✓ Su nivel de confianza.
- ✓ Su nivel de riesgo.
- ✓ Su nivel de incidencia.
- ✓ Su nivel de impacto.
- ✓ Su nivel de complejidad.
- ✓ Su nivel de resolución.

Todos los elementos administrados y gestionados demuestran algún grado o nivel de debilidad en uno o más activos que podrían ser atacados y por ende estar expuestos a una amenaza, con consecuencias graves como el robo, destrucción, perdida, intercepción, extracción y hasta la modificación de información de forma fraudulenta, siendo esta amenaza una causa potencial de un incidente no esperado en la infraestructura de red.

La vulnerabilidad se presenta principalmente por:

- ✓ Desactualización del personal.
- ✓ Desactualización tecnológica.
- ✓ Falta de conocimiento.
- ✓ Falta de sensibilización.
- ✓ Omisiones de seguridad.
- ✓ Falta de registros y controles de seguridad.
- ✓ Conexiones de usuarios cerradas incorrectamente.
- ✓ Cierre incorrecto de la conexión de base de datos.

Entonces, cualquier incidente de algún dispositivo perteneciente a la red, es importante contar con una regla o procedimiento que admita su pronta recuperación para su debido registro, reconocimiento y análisis lo que permitirá minimizar el costo operativo de su recuperación.

3.3.1. MANIOBRAS/ESTRATEGIAS DE RESTAURACIÓN.

Dentro de una infraestructura tan grande y tan diversa como la existente en el departamento de IP_MPLS, siempre está latente la probabilidad de ocurrencia de una amenaza o incidente.

No basta con la implementación de las mejores herramientas tecnológicas, también es necesario una selección de las observaciones para la identificación de riegos, solo así se podrá obtener un resultado que indique la probabilidad cercana de su ocurrencia.

Se seleccionará la maniobra o estrategia acorde al incidente que garantice la minimización de daños a los recursos y servicios provistos por el área de IP_MPLS.

La ejecución de la técnica correcta, estándares o métodos alternativos válidos para el desarrollo de estrategias o maniobras de restauración están dadas por:

- ✓ Información del incidente a los canales apropiados.
- ✓ No urgentes, no hacer nada.
- ✓ Planificación minuciosa
- ✓ Reubicación de personal y reutilización de recursos.
- ✓ Conexiones de trabajo remoto
- ✓ Realización de pruebas continuas
- ✓ Reubicación de operaciones, no de personal.
- ✓ Reubicación de operaciones y de personal.

Antes, durante y después de ocurrida una amenaza en el departamento de IP_MPLS, también existirán consecuencias de grupo de trabajo que beneficiarán y mejorarán las próximas acciones frente a un incidente de cualquier tipo.

- ✓ **La fusión en una asociación.**

  El trabajar en una verdadera asociación a veces figura adecuar un nuevo proceso o procedimiento hacia nuevas fusiones.
  Un sistema titular de herramientas y programas no puede ser la solución más eficaz, así que estar abiertos a cambios y negociaciones es una forma de avanzar rápidamente.

- ✓ **Crear un entorno de pruebas.**

  La instauración de este ambiente de unificación de tecnologías de varios fabricantes dentro de la CNT, corresponderá a su eficacia ante la presencia de una amenaza a la infraestructura, siendo un requisito previo necesario para probar y soportar la red de nueva generación que crece día a día.

- ✓ **Plan colaborativo.**

  Para la obtención más rápida de soluciones, se necesita una estrecha cooperación y despliegue de la planificación colaborativa del área de IP_MPLS, para la introducción de estos nuevos procedimientos que aseguran el aceleramiento de pruebas y aceptación, llevando al rápido despliegue de la red.

- ✓ **Gestión del cambio.**

  Cualquier proyecto, o plan que tenga como objetivo el mejoramiento de la infraestructura física, tecnológica u organizacional requiere un grado de flexibilidad de las partes que lo conforman.

  La necesidad de gestionar este cambio deberá ser de una forma controlada para confirmar que no se impacta la planificación inicial del proyecto o su implementación simultáneamente a los procesos y herramientas para la vigilancia oportuna de las operaciones.

- ✓ **Gestión del equipo.**

  La creación de un equipo con la adecuada idea de trabajo operativo durante corto espacio de tiempo, se convierte en un desafío.

  No se debería detener en el proceso de incorporar personal que asegure la culminación y éxito de operaciones para que cada uno sepa que realmente está contribuyendo con su trabajo en los procesos planificados.

- ✓ **Definición de los objetivos.**

  La definición de los objetivos y la distribución del equipo dentro del área de IP_MPLS, establecerá resultados y una experiencia de un verdadero equipo de trabajo.
  El producto final es la determinación de una adecuada estructura para escalar rápidamente las situaciones de riesgo. Entonces resulta vital el mantener el impulso sobre el proyecto.

- ✓ **Selección de estrategia.**

  Están definidas por procedimientos funcionales en los cuales se generan estándares del ejercicio del negocio que serán medidos con las herramientas de control de las que dispone la CNT.

  Evitará también, el recorrer toda el área de IP_MPLS para la consulta de las soluciones posibles ante cualquier incidente o amenaza ocurrente.

  Una buena estrategia, es la manera de intercambiar el conocimiento adquirido en el área por un largo tiempo de trabajo, permitiendo la actualización interna de todos los participantes del departamento de IP_MPLS.

- ✓ **Aplicación de la estrategia para la solución.**

  Una vez que el origen de la interrupción se ha identificado, se procederá con la recolección de la información, la evaluación y el análisis del impacto sobre el negocio y sus operaciones, que determinarán en su conjunto los tiempos de recuperación necesarios para la normalización de los servicios del departamento de IP_MPLS.

  Cabe recalcar que no si no existe el seguimiento propicio, el modelo termina fracasando.

El resultado para el área de IP_MPLS, después de la aplicación de la estrategia ante incidentes o amenazas, es la mejora continua, el registro de los incidentes, la recopilación de nueva y actualizada información, además, tiempos de respuesta menor que minimizarán la probabilidad de su ocurrencia.

3.4. DESARROLLO Y PERFECCIONAMIENTO DE PLANES.

3.4.1. LOS CONTROLES NECESARIOS PARA IDENTIFICAR RIESGOS

Dentro de las posibilidades reales de la CNT y su departamento de IP_MPLS, está la disponibilidad de que su personal sea preparado en cuanto a la importancia de los activos que posee la empresa.

Una selección apropiada de los controles para la identificación de los riesgos dependerá de las herramientas tecnológicas u organizacionales con los que cuenta el área de IP_MPLS.

Tabla 5.
Ejemplo de controles que evitarán incidentes.

Acción	**¿Qué se examina?**	**Frecuencia de revisión**	**¿Quién lo examina?**	**Riesgos asociados a la acción tomada**
Monitorear red de datos	La operación de los servicios activos de la red	Diaria	Jefe de Grupo – Responsable de área.	Paralización de los servicios en la red. Paralización de acceso a los sistemas de información.
Analizar desempeño y capacidad	Análisis de desempeño y capacidad	Semanal	Responsable de área - Administrador	Sub-utilización. Saturación.

			de Red - Jefe de Grupo.	Obsolescencia.

Estas herramientas podrán ser:

- ✓ Tecnológicas
- ✓ No tecnológicas

3.4.1.1. TECNOLÓGICAS.

El control tecnológico requiere de un previo conocimiento de las herramientas aplicables y disponibles dentro del área de IP_MPLS, así tenemos:

- ✓ **Módulos de seguridad.**

Los mecanismos de seguridad pueden ser herramientas, procesos, normas y establecimiento de procedimientos como los detallados a continuación:

- ✓ Sistemas de control de acceso (ACS)
- ✓ Firewall (Cortafuegos).
- ✓ Políticas de seguridad.
- ✓ Elementos para acceso remoto como Secure shell o IPSec.
- ✓ Elementos de integridad VPN.
- ✓ Seguridad en plataformas tecnológicas.
- ✓ Sistemas de alarmas.
- ✓ Seguridad de sistemas operativos.
- ✓ Seguridad en redes inalámbricas.
- ✓ Gestión de seguridad.
- ✓ Seguridad en base de datos.

- ✓ Seguridad infraestructura de red.

(ABOSO, 2006)

- ✓ **Monitoreo de alarmas.**

  La disponibilidad de los sistemas de alarmas en la infraestructura de la red resulta un elemento importante para la detección e identificación de problemas, se convierte en una herramienta con la que el administrador dispone de un apoyo tecnológico para conocer que existe un problema en la red.

  Igualmente es tratada como técnica de monitoreo, que contiene un conjunto de dispositivos que permiten anunciar que ha acontecido una molestia en la red mediante su aplicación.

- ✓ **Administración de la seguridad.**

  El objetivo es defender los recursos de la infraestructura de la red alejada del alcance de virtuales usuarios maliciosos, implementando una estrategia de control de acceso y control a la red IP_MPLS

- ✓ **Descubrimiento de intrusos.**

  El objetivo de lograr la identificación de intrusos, lo es posible a través de un sistema de detección de intrusos que alerte y registre el tráfico que transita por la red, apoyado en un esquema de notificaciones o alarmas que indiquen el momento en que se detecte una situación anormal en la red.

- ✓ **Firewall.**

  Es un sistema de confirmación trazado para impedir el acceso no autorizado a las comunicaciones malignas.
  Siendo un impedimento en contra de sistemas malignos desde internet, por políticas de sistema puede bloquear cualquier tipo de sistema a internet, a menos que sea configurado de manera diferente.

  A pesar de ser una herramienta segura y confiable, el firewall es vulnerable a ataques ejecutados desde puertos usb, cd rom, dvd o hardware, por lo que el complemento apropiado es el uso de un antivirus.

  Las consideraciones significativas que se debe trabajar para obtener superior seguridad en la red, es que mientras más bajo en el modelo OSI actué el firewall implementado en el área de MPLS, mayor será la eficacia con la que operará para resistir futuras agresiones de red.
  En definitiva todos estos elementos en su conjunto conforman el modelo de seguridad necesario para la red IP_MPLS de la Corporación Nacional de Telecomunicaciones.

3.4.1.2. NO TECNOLÓGICAS.

En este sentido, solo existe una manera de fortalecer al Departamento de IP_MPLS, esto se logrará con la implementación de ciertos controles necesarios para proteger los activos que posee.

- ✓ **Instrucción de personal.**

La meta principal de las estrategias de seguridad es crear los requerimientos y recomendados para preservar convenientemente la infraestructura IP y la información ahí comprendida.

Una política define los mecanismos por los cuales estos requerimientos deben ser plasmados para su funcionamiento y ejecución.
El grupo IP_MPLS de CNT aplica todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

Esto se lo logrará con la formación de personal, que permitirá su desarrollo en la administración de la seguridad tecnológica, esta formación abarcará:

- ✓ Cursos elementales de seguridad
- ✓ Cursos concretos de seguridad
- ✓ Cursos especialistas de seguridad
- ✓ Y estos controles acompañados de una importante concientización acerca de la relevancia de la seguridad.

- ✓ **Realización de auditoría.**

Una auditoria de confianza se orientará en el examen de vulnerabilidades, cumplimiento legal de estándares implementados en la infraestructura de red del área IP_MPLS de la CNT.

Algunos tópicos que una auditoria dejaría en evidencia de que existe algún tipo de posible incidente o amenaza sería los siguientes:

Auditoría en sistemas de código, sistemas operativos, antivirus, páginas web, redes LAN, redes WIFI, firewall, políticas de seguridad, distribución física de la red, etc.

Se entenderá que una auditoria de seguridad de red siempre se debe realizar debido al significante crecimiento de los ataques y amenazas que continuamente comprometen la seguridad de la infraestructura de red en la CNT.
Esta auditoría arrojará como resultado todas aquellas debilidades potencialmente dañinas para la infraestructura del área de IP_MPLS, brindando así un confiable control para la identificación de riegos y amenazas.

El Retorno de inversión (ROI) que brinda una auditoria se refleja en la continuidad de las operaciones y la provisión de los servicios en el área de IP_MPLS.

3.4.2. LOS CONTROLES APROPIADOS QUE REDUCIRÁN RIESGOS.

Cada vez son más los recursos que deben ser implementados para brindar el confort laboral, para cumplir exitosamente las operaciones dentro del área de IP_MPLS en la Corporación Nacional de Telecomunicaciones.

Los conflictos tecnológicos pueden ser claramente reducidos con la ayuda de la tecnología, para aumentar la productividad y tiempo efectivo realizando actividades de mejora de servicios y/o procesos en forma eficiente.

Se podrá alcanzar el objetivo de la reducción de riesgos e incidentes dentro del área de IP_MPLS, con la aplicación de los controles adecuados que pueden ser:

- ✓ Tecnológicos
- ✓ No tecnológicos

3.4.2.1. Tecnológicas.

La ayuda tecnológica para realizar control y obtener seguridad en la infraestructura de la red con el fin de reducir riegos, se obtiene de las herramientas informáticas implementadas por la Corporación Nacional de Telecomunicaciones, para llevar registros de cualquier incidente.

Las aplicaciones permitirán llevar un control minucioso de todos los eventos sucedidos en la red, tanto de usuarios internos como usuarios con intenciones maliciosas en contra de la red.

La arquitectura tecnología orientada a controlar o resolver todos estos, está basada en la implantación de una política de acceso a la red y que recursos se pueden utilizar por esos usuarios.

Estos controles básicamente se enfocan en 3 aspectos que son:

- ✓ Control de sistemas de aplicaciones
- ✓ Control de sistemas de redes
- ✓ Control de sistema de administración o gestión

3.4.2.2. No tecnológicas.

Para poder gestionar de mejor manera una arquitectura tecnológica puntual implementada dentro de la plataforma de tecnologías de la Corporación Nacional de Telecomunicaciones y de su departamento de IP_MPLS para reducir riesgos, es imprescindible llevar un control meticuloso y ordenado acerca de su funcionamiento y operación.

Estos controles conllevan aspectos como:

- ✓ Control de instrucciones
- ✓ Control de cambios
- ✓ Control de cumplimiento
- ✓ Control de la continuidad

3.5. PRUEBAS, MANTENIMIENTO, APLICACIÓN Y SOLUCIÓN. GARANTÍA EN LA PRONTA RECUPERACIÓN DE LAS OPERACIONES.

Se debería desplegar y conservar una carrera de gestión en cuanto a la continuidad del negocio y a la provisión de los servicios en la CNT, ésta deberá tratar las exigencias de seguridad de la infraestructura e información necesarias para la continuidad de operaciones normales.

La pronta identificación de los eventos o incidentes que tienen la potencialidad de originar interrupciones a los procesos de negocio es una precaución y una garantía del rápido restablecimiento de las operaciones normales del área afectada.

Frente a cualquier incidente o amenaza de paralización de servicios prestados por la CNT mediante su departamento de IP_MPLS, es preciso el registro de todo cambio, acción, reorganización,

procedimiento, proceso o plan de mejora implementado, que deberá garantizar una recuperación de las acciones y/o servicios dentro del departamento de IP_MPLS de la CNT.

Estos registros deben ser controlados y poseer un formato de cada uno de ellos, por lo tanto el compromiso está sobre la dirección del área, en colocar los trámites necesarios a fin de disponer de una ajustada gestión de los incidentes de seguridad, infraestructura y de la información, con la ayuda de la nominación de un equipo responsable por la gestión de incidentes de seguridad del área de IP_MPLS.

En la siguiente tabla se menciona varios aspectos que ayudaran a mejorar los procedimientos y garantizar una pronta recuperación de las operaciones y de sus servicios.

Tabla 6.
Acciones y resultados del área de IP_MPLS.

ACCIONES DEL ÁREA IP_MPLS	**RESULTADOS PARA LA CNT.**
✓ Adiestramiento y profesionalización adecuada o apropiada.	✓ Adiestramiento orientado a Objetivos de Corto y largo Plazo. ✓ Alto rendimiento laboral. ✓ Buen desempeño en el cargo. ✓ Óptima utilización de recursos físico, tecnológico y humano.
✓ Estándares consistentes	✓ Actuación y desempeño consistente por parte del trabajador.

	✓ La calidad de su labor es confiable.
✓ Control existente de la documentación sobre métodos de trabajos y procedimientos operativos y dirección en el cargo.	✓ Capacidad para producir servicios de calidad de manera consistente. ✓ Alto rendimiento operativo de equipamiento y personal. ✓ Minimización de accidentes laborales. ✓ Desempeño del cargo definido. ✓ Orientación única en las metas. ✓ Motivación constante. ✓ Supervisores con facilidad en lograr los objetivos.
✓ Focalización en la cantidad y en la calidad.	✓ El trabajo se orienta en cumplir con las labores con el fin de satisfacer a las necesidades de los clientes. ✓ Los trabajadores se enfocan en obtener mejores resultados cubriendo sus asignaciones laborales.
✓ Equipamiento actualizado y en buen estado.	✓ Calidad consistente. ✓ Minimización de accidentes laborales. ✓ Reducción en los costos de los servicios para los clientes. ✓ Aumento de la producción y productividad de los servicios provistos por la CNT.

✓ Confianza y entrega en la CNT y su área de IP_MPLS.	✓ Mejora la comunicación. ✓ Aumento de la capacidad para solucionar problemas. ✓ Habilidad para identificar y resolver los verdaderos problemas. ✓ Motivación en la creatividad y la innovación.
✓ Mejora continua en la inspección y/o calibración de instrumentos.	✓ Resultados y productos consistentes
✓ Factores generales	✓ Edificaciones eficientes ✓ Orden ✓ Aseo

Por lo tanto, si la capacidad para actuar rápidamente ante una interrupción de la provisión de servicios, mediante el establecimiento de un plan que restablecerá y recuperará funciones críticas de la organización, se puede garantizar una pronta recuperación de las operaciones.

El aseguramiento de la normalización de las operaciones en el área de IP_MPLS, está dada esencialmente por 2 componentes:

- ✓ **Personal**

  El personal del departamento de IP_MPLS se adapta a la tecnología y a la estructura por medio de adiestramiento, aprendizaje y cambio organizacional planeado o controlado, cediendo a que la técnica opere y se desarrolle obteniendo un mayor provecho y beneficio de sus aplicaciones.

- ✓ **Tecnología.**

  La tecnología empleada se ajusta para afirmar o habilitar salidas estructurales valiosamente importantes que en su conjunto trabajan frente a la solución de incidentes, hablamos de software, hardware y las comunicaciones disponibles en la CNT.

Así, la Identificación inmediata de los incidentes o amenazas procede eligiendo una sistemática o herramienta ajustada para realizar un Análisis de Impacto sobre el Negocio y las actividades.

CAPÍTULO IV

4. DISEÑO DEL PLAN DE CONTINUIDAD DE NEGOCIO PARA LA CNT E.P. Y SU DEPARTAMENTO IP_MPLS.

Dentro de este documento se pone en manifiesto el Plan de Continuidad de Negocio para la CNT y su Departamento de IP_MPLS, considerando la falta de gestión en varios aspectos que, en el siguiente listado se encuentran detallados como posibles hechos de paralización en las operaciones y riesgos que pudieran presentarse debido a éstas, pero sobre todo el conseguir lineamientos en base a logro de objetivos y beneficios operativos.

- ✓ Estricto respeto de las políticas de seguridad.
- ✓ Organización de la seguridad de la información.
- ✓ Manejo de los activos de la información, comunicaciones y operaciones.
- ✓ Seguridad de los recursos humanos.
- ✓ Seguridad de locales y control de accesos.
- ✓ Lineamientos de gestión de continuidad de negocio y operaciones.
- ✓ Cumplimiento de objetivos y metas.

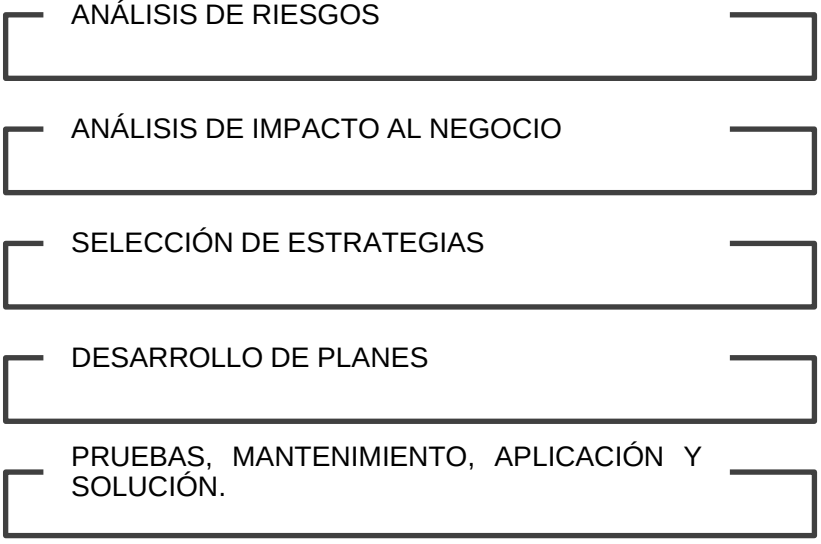
Este conjunto de prácticas elementales descritas en este Plan de Continuidad, no es de ninguna manera, una metodología o inventiva, tampoco un detalle de paso a paso para su establecimiento obligatorio, el afán de este proyecto es proveer una guía general ya que será de adaptación, seguimiento y actualización continua según las necesidades inmediatas del departamento de IP_MPLS de la CNT, ya que no se hace énfasis en ninguna de las plataformas tecnológicas utilizadas.

En capítulos anteriores de este trabajo, se ha mencionado la necesidad de identificar y analizar los diferentes factores de riesgo, amenazas e

incidentes que eventualmente podrán afectar a las actividades, procesos y servicios provistos por el área de IP_MPLS en la CNT, para tener una estimación de riesgo lo que se supone puede fallar y a continuación las consecuencias que resultarán para la institución.

Con la lista de los procesos críticos se asegura la información específica de los procesos en función de la tecnología, entonces podemos decir que, si la tecnología no origina su ocupación también se convierte en un riesgo o una amenaza latente.
En el diseño de continuidad de negocio lo más importante es la cultura organizativa, la visión con la que el personal involucrado manifiesta su desenvolvimiento para la utilización de las herramientas disponibles y el desarrollo de nuevos servicios a sus clientes y usuarios.

Se considerará la probabilidad de que suceda cada uno de las posibles amenazas, para poder priorizar sus consecuencias potenciales, desarrollando un plan para contrarrestarlas tomando en cuenta las siguientes fases:



4.1. ANÁLISIS DE RIESGOS.

La relación tácita que consta entre amenaza, incidente e impacto, es la condición principal a tomar en cuenta el instante de la validación de acciones de seguridad para la preservación y corrección de los activos que se desean salvaguardar y deben ser siempre estimados cuando se realiza un Análisis de Riesgo.

El riesgo se hace presente cuando las amenazas y las vulnerabilidades están latentes y atentan contra los activos que son los que tienen un valor adicional y que a la vez, requieren de seguridad para mantenerse a buen recaudo.

Para realizar una identificación de los diferentes y variados factores de riesgo, incidente o amenaza que eventualmente pueden afectar a la infraestructura lógica, tecnológica y humana que conforman el área de IP_MPLS, se deberá suponer lo que tiene mayor posibilidad de tener un mal funcionamiento o estar con mucha mayor posibilidad de falla dentro de la misma, esto permitirá estimar las consecuencias directas e inmediatas sobre los servicios que provee la CNT.

Figura 20.

Riesgo sobre los Activos

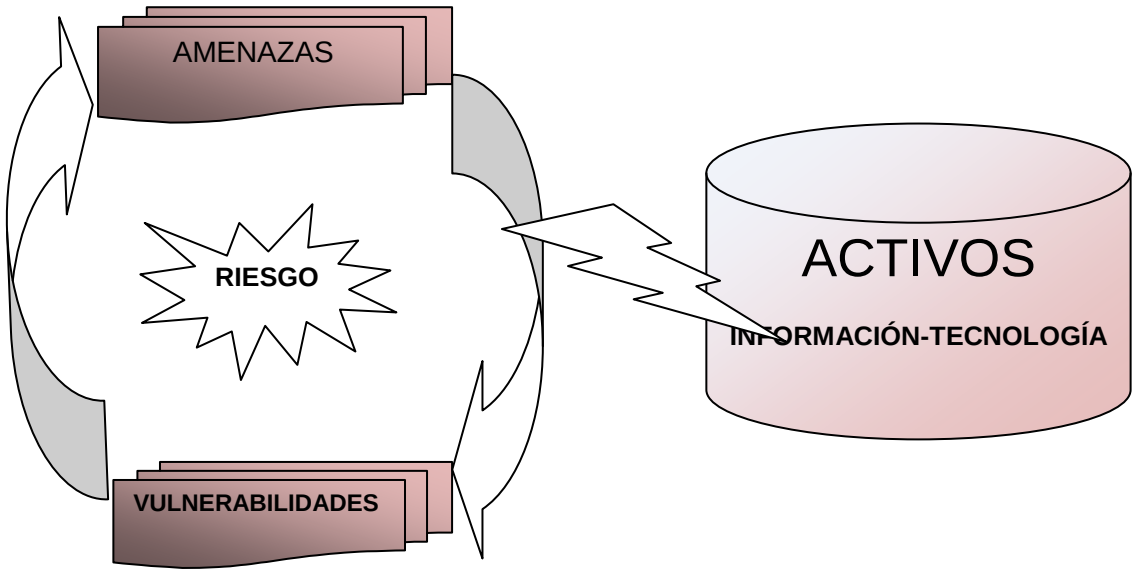


Tabla 7.
Tabla de análisis de riesgos.

Áreas comprometidas	Id Riesgo	Impacto esperado	Probabilidad de fallas	Área de acción	Prioridades	Estrategias
Todas las Oficinas	Perdida de información	3	2	Total	Respaldo de información	Formación de equipos de trabajo
Departamento Técnico	Fallas en servidores	3	2	Equipamientos	Respaldo de servicios y servidores	Manejo de equipos comprometidos
Actividades de Nivel 1	Fallas de los servicios de RED	3	1	Servicios de RED	Levantamiento de servicios de red	Movilidad de red
Actividades de nivel 2	Fallas de los servicios de RED	3	3	Servicios de RED	Levantamiento de servicios de red	Redundancia de red
Actividades de nivel 3	Fallas de los servicios de RED	2	3	Servicios de RED	Levantamiento de servicios de red	Movilidad de red
Backbone ATM	Fallos en gestión	4	2	GESTION IP_MPLS	Recuperación de la comunicación de Gestión ATM	Conocimientos de Backbone ATM

4.1.1. IDENTIFICACIÓN DE ACTIVOS.

La alineación del entorno que rodea a los activos y la tecnología garantiza una continuidad de sus operaciones, una vista técnica del entorno en donde se despliegan y desarrollan los procesos.

La identificación de activos, deja en relieve la correcta provisión de servicios del departamento de IP_MPLS y muestra consideraciones propias para cada uno de ellos, así:

Tabla 8. .

Identificación de riesgos en el área de IP_MPLS sobre sus activos.

Activos	**CAUSA DE** **Riesgo – Amenaza – Incidente**
✓ Sistemas (software, hardware)	✓ Inapropiado ajuste de las políticas de seguridad a las requeridas en la CNT y su departamento de IP_MPLS. ✓ Delitos informáticos provocados por hackers. ✓ Introducción de virus, malware y código malicioso. ✓ Distribución premeditada o accidental de información. ✓ Fallos en sistemas de información. ✓ Accesos no autorizados. ✓ Mal uso de los servicios informáticos que requieren autenticación.

	✓ Intentos recurrentes de acceso. ✓ Intentos no recurrentes de acceso. ✓ Fallos en sistemas de comunicaciones. ✓ Actualizaciones y desactualización de elementos activos. ✓ Packet sniffers. ✓ Man in the middle.
✓ Infraestructura funcional de las Redes	✓ Incidentes suministro eléctrico. ✓ Fallo en cableado eléctrico. ✓ Terminales defectuosas. ✓ Instalación de equipamiento en paredes viejas o húmedas.
✓ Estaciones de trabajo (personal)	✓ Perdida de información. ✓ Robo de información. ✓ Venta de información. ✓ Borrado de información. ✓ Destrucción de información. ✓ Manipulación y modificación de información. ✓ Interrupción de los servicios de red. ✓ El añadir o eliminar una estación de trabajo en la red.
✓ Servidores	✓ Caídas de operación de los sistemas. ✓ Fallos en los sistemas de

	información. ✓ Falta de conexión con bases de datos. ✓ Falta de respaldos.
✓ Equipos de conectividad	✓ Equipamiento con desperfectos de fabricación. ✓ Falta de mantenimiento. ✓ Equipos que no cumplen con requerimientos establecidos. ✓ Falta de configuración. ✓ Capacidad de equipamiento ✓ subutilizada. ✓ Servicios de red (páginas o anuncios web). ✓ Correo electrónico. ✓ Telefonía interna y externa.
✓ Enlaces, transporte de información.	✓ Enlaces entre estaciones mal distribuidas. ✓ Vandalismo, terrorismo, sabotaje, robo, daños premeditados. ✓ Desastres naturales a los que está expuesta la red. ✓ Exposición de enlaces a posibles ataques.
✓ Bases de datos	✓ Actualizaciones. ✓ Respaldos. ✓ Modificaciones. ✓ SQL injection. ✓ Key loggers.

	✓ Hacking Wireless. ✓ Rootkits. ✓ Buffer overflow. ✓ Exploits. ✓ DoS / DdoS. ✓ Conexiones de usuarios cerradas de manera errónea. ✓ Desconocimiento de los procedimientos.
✓ Aplicaciones y técnicas de software	✓ Error u Omisión del empleo de las técnicas y políticas de seguridad. ✓ Desactualización de software. ✓ Falta de registros y controles. ✓ Alarmas. ✓ Tecnologías de información mal utilizadas.
✓ Espacio e infraestructura física	✓ Humedad. ✓ Disposición incorrecta del cableado. ✓ Mala organización física del entorno. ✓ Falta de orden y aseo. ✓ Instalaciones de agua defectuosa o vieja. ✓ Instalación de equipamiento. ✓ Sistemas de aire acondicionado con daños o mal funcionamiento. ✓ Temblores, terremotos, erupciones volcánicas, inundaciones, tsunamis,

	inundaciones, derrumbes. ✓ Guerras, revoluciones civiles, militares o policiales. ✓ Terrorismo, sabotaje, vandalismo. ✓ Robo de infraestructura, ✓ Huelgas, paralizaciones, bloqueo de carreteras.
✓ Personal	✓ Incidentes por ingerir alimentos en el lugar de trabajo ✓ Derrame de líquidos o sustancias por personal de limpieza sobre equipamiento tecnológico. ✓ Desactualización del personal ✓ Falta de controles de seguridad ✓ Falta de Concientización en seguridad ✓ Amenaza de bomba.

4.1.2. TIEMPOS DE RECUPERACIÓN DE SERVICIO.

Con la identificación de los procesos críticos, se conocerá los tiempos de recuperación necesarios para devolver la continuidad de las operaciones al departamento de IP_MPLS de la CNT, según el ente regulador MINTEL (Ministerio de Telecomunicaciones).

Tabla 9.

Procesos críticos en el área de IP_MPLS.

Procesos/Servicios - críticos	**Tiempos de recuperación y prioridad 24/7.**
Telefonía fija /Cu	Hasta 48 h
Telefonía fija /Wimax	Hasta 48 h
Internet fijo /Cu	Hasta 24 H
Internet fijo /Wimax	Hasta 24 H
ISPs	7 horas
Enlaces dedicados Cu	4 horas
Enlaces dedicados FO	4 horas
Enlaces dedicados Radio Enlaces	7 horas

4.1.3. VALORACIÓN DE EFECTIVIDAD EN LAS DISPOSICIONES DE CONTROL.

Con la identificación de los procesos críticos, se conocerán las medidas de control para la recuperación de los servicios, por ende devolver la continuidad de las operaciones al departamento de IP_MPLS.

Cada una de estas medidas deberá tener asignado un valor de efectividad ante cada incidente. Lo que permitirá un mejor registro de la severidad de cada amenaza a la infraestructura física y lógica del departamento.

Tabla 10.

Valoración de las medidas de control.

MEDIDAS DE CONTROL	RESPUESTA EFECTIVIDAD
NINGUNO. No se ha tomado ninguna medida de control, o no amerita.	**1**
BAJO. Medidas de control de nivel bajo.	**2**
MEDIO. Las medidas tomadas han sido suficientes.	**3**
ALTO. Se tomaran medidas de control estrictas.	**4**
DESTACADO. Se han tomado todas las medias de control.	**5**

4.1.4. ESTRATEGIAS DE CONTROL.

Cada estrategia de control utilizada para mitigar un incidente, hará que el alcance del mismo sea reducido según la efectividad que posee, resultando positivo el registro de cada acción tomada.

Tabla 11.

Valoración de las Estrategias de control en el área de IP_MPLS.

ESTRATEGIAS DE CONTROL	**Respuesta – Efectividad**
Formación de equipos de trabajo	3
Conocimientos del área IP_MPLS	3
Manejo de equipos	1
Recursos disponibles	2
Personal capacitado	5
Entrenamiento continuo	5
Políticas de control	2
Implementación de virtual data center	3
Movilidad en la red	2
Nueva configuración de comunicaciones generales	4
Implementación de nuevos centros de gestión	5
Estudio técnico de seguridad	4
Clasificación priorizando activos	3
Políticas de seguridad	3
Cursos de entrenamiento.	2

Actualización y capacitación	
Informes técnicos periódicos	1
Realización de pruebas	3
Respaldos tecnológicos.	4
Seguimiento de los resultados	3
Registro y responsabilidad de cambios	4

Se han resumido con cada cuadro, la tecnología y activos que deben ser resguardados, con el objetivo de brindar la oportunidad de recibir retroalimentación que permite conocer a mayor profundidad los posibles riesgos a que se someten los usuarios en sus actividades diarias, dimensionando la fuerza del trabajo para la realización del análisis de riegos.

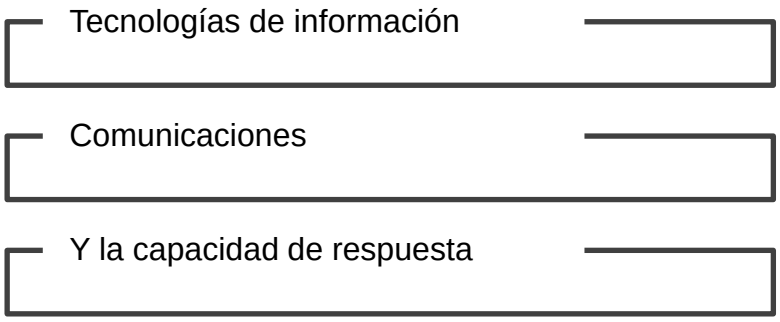
Se ha puesto de manifiesto la capacidad de realizar un análisis de riesgo a los productos y servicios ofrecidos y gestionados por el departamento de IP_MPLS, sus procesos de mayor relevancia y que activos se ven más afectados ante un ataque afirmando que los equipos están totalmente seguros para transmitir la información y/o proveer el servicio.

Se considerará que:

Los recursos consumibles son baratos y fáciles de reponer, el hardware tiene un gran valor económico y de inversión, pero fácil de reemplazar, el software, representa una gran inversión y también es fácil de reponer, sin embargo, los datos y la información son definitivamente el activo más importante en el área de IP_MPLS y la CNT, ya que los procesos

de negocio y servicio no deben discontinuarse por más de un corto tiempo.

La infraestructura necesaria para apoyar los procesos críticos ante incidentes del plan de continuidad de negocio se verá apoyada en tres pilares que son:



4.2. ANÁLISIS DE IMPACTO AL NEGOCIO.

Para conocer el impacto que puede tener una amenaza, un riesgo o un incidente dentro del departamento de IP_MPLS, una excelente estrategia será el asignar un valor numérico a una eventualidad, lo cual permitirá que ésta, deje de ser tan abstracta ante el análisis, brindando la posibilidad de manejar de mejor manera un rango de prioridad para cada uno de los riegos que se han identificado.

Con el conocimiento previo de ésta valoración a la información, se podrá incluir una adecuada repartición o asignar los recursos necesarios para una rápida solución ante una amenaza.

La realización de una matriz de valorización del riesgo, es la herramienta que clarificará la información que se tabulará en la tabla de calidad de la gestión para la obtención del Riesgo Residual, permitiendo determinar las prioridades

4.2.1. RIESGO RESIDUAL (RR).

Para el departamento de IP_MPLS, el riesgo remanente o residual, es el que se determina solamente después de que se han tomado todas las medidas de seguridad para contrarrestar los efectos negativos que pudiera causar.

Sin embargo, la ISO 27005 deja claro que este riesgo residual no se refiere al riesgo efectivo después de la aplicación y toma de medidas, sino al riesgo teórico que es calculado durante el análisis de riesgos en la fase de Planeamiento.

El alineamiento del SGSI (*Sistema de Gestión de Seguridad de la Información*) con el Proceso de Gestión de Riesgo, se verá plasmado en el análisis del riesgo residual después de la valoración entre la probabilidad de ocurrencia de una amenaza y la consecuencia o impacto que pudiera tener en el departamento de IP_MPLS.

Tabla 12.

Matriz de Valoración de Riesgo - Amenaza - Incidente.

NIVEL/VALORACIÓN DE RIESGO - AMENAZA – INCIDENTE					
PROBABILIDAD	**3**	**ALTO**	4	5	5
	2	**MEDIO**	2	3	5
	1	**BAJO**	1	2	4
			BAJO	**MEDIO**	**ALTO**
			1	**2**	**3**
Vs.			**IMPACTO – CONSECUENCIA**		

Una vez que es conocido el valor cuantitativo del riesgo analizado por la matriz de riesgos, el siguiente paso es obtener el RR (*Riesgo Residual*), la valoración se obtiene mediante el cálculo en la tabla, entre el cruce de la probabilidad de ocurrencia y el impacto que pudiera tener una amenaza, permitirá conocer el nivel de riesgo que arroja tres resultados posibles, como indica el cuadro siguiente:

Tabla 13.

Valoración del Riesgo Residual.

RR = 1	La amenaza, riesgo o eventualidad, ha sido Controlada.
RR > 1	Indica que las medidas tomadas aun no tienen el efecto esperado por lo tanto está latente un mayor riesgo de ocurrencia.
RR < 1	Se han tomado las medidas apropiadas y las eventualidades están bajo control.

4.2.2. CATEGORIZACIÓN DE RIESGO.

En el siguiente cuadro se presenta cada uno de los riesgos evaluados según su probabilidad de ocurrencia el impacto sobre las actividades del departamento de IP_MPLS, asignando un valor apreciable, con el objetivo de hacer tangible numéricamente para una mejor comprensión.

Tabla 14.

Valoración de Riesgo - Nivel de Riesgo.

RIESGOS Y PROCESOS CRÍTICOS DE RECUPERACIÓN	VALORIZACIÓN DEL RIESGO		
	PROBABILIDAD	IMPACTO-CONSECUENCIA	**NIVEL DE RIESGO**
	3 ALTO	3 ALTO	**5 Alto**
	1 BAJO	1 BAJO	**1 Bajo**

1	Políticas de seguridad ajustadas de manera desacertada a las requeridas en la CNT y su departamento de IP_MPLS.	2	3	**5**
2	Introducción de virus, malware y código malicioso	3	2	**5**
3	Fallos en sistemas de información	1	2	**2**
4	Mal uso de los servicios informáticos que requieren autenticación	2	2	**3**
5	Intentos no recurrentes de acceso	1	2	**2**
6	Actualizaciones y desactualización de elementos activos.	1	3	**4**
7	Man in the middle	1	3	**4**
8	Delitos informáticos hackers	1	3	**4**

9	Distribución premeditada o accidental de información	3	2	**5**
10	Accesos no autorizados	1	1	**1**
11	Intentos recurrentes de acceso	1	2	**2**
12	Fallos en sistemas de comunicaciones	1	1	**1**
13	Packet sniffers	1	1	**1**
14	FIREWALL	2	1	**2**

15	Incidentes suministro eléctrico	1	1	**1**
16	Fallo en cableado eléctrico	1	1	**1**
17	Instalación de equipamiento en paredes viejas o húmedas.	1	1	**1**

18	Perdida de información	3	2	**5**
19	Venta de información	2	3	**5**
20	Destrucción de información	1	1	**1**
21	Interrupción de los servicios de red	1	1	**3**
22	Robo de información	1	3	**4**
23	Borrado de información	1	3	**4**
24	Manipulación y modificación de	1	2	**2**

	información.			
25	El añadir o eliminar una estación de trabajo a la red.	1	2	**2**

20	Caídas de operación de los sistemas	1	2	**2**
21	Fallos en los sistemas de información	2	1	**2**
22	Falta de respaldos	1	3	**4**

22	Equipamiento con desperfectos de fabricación	1	1	**1**
23	Falta de mantenimientos	1	1	**1**
24	Equipos que no cumplen con requerimientos establecidos	1	1	**1**
25	Falta de configuración	1	2	**2**
26	Capacidad de equipamiento subutilizada.	1	1	**1**
27	Servicios de red (páginas o anuncios web).	1	1	**1**
28	Correo electrónico	1	1	**1**
29	Telefonía interna y externa.	1	1	**1**

30	Enlaces entre estaciones mal distribuidos	1	2	**2**
31	Vandalismo, terrorismo, sabotaje, robo, daños premeditados.	1	2	**2**
32	Desastres naturales a los que está expuesta la red.	1	1	**1**
33	Exposición de enlaces a posibles ataques	1	2	**2**

33	Actualizaciones.	1	2	**2**
34	Respaldos	1	2	**2**
35	Modificaciones	2	2	**3**
36	SQL injection	1	1	**1**
37	Key loggers	1	1	**1**
38	Hacking Wireless	2	1	**2**
39	Rootkits	1	1	**1**
40	Buffer overflow	1	1	**1**
41	Exploits	1	1	**1**
42	DoS / DDoS	1	1	**1**
43	Conexiones de usuarios cerradas de manera errónea.	2	2	**3**
44	Desconocimiento de procedimientos.	1	1	**1**

45	Error u Omisión del empleo de las técnicas y políticas de	1	2	**2**

	seguridad.			
46	Desactualización de software	1	1	**1**
47	Falta de registros y controles.	2	2	**4**
48	Alarmas	1	2	**2**
49	Tecnologías de información	1	2	**2**

50	Humedad	1	1	**1**
51	Disposición incorrecta del cableado	2	1	**2**
52	Mala organización física del entorno	1	1	**1**
53	Falta de Orden y aseo	1	1	**1**
54	Instalaciones de agua defectuosas o viejas	1	1	**1**
55	Instalación de equipamiento	1	1	**1**
56	Sistemas de aire acondicionado con daños o mal funcionamiento.	1	2	**2**
57	Temblores, terremotos, erupciones volcánicas, inundaciones, tsunamis, inundaciones, derrumbes.	1	1	**1**
58	Guerras, revoluciones civiles, militares o	1	2	**2**

	policiales.			
59	Terrorismo, sabotaje, vandalismo.	1	2	**2**
60	Robo de infraestructura,	2	2	**3**
61	Huelgas, paralizaciones, bloqueo de carreteras.	1	1	**1**

61	Incidentes por ingerir alimentos en el lugar de trabajo	3	1	**4**
62	Derrame de líquidos o sustancias por personal de limpieza sobre equipamiento tecnológico.	3	3	**5**
63	Desactualización del personal	1	2	**2**
64	Falta de controles de seguridad	1	2	**2**
65	Falta de Concientización en seguridad	2	2	**3**
66	Amenaza de bomba	1	1	**1**

El formato estándar de reporte de riesgos, amenazas o incidentes ocurridos en el departamento de IP_MPLS, estará compuesto por:

- ✓ Un reporte inicial de incidentes.
- ✓ Reporte de monitoreo.

- ✓ Modo de reporte a nivel gerencial.
- ✓ Evaluación de incidentes.

Tabla 15.

Reporte Inicial de Incidentes.

DEPARTAMENTO IP_MPLS		
REPORTE INICIAL DE INCIDENTES		
# Reporte.		
Localización del Incidente:		
Hora del incidente:		
Fecha del incidente:		
Responsable a cargo:		
Área:		
Hora de notificación del incidente:		
Fecha de notificación del incidente:		
Sección afectada:		
Tipo de incidente:		
Causas del Incidente:		
Existen clientes Afectados	SI	NO
Equipos/dispositivos afectados	SI	NO
Existe grupo de trabajo	SI	NO
Grupo de trabajo completo	SI	NO
Causa de paralización de servicios	SI	NO
Facilidad de traslado	SI	NO
Resultados		

Observaciones	

Tabla 16.

Monitoreo de Incidentes.

DEPARTAMENTO IP_MPLS		
MONITOREO DE INCIDENTES		
Tipo de incidente:		
Pormenores del incidente:		
Detalles de acciones	Inicio	Fin
Fecha de incidente:		
Hora de incidente:		
Responsable:		
Cargo:		
Área.		
Detalle de las actividades de control realizadas.		
RESULTADOS		

OBSERVACIONES	

Tabla 17.

Modo de Reporte a Nivel Gerencial.

DEPARTAMENTO IP_MPLS		
MODO DE REPORTE A NIVEL GERENCIAL		
Tipo de incidente:		
Pormenores de las acciones tomadas.		
Detalles de acciones	Inicio	Fin
Fecha de incidente:		
Hora de incidente:		
Responsable:		
Cargo:		
Área.		
Designación gerencial de requerimientos para atender incidentes.		

Recurso humano designado de gerencia	
Gerente responsable.	
Recomendaciones	

Tabla 18.

Evaluación de Incidentes.

DEPARTAMENTO IP_MPLS			
EVALUACIÓN DE INCIDENTES			
Lugar del incidente			
Fecha de incidente:		Hora	
Determinación de causas del incidente.			
Incidentes naturales			
Accidentes operacionales			
Incidentes externos.			
Incidentes de seguridad			
Incidentes de infraestructura			
Incidentes tecnológicos			
Proceso de comunicación de incidentes.			
Responsable			
Medios utilizados			
Eficacia de comunicación			
Detalles adicionales			
Resultados de acción			

Detalle de la aplicación de los controles.	
Observación de procedimientos aplicados.	
Cumplimiento de los procedimientos.	
Cumplimiento de los grupos de trabajo.	
Áreas afectadas	
Sistemas de comunicaciones	
Infraestructura física afectada	
Plataforma (AMG-WIMAX-IP-METRO-AAA BRAS-BACKBONE-ATM)	
Alcance del impacto	
Origen y causas	
Personal inmerso en el incidente	
Equipamiento utilizado	

Acciones de control empleadas	
Otros	
Avance de la contingencia	
Comunicaciones realizadas	
Secciones afectadas	
Soporte adicional	
Riesgos adicionales	
Observaciones	
Responsables	
Cargo	

ANÁLISIS DE IMPACTO AL NEGOCIO
OBTENCIÓN DEL RIESGO RESIDUAL Y % DE RIESGO

Tabla 19.

Riesgo Residual - Porcentaje de probabilidad de ocurrencia de una amenaza.

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Políticas de seguridad ajustadas de manera desacertada a las requeridas en la CNT y su departamento de IP_MPLS.	5	Revisiones periódicas de las políticas implantadas.	4	**2,67**	**1,88**	37,50%
		Elaboración de reglas y procedimientos para cada servicio del área.	3			
		Documentación, registro, sensibilización de los operadores ligados a su control y la seguridad de los sistemas.	1			
Introducción de virus, malware y código malicioso	5	Antivirus actualizado	3	**3,67**	**1,36**	27,27%
		Concientización de los usuarios	5			
		Firewall	3			
Fallos en sistemas de información	2	Actualización, mantenimiento, disponibilidad.	3	**2,67**	**0,75**	15,00%
		Software de control	2			
		Formación adecuada de usuarios	3			

Mal uso de los servicios informáticos que requieren autenticación	3	Capacitación para superar la resistencia a cambios.	4	**3,67**	**0,82**	16,36%
		Organización y división de departamentos y áreas.	3			
		Procedimientos informáticos alternos.	4			
Intentos no recurrentes de acceso	2	Mejoramiento en políticas de Accesos y control de usuarios.	5	**4,33**	**0,46**	9,23%
		Implementación de claves seguras	5			
		Firewall, antivirus actualizados.	3			
Actualizaciones y desactualización de elementos activos.	4	Control y registros actuales de actualizaciones de activos.	4	**4,00**	**1,00**	20,00%
		Programación y planificación de controles a los activos.	5			
		Respaldos de información, configuraciones e inventarios de equipos y dispositivos fuera del lugar donde se hallan actualmente instalados.	3			
Man in the middle	4	Mejor encriptación de señal.	5	**3,67**	**1,09**	21,82%
		Implementación de Claves seguras	3			
		Control de accesos a nuevos usuarios.	3			
Delitos informáticos hackers	4	Firewall	2	**3,00**	**1,33**	26,67%
		Mejoramiento de restricciones de accesos a la red.	3			

		Control y registro de usuarios que ingresan a la red.	4			
Distribución premeditada o accidental de información	5	Registro en el manejo de información.	2	**3,00**	**1,67**	33,33%
		Concientización a usuarios en el manejo de información	3			
		clasificación de la Información	4			
Accesos no autorizados	1	Control de accesos	2	**3,00**	**0,33**	6,67%
		Registro de accesos	3			
		Restricciones a la manipulación de información y equipos	4			
Intentos recurrentes de acceso	2	Mejoramiento en políticas de Accesos y control de usuarios.	2	**3,00**	**0,67**	13,33%
		Implementación de claves seguras	3			
		Firewall, antivirus actualizados.	4			
Fallos en sistemas de comunicaciones	1	Mantenimiento periódico	2	**3,00**	**0,33**	6,67%
		Estudio de posibles actualizaciones en equipos con varios años de utilización.	3			
		Implementación de un soporte redundante en el sistema que permita disponibilidad.	4			
Packet sniffers	1	Concientización a usuarios en la utilización de Packet Sniffers.	2	**3,00**	**0,33**	6,67%
		Mejoramiento de políticas de seguridad.	3			

		Uso programado y registro de herramientas de control sobre eventos en la infraestructura de red.	4			
FIREWALL	2	Control interno en la utilización de programas, manejo y descarga de archivos ajenos a la red.	2	**3,60**	**0,56**	11,11%
		Implementación de Antivirus.	3			
		una adecuada administración con la creación de VPNs	5			
		control y gestión del ancho de banda para los usuarios	4			
		tomar como referencia periodos de tiempo cortos para la actualización de firewall	4			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Incidentes suministro eléctrico	1	Implementación sistemas de respaldos de energía alterna.	5	**5,00**	**0,20**	4,00%
		revisiones periódicas de instalaciones eléctricas	5			
		Implementación de sistemas de alarmas.	5			

Fallo en cableado eléctrico	1	revisiones periódicas de instalaciones eléctricas	5	**4,67**	**0,21**	4,29%
		Aumentos de puntos eléctricos que eviten sobrecargas.	5			
		Cambios de mantenimiento en cableado con varios años de uso.	4			
Instalación de equipamiento en paredes viejas o húmedas.	1	Trabajos de mejoramiento de infraestructura.	4	**4,00**	**0,25**	5,00%
		Mantenimientos periódicos.	4			
		estudio previo de locales e instalaciones físicas	4			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Perdida de información	5	Respaldos de información	4	**3,67**	**1,36**	27,27%
		restricciones en el manejo de información	3			
		Selección de responsables de manejo de información	4			
Venta de información	5	Respaldos de información	4	**3,00**	**1,67**	33,33%
		restricciones en el manejo de información	2			
		Selección de responsables de manejo de información	3			
Destrucción de	1	Respaldos de información	2	**3,00**	**0,33**	6,67%

información		restricciones en el manejo de información	3			
		concientización en el uso de información	4			
Interrupción de los servicios de red	3	Redundancia en los servicios de red.	4	**3,00**	**1,00**	20,00%
		Plan de recuperación alternos	3			
		Uso apropiado de recursos de red.	2			
Robo de información	4	Respaldos de información	4	**3,33**	**1,20**	24,00%
		restricciones en el manejo de información	3			
		concientización en el uso de información	3			
Borrado de información	4	Respaldos de información	2	**3,00**	**1,33**	26,67%
		restricciones en el manejo de información	3			
		Establecer horarios de actualización y deshecho de información.	4			
Manipulación y modificación de información.	2	Establecer horarios de actualización y deshecho de información.	2	**3,00**	**0,67**	13,33%
		designar responsables de manejo de información	3			
		registro y control de cambios de la información	4			

El añadir o eliminar una estación de trabajo a la red.	2	establecer procedimiento para la creación de nuevos usuarios	4	**3,67**	**0,55**	10,91%
		registro y control de nuevos usuarios	3			
		Actualizaciones periódicas.	4			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Caídas de operación de los sistemas	2	Redundancia	4	**3,33**	**0,60**	12,00%
		concientización de uso y manipulación de equipos	3			
		registros y control de uso	3			
Fallos en los sistemas de información	2	Actualización, mantenimiento, disponibilidad.	4	**3,67**	**0,55**	10,91%
		Software de control	4			
		Formación adecuada de usuarios	3			
Falta de respaldos	4	registro de respaldos	3	**3,00**	**1,33**	26,67%
		revisiones periódicas en los respaldos	3			
		designación de responsables	3			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Equipamiento con desperfectos de fabricación	1	garantías en contratos	4	**4,33**	**0,23**	4,62%
		aseguramiento de equipos	4			
		Sometimiento de pruebas a equipamientos nuevos.	5			
Falta de mantenimientos	1	planes de mantenimiento periódicos	4	**4,00**	**0,25**	5,00%
		designación de responsabilidades	3			
		Subcontratación de servicios de mantenimiento.	5			
Equipos que no cumplen con requerimientos establecidos	1	garantías extendidas	4	**4,00**	**0,25**	5,00%
		seguro de equipos	4			
		pruebas de aceptación	4			
Falta de configuración	2	registros de control	3	**3,67**	**0,55**	10,91%
		establecimientos de horarios y responsables	4			
		Respaldos de configuración de dispositivos y equipos.	4			
Capacidad de equipamiento subutilizada.	1	análisis de creación de nuevos servicios	3	**3,00**	**0,33**	6,67%
		implantación de nuevos servicios	4			
		Pruebas periódicas de la capacidad de quipos.	2			

Servicios de red (páginas o anuncios web).	1	ajuste de políticas de acceso a la red	2	**3,00**	**0,33**	6,67%
		contraseñas seguras	3			
		buen uso de los recursos empresariales de red	4			
Correo electrónico	1	Control en la descarga de archivos proveniente de remitentes de correo externo.	3	**3,33**	**0,30**	6,00%
		ajuste de políticas de uso de correo corporativo	4			
		Concientización de uso de correo como herramienta de trabajo.	3			
Telefonía interna y externa.	1	mantenimiento periódico de centrales	3	**4,00**	**0,25**	5,00%
		implementación de redundancia y/o líneas privas	5			
		Realización de pruebas y cambio periódico de equipos.	4			
Enlaces entre estaciones mal distribuidos	2	Estudio y análisis de capacidad de enlaces.	3	**3,33**	**0,60**	12,00%
		mejoramiento de enlaces entre estaciones con intercambio de información	3			
		Utilización apropiada de enlaces.	4			
Vandalismo, terrorismo, sabotaje, robo, daños premeditados.	2	Propaganda de concientización a ciudadanía.	2	**3,33**	**0,60**	12,00%
		redundancia de infraestructura	3			

		implementación de alarmas	5			
Desastres naturales a los que está expuesta la red.	1	Redundancia	2	**3,20**	**0,31**	6,25%
		construir una red segura	4			
		utilizar sistemas de monitoreo de alarmas	4			
		mantener una red segura	3			
		monitoreo de red frecuente	3			
Exposición de enlaces a posibles ataques	2	Redundancia	3	**3,00**	**0,67**	13,33%
		utilización de medidas de protección a la red	3			
		implementación de alarmas	3			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Actualizaciones.	2	buena práctica de actualizaciones	3	**3,33**	**0,60**	12,00%
		registro de actualizaciones	3			
		elaboración de cronogramas de actualización	4			
Respaldos	2	buena práctica de resoplados	3	**3,33**	**0,60**	12,00%
		registro de resoplados	3			
		elaboración de cronogramas de respaldos	4			
Modificaciones	3	buena práctica de procedimientos en modificación de información	3	**3,33**	**0,90**	18,00%

		control de modificaciones	3			
		establecimiento de cronogramas	4			
SQL injection	1	preparación de procesos de introducción de código	2	**3,00**	**0,33**	6,67%
		controles de introducción de código	3			
		recuperación de procesos de introducción de código	4			
Key loggers	1	implementación de firewall	4	**3,67**	**0,27**	5,45%
		implementación de antivirus	4			
		control de acceso y uso de recursos a usuarios	3			
Hacking Wireless	2	implementación de firewall	4	**3,67**	**0,55**	10,91%
		implementación de antivirus	4			
		control de acceso y uso de recursos a usuarios claves seguras	3			
Rootkits	1	implementación de firewall	4	**4,00**	**0,25**	5,00%
		implementación de antivirus	4			
		control de acceso y uso de recursos a usuarios	4			
Buffer overflow	1	implementación de firewall	4	**4,00**	**0,25**	5,00%
		implementación de antivirus	4			
		control de acceso y uso de recursos a usuarios	4			
Exploits	1	implementación de firewall	4	**4,00**	**0,25**	5,00%
		implementación de antivirus	4			

		control de acceso y uso de recursos a usuarios	4			
DoS / DDoS	1	implementación de firewall	4	**4,00**	**0,25**	5,00%
		implementación de antivirus	4			
		control de acceso y uso de recursos a usuarios	4			
Conexiones de usuarios cerradas de manera errónea.	3	Cultura y concientización de usuarios en el uso de recursos de red.	4	**4,00**	**0,75**	15,00%
		herramientas de software	4			
		establecimiento de horarios y responsables que supervisen a usuarios	4			
Desconocimiento de procedimientos.	1	cursos de capacitación	4	**3,67**	**0,27**	5,45%
		establecimiento de procedimientos apropiados	4			
		Repartición de información a través de intranet.	3			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Error u Omisión del empleo de las técnicas y	2	concientización de personal	3	**3,00**	**0,67**	13,33%
		cursos de capacitación	3			

políticas de seguridad.		designación de responsables con cronogramas de trabajo	3			
Desactualización de software	1	históricos de actualizaciones	3	**4,33**	**0,23**	4,62%
		cronogramas de actualización	5			
		designación de responsables de actualización	5			
Falta de registros y controles.	4	inicio de plan de registro y documentación de controles	4	**4,00**	**1,00**	20,00%
		cronograma de registros y control	4			
		seguimiento y mejora continua de controles y registros establecidos	4			
Alarmas	2	plan de implementación de alarmas sobre infraestructura	4	**3,67**	**0,55**	10,91%
		agilidad en ejecución de plan	3			
		seguimiento y cambios de equipos	4			
Tecnologías de información	2	concientización de la utilización de tecnologías de información	3	**3,67**	**0,55**	10,91%
		capacitación en tecnologías de información	4			
		pruebas y mantenimiento	4			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO

Humedad	1	readecuación de infraestructura física	4	**4,33**	**0,23**	4,62%
		Corrección de problemas en instalaciones de agua.	4			
		Cambio de estación de trabajo.	5			
Disposición incorrecta del cableado	2	construcción de canalización	4	**3,33**	**0,60**	12,00%
		control de acceso y manipulación de equipos e infraestructura	3			
		Contratación de servicios especializados.	3			
Mala organización física del entorno	1	readecuación distributiva de equipos	4	**4,00**	**0,25**	5,00%
		mejoramiento de aéreas	4			
		ampliación de locales y estaciones	4			
Falta de Orden y aseo	1	Cronogramas	3	**3,00**	**0,33**	6,67%
		Empresas	3			
		Experiencia	3			
Instalaciones de agua defectuosas o viejas	1	readecuación de infraestructura física	2	**3,00**	**0,33**	6,67%
		Corrección de problemas en instalaciones de agua.	3			
		cambio de tuberías y obra civil	4			
Instalación de equipamiento	1	normas de seguridad para instalación de dispositivos	2	**3,00**	**0,33**	6,67%
		procedimientos seguros de instalación	3			

		análisis y estudio previo de instalación	4			
Sistemas de aire acondicionado con daños o mal funcionamiento.	2	mantenimiento preventivo periódico	2	**3,00**	**0,67**	13,33%
		realización de cronogramas de mantenimiento	3			
		cambios de equipos con varios años de funcionamiento	4			
Temblores, terremotos, erupciones volcánicas, inundaciones, tsunamis, inundaciones, derrumbes.	1	preparación al personal	3	**2,00**	**0,50**	10,00%
		preparación física de establecimientos	2			
		esperar	1			
Guerras, revoluciones civiles, militares o policiales.	2	preparación al personal	3	**2,33**	**0,86**	17,14%
		preparación física de establecimientos	3			
		esperar	1			
Terrorismo, sabotaje, vandalismo.	2	preparación al personal	3	**3,67**	**0,55**	10,91%
		implementación de alarmas	4			
		conformación de equipos de trabajo especializados	4			
Robo de infraestructura,	3	concientización al personal	3	**3,67**	**0,82**	16,36%
		propaganda dirigida a la ciudadanía para cuidar la infraestructura	3			
		implementación de alarmas	5			
Huelgas, paralizaciones, bloqueo de carreteras.	1	diálogos con dirigentes	2	**3,33**	**0,30**	6,00%
		planes de control	3			

		respaldo de actividades	5			

		calidad de gestión				
Actividad	**nivel de riesgo**	tipo de medida de control	efectividad	**promedio**	**Riesgo Residual**	% de RIESGO
Incidentes por ingerir alimentos en el lugar de trabajo	4	supervisión del personal	3	**3,33**	**1,20**	24,00%
		cultura laboral	3			
		definición de políticas de seguridad	4			
Derrame de líquidos o sustancias por personal de limpieza sobre equipamiento tecnológico.	5	preparación y experiencia del personal	4	**3,67**	**1,36**	27,27%
		señalización de advertencia	3			
		procedimientos de comunicación inmediata en caso de incidentes	4			
Desactualización del personal	2	capacitación periódica	2	**3,00**	**0,67**	13,33%
		programas de evaluación continua	3			
		experiencia en personal	4			
Falta de controles de seguridad	2	creación de controles y planes de información sobre seguridad	4	**3,67**	**0,55**	10,91%
		ajuste de políticas de seguridad	3			
		capacitación en seguridad	4			
Falta de Concientización en seguridad	3	cursos de identificación con la empresa	4	**4,33**	**0,69**	13,85%
		concientización organizacional	4			
		seguimiento y evaluación continua	5			

Amenaza de bomba	1	llamar a los bomberos	5	**4,33**	**0,23**	4,62%
		llamar a la policía	4			
		llamar a la cruz roja	4			

En la tabla 19., se muestra un esquema sencillo para el cálculo u obtención del RR, mediante la aplicación de medidas de control tomadas para cada tipo de incidente, las cuales se obtuvieron con un cruce en la matriz de riesgos. También describe el porcentaje de posibilidad de ocurrencia de una amenaza riesgo o incidentes según el listado obtenido en el análisis.

Tabla 20.

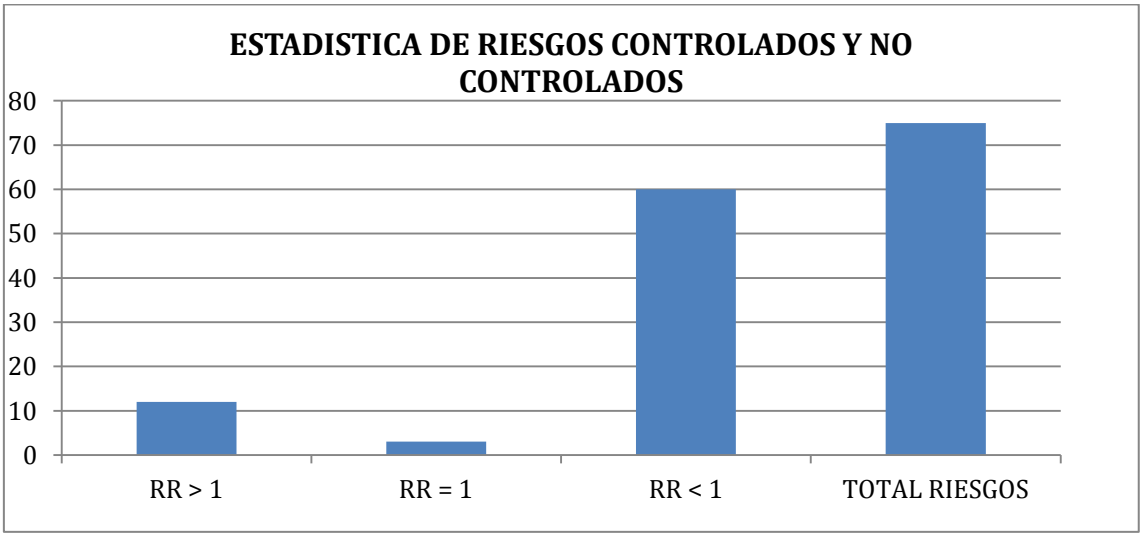
Estadística riesgos.

CONCLUSION ESTADISTICA DE RIESGOS

% RR	PORCIONES	OBSERVACION
RR > 1	12	PROBABILIDAD DE OCURRENCIA
RR = 1	3	RIESGOS CONTROLADOS
RR < 1	60	SE HAN TOMADO LAS MEDIDAS NECESARIAS PARA LOS RIESGOS IDENTIFICADOS.
TOTAL RIESGOS	75	

Tabla 21.

Gráfico estadístico de riesgos.



4.3. SELECCIÓN DE ESTRATEGIAS.

Elaborar un sistema de estrategias significa: la planeación, organización, dirección y control de todas las actividades que

garanticen la probidad de la infraestructura tecnológica, de los recursos, servicios y activos de la Corporación Nacional de Telecomunicaciones.

Los objetivos que se alcanzan ante la implantación de estas normas serán:

- ✓ Constituir un diseño de confianza para el uso y manejo de los activos que se hallan bajo la responsabilidad del área de IP_MPLS, frente a una situación de riesgo.

- ✓ Responsabilidad y compromiso íntegro de todo el personal del área de IP_MPLS, con los procesos de seguridad.

- ✓ La selección de las estrategias deben garantizar que la asistencia del servicio de seguridad domine en disponibilidad, calidad y buen uso.

- ✓ Los empleados sin excepción se cambian a un rol de mediadores del sistema de selección de estrategias

Una vez calculado el RR, valorizado los riesgos, adoptado las medidas de control para cada riesgo, merece la atención y análisis el comportamiento que mitigará el impacto sobre la infraestructura de la red, con la aplicación de medidas correctivas para salvaguardar los activos del departamento de IP_MPLS de la CNT.

La selección de estrategias deberán cumplir con aspectos como:

Tabla 22.

Características Causa - Efecto de las medidas de control.

CAUSA	EFECTO
Experiencia de proyección con hechos concretos y conocidos.	Este conocimiento previo será de vital influencia en su efecto, para futuros acontecimientos.
Controles.	Con el aporte dispuesto que permita concentrar procesos sobre una situación o incidente acontecido.
Riesgo, amenaza, incidente.	Valorizado adecuadamente con la utilización de una matriz, y la posibilidad de ocurrencia de imprevistos o hechos desafortunados que pudieran tener un efecto contrario.
La decisión de elegir.	Un rumbo de acción predeterminado entre varias opciones.
Un planeamiento de decisiones.	Los cuales definirán rumbos y medios para lograr objetivos.
Medidas apropiadas.	Para las decisiones que se adjudican en la determinación o alcance de metas y programas.

Políticas establecidas según requerimientos del área.	Para determinar distintas funciones de riesgo, amenazas o incidentes, en donde se conocen las variantes ante circunstancias ya acontecidas.
El logro de objetivos cuantificados.	Para un mejor acoplamiento de resultados.
Procedimientos detallados a ejecutar.	Para el despliegue de actividades.
Normas y lineamientos.	Que reflejen procedimientos y procesos.
Programas y cronogramas de acciones relacionadas.	Con orden en el tiempo, que controlen y coordinen operaciones.
Implantación y adquisición de nuevas tecnologías.	Pueden parecer costosas en la etapa inicial, pero a largo plazo disminuye mucha inversión subsecuente, especialmente cuando a una aplicación costosa y de baja tecnología es reemplazada por una que mejora procesos y servicios a la CNT.

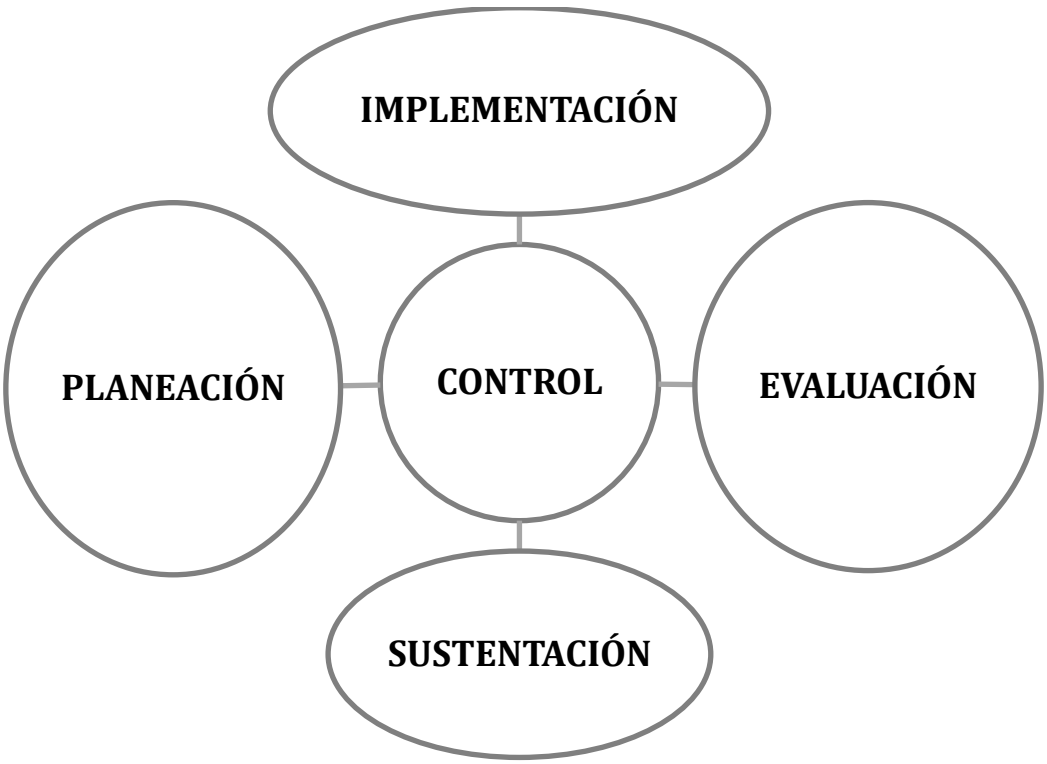
Los aspectos detallados en la Tabla 20, contemplan y alcanzan a los procesos operativos que están relacionados con clientes (servicios de voz, datos, enlaces dedicados, etc.), y los medios empleados, además, los procesos de soporte que facilitan los

recursos a los clientes (factor humano), los recursos específicos que son las herramientas (equipos, instrumentos, materiales, software, hardware, plataformas) y los recursos transversales que para el departamento de IP_MPLS de la CNT es la información.

4.4. PERFECCIONAMIENTO DE PLANES

El desarrollo del plan debe contemplar a cada incidente acontecido dentro del departamento del área de IP_MPLS, en el que se registrará un adecuado procedimiento de detalles que evidencien los procesos dirigidos para su solución, se deberán a los siguientes procesos de análisis.

Figura 21.
Procesos de análisis.



El perfeccionamiento continuo del plan desarrollado, asegura que el acceso a la información, servicios, procesos y recursos que mantienen funcional la infraestructura, se encuentre disponibles ante la ocurrencia de un incidente, atentado o desastre.

El alcance de los servicios resulta fundamental para el almacenamiento y posterior tratamiento de la información, así como, para el normal desarrollo de las actividades y provisión de servicios de la CNT.
Enfocaremos el mejoramiento de planes de las estrategias asumidas por el área de IP_MPLS, con un adecuado proceso que permita:

4.4.1. CONTROL.

El control ante cualquier acontecimiento que atente contra el normal desenvolvimiento de las actividades y provisión de servicios a usuarios de la Corporación Nacional de Telecomunicaciones, incluye, contemplar los elementos claves de seguridad en la entidad.

4.4.2. PLANEACIÓN.

Abarca una apropiada introducción y planificación previa, para que la unidad demuestre los conceptos claves, además de describir el proceso de planificación para los ambientes físicos disponibles y proveedores de servicio en el área de IP_MPLS.

4.4.3. IMPLEMENTACIÓN.

El diseño y la implementación, muestra otro pilar importante e ineludible ante cualquier mejora, proporcionando una guía práctica sobre el delineamiento como una solución para el ambiente físico del departamento de IP_MPLS.

4.4.4. SUSTENTACIÓN.

Esta referido a sostener estos procesos y operaciones, para describir la marcha adecuada y necesaria en el intercambio y la mejora de los procesos internos programados y por programar ante situaciones aun no ocurridas o desconocidas con una probabilidad de ocurrencia significativa.

4.4.5. EVALUACIÓN.

La evaluación periódica proveerá detalles de la infraestructura y de sus componentes con registros antes y después del acontecimiento o suceso, proporcionando pormenores útiles, por ejemplo: sobre el hardware y el software utilizado para obtener soluciones técnicas y administrativas que pudiesen presentar algún tipo de vulnerabilidad.

Algunos aspectos que se deben cubrir y tomar en cuenta para la protección de los activos como la información, la infraestructura física y a los usuarios internos o externos son los siguientes:

- ✓ Un procedimiento único que muestre la capacidad de recuperación de desastres en el área de IP_MPLS de la CNT.
- ✓ Los objetivos de recuperación de las operaciones, procesos y servicios críticos o prioritarios e importantes en el área.
- ✓ Recurso o procesos alternativos de respaldo que permitan una pronta recuperación.
- ✓ Actualización e inventarios detallados de sistemas, registros, procesos, recursos, configuraciones, bases de datos, herramientas que se hallan disponibles y que son actuales.
- ✓ Atención en la relación directa de dispositivos, datos, sistemas, hardware y software.

- ✓ Revisiones previas y precisas para los mecanismos óptimos en el proceso manipulación de información y de datos.
- ✓ Argumentos de instrucciones válidos.
- ✓ Escogimiento de perfiles válidos o ajustados para su aplicación en el departamento de IP_MPLS.
- ✓ Identificación de registros validos.
- ✓ El almacenamiento de los registros validos.
- ✓ La recuperación de los registros validos.
- ✓ Procedimientos adecuados y controlados ante cambios en la provisión de servicios del departamento de IP_MPLS.
- ✓ Trabajos conjuntos y coordinados con otras áreas operativas de la Corporación Nacional de Telecomunicaciones.
- ✓ Contratos, negociaciones y acuerdos que soporten como respaldo ante un incidente, desastre o amenaza con fabricantes y proveedores de servicios iguales a los de la CNT.
- ✓ Recursos, herramientas, materiales y medios útiles aplicables para la solución de desastres y/o amenazas.
- ✓ Disponibilidad de resultados obtenidos de los ejercicios ante acontecimientos anteriores, ya que servirá como una guía práctica y ágil para una pronta recuperación.

4.4.6. FORMULARIOS Y/O BOLETINES DE REGISTRO.

La periodicidad con la que podrían ser presentados estos formularios y/o boletines de registro de incidentes dependerá de cuan frecuentes son los sucesos que agreden a la continuidad de las operaciones de la CNT y su departamento de IP_MPLS, así tenemos varios ejemplos:

Formularios y/o boletines restringidos. Serán boletines o registros de tipo corto que servirán como historial de las medidas tomadas frente a una amenaza. Teniendo los siguientes tipos:

4.4.6.1. Formularios - Boletines del tipo exclusivo.

Se alerta de forma rápida el cómo hacer frente preventivamente a los fallos en todos los procesos comprometidos.

Tabla 23.
Reporte de tipo exclusivo.

Reporte:	Preliminar		X		Final
Nombre del Evento:	Falla en conexión de cables en subestación		**OT:**		Aviso
Preparado por:	William Murillo		**Puesto de Trabajo:**		MPLS
Equipo (cisco):	Subestación		**Componente o ítem que falló**		Cables eléctricos
Fecha del Evento:	07 mar. 2012	**Hora Parada:**	8:30 am	**equipo:**	
Fecha de Arranque:		**Hora Arranque:**		**Componente:**	
Pérdidas de producción	No hay	**Pérdidas ($):**	Costo Repuesto	**Ambiente:**	No hay

4.4.6.2. Formularios - Boletines semanales.

En este informe se proporciona las actividades programadas en la semana que incluirán: la seguridad, nivel de amenaza, infraestructuras críticas y sus posibles Soluciones.

Tabla 24.

Reporte semanal.

CONTROL SEMANAL	Fecha inicio :	Fecha finalización :
Nombre de quien reporta:		
Equipo que presenta la falla: □ A1 □ B1 □ C1 □ D1 □ E1 Localidad :	Router ( ) Switch ( ) PC ( ) Cableado ( ) Modem ( ) Access Point ( )	Gravedad: Alta ( ) Media ( ) Baja ( )
Descripción de la problemática presentada: Durante las inspecciones de rutina, transformadores e interruptores de la subestación se encontraron los cables del transformador de 5 MVA con tornillos que	**SECUENCIA DE EVENTOS** El equipo transformador de energía se encontraba sin energía, Esta falla es un potencial riesgo, por alta corrosión en los tornillos que realizan la unión de los cables de potencia. **ESTADO ACTUAL** Tornillos en cables de alta sin estándar de manufactura y sin hileras de rosca sobre saliendo en el tornillo. Bloques de madera dentro de cubículo de 23 Kv, esto es usar material combustible dentro de un equipo que esta propenso al calor.	

no cumplen el estándar de manufactura y madera como elemento de sello dentro de cubículo de 23 kv.	También no proporciona hermeticidad al cubículo que puede en temporada de invierno entrar humedad y producirse un arco eléctrico. **POSIBLES CAUSAS** Tornillos inadecuados en la conexión del transformador, se requiere tornillos inoxidables No se utilizó Espuma para sellar de tipo dieléctrica para los cables de salida de los motores y transformador.
Resultados obtenidos	**ACCIONES:** No se ha realizado cambio de tornillos dentro del transformador, se dejo un Punch Ítem para compra de tornillos y cambio en un futuro próximo. No se realizo cambio de las maderas dentro de este cubículo, se deja reporte para que en un futuro se coloque el sellador adecuado. **RECOMENDACIONES** Revisar las próximas celdas, interruptores y transformadores para detectar esta posible falla.
Tiempo empleado en la resolución:	Firma:

4.4.6.3. Formularios - Boletines sobre amenazas

Clasificados según su tipo propagación en la infraestructura, es decir, propagación limitada o rápida y superior, enfocados en un aspecto concreto del control y la seguridad.

Tabla 25.

Reporte de amenazas.

NIVEL DE RIESGO	**DESCRIPCION**	
Id. Riesgo: ( )	**Detalle especifico del problema:** El nivel del riesgo es dependiente de la utilización del equipo comprometido.	
	Localidad: **Alarmas:** **Frecuencia:** **Tipo de Respaldos:**	
ALTO	Aplicaciones comprometidas	Archivos de administrador de red.
	Programas en ejecución	Código fuente de aplicaciones.
	Configuraciones a realizar	Router en la localidad de Tumbaco.
	Equipos comprometidos	Router, Laptops, módems
	Recursos que son usados por las aplicaciones	Sistemas operativo Linux.
	Información de aplicaciones de los usuarios	Directorio /opt
MEDIO	Montaje de dispositivos	Dispositivos de almacenamiento de información
	Aplicaciones opcionales para usuarios	Actualización de elementos detectados de red.
	Recuperación de archivos	Módulos de reportes, historiales, información adicional, manuales, etc.

BAJO	Contenidos Variables	Actualizaciones de firmware.
	Procesos de sistema	Determinación de nivel de fiabilidad del equipo cliente
	Fallos en el respaldo de las fuentes de energía	Estado del sistema: Fiable – No fiable – Indeterminado
Hora :	Fecha:	Responsable:

4.4.6.4. Formularios – Boletines de responsabilidad.

Con el fin de realizar una localización más eficiente de los cambios manejados y ejecutados dentro de los procesos y dispositivos de protección del departamento de IP_MPLS, los responsables de la seguridad deberán registrar su labor cuidadosamente a través de dichos formularios o boletines.

Tabla 26.

Reporte de responsabilidad

Fecha:	**Localidad**	**Tipo de incidente:**	
12 abril 2012	**UIO CNTRO001**	**Fallo en router de borde**	
		172.1XX.XX.XXX router	
Procesador	**Memoria RAM**	**MEMORIA SWAP**	**Tiempo de análisis**
Listado de acciones tomadas frente al incidente			
Configuración de router		**Detalle de lo realizado.**	
Reset router	**Aplica ( )**		
Ejecución de IDS	**Sistema detector de intrusos**	**Tipo de herramienta:**	**Herramienta informática**
Pruebas de cables	**Pruebas de conectividad entre dispositivos de red**		**Herramientas básicas.**
Acceso remoto	**Habilitación de puertos, comprobación de claves, definición de privilegios de acceso.**		**Pcs, portátil o escritorio**
Chequeos adicionales:	**Análisis de datos de logs desde distintos equipos.** **Verificación de direcciones IP.** **Administración de red.** **Control de red.** **Monitoreo de red.**		**Pc portátil** **Cables de consola, cables de red, pc portátil.**

	Monitoreo de interfaces.		
Estado de perfiles de usuario.			**Pcs.**
Resultados obtenidos.			
Descripción:	**Realización de pruebas de conectividad sin novedad. Verificación de direcciones sin novedad.**		
Firma Responsables			

4.5. PRUEBAS, MANTENIMIENTO APLICACIÓN Y SOLUCIÓN.

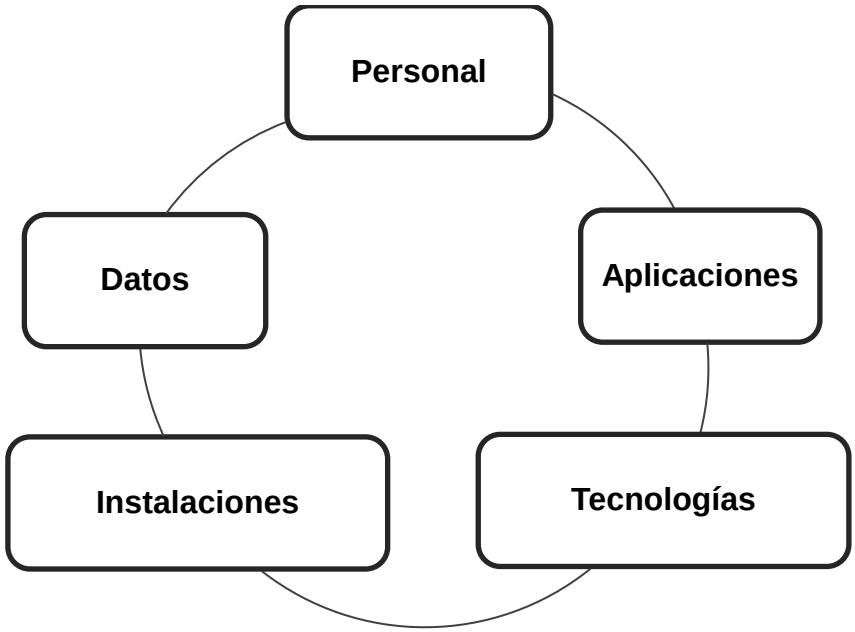
De la misma manera que los japoneses han desarrollado técnicas y programas de prevención de desastres ante la gran cantidad y magnitud de temblores y terremotos ocurridos en ese país, en la CNT y su departamento de IP_MPLS, se someterá a un periodo de educación y control de los procesos para la provisión de los servicios, minimizando amenazas, reduciendo riesgos, contemplando soluciones que estabilicen y mejoren las actividades.

Como los eventos que pudieran convertirse en un riesgo, amenaza o incidente para la CNT han sido identificados, al igual que su campo de interacción dentro de las actividades internas es necesario clasificarlos para un tratamiento por separado.

Los campos y/o aspectos en los que se debe garantizar su disponibilidad buen funcionamiento y continuidad con la realización de pruebas continuas, mantenimiento y pronta solución son:

Figura 22.

Campos para garantizar disponibilidad, buen funcionamiento y realización de pruebas.



Se debe considerar que más del 70% de los procesos y las actividades que se realizan en el departamento de IP_MPLS de la CNT diariamente son repetitivos, por eso se puede mencionar que, “no existe beneficio o frutos sobre un servicio sin un debido proceso”, el procedimiento estará compuesto por métodos para la realización de pruebas que estará basado en:

- ✓ Preliminares de las pruebas.
- ✓ Comprobación de lo realizado en el plan de continuidad.
- ✓ Revisión del plan de continuidad de negocio y su subsistencia.
- ✓ Pruebas sobre el plan de continuidad de negocio del área de IP_MPLS.

- ✓ Contexto y ambiente de las pruebas para el plan de continuidad de negocio.

4.5.1. PRELIMINARES DE LAS PRUEBAS.

Debe contemplar todos los procesos institucionales de la CNT, ya sean manuales o automáticos, evaluando el volumen de información, usuarios masivos o corporativos, personal del área, materiales utilizados con la finalidad de determinar la complejidad de la situación.

Es decir:

- ✓ Selección previa de planes de a ser probados.
- ✓ Selección de personal y sus responsabilidades correspondientes a su rol en el área de IP_MPLS.
- ✓ Previa autorización y aprobación del plan en la CNT.
- ✓ Entrenamiento y conocimiento de los procesos por parte del personal.
- ✓ Acuerdos de horarios de pruebas.
- ✓ Elaboración de informes sobre resultados que aseguren descubrir vulnerabilidades.
- ✓ Establecer la completa disponibilidad de los recursos a utilizarse.

Los principales objetivos a ser conseguidos son:

- ✓ Entrenar al equipo de trabajo que realizara las pruebas ante la presencia real de una amenaza en el departamento de IP_MPLS.
- ✓ Resolver los procesos críticos en el campo comercial de la CNT, ante compañías y empresas que reciben y hacen uso de sus servicios.

Tabla 27.

Ejemplo de procesos institucionales.

Recurso/Acción	Opción 1	Opción 2	Opción X
Procesos de recuperación.	✓ Manual	Automático	Combinado
Tiempo de recuperación de servicios y actividades.	Horas	✓ Días	Semanas
Personal disponible para la solución de problemas.	Designado	✓ Turno	Emergencia
Alternativas emergentes.	Contratistas nacionales.	Subcontratación de servicios	✓ Otro.
Redundancia de activos.	✓ Total	Parcial	Ninguna
Programa de vacaciones del personal.	Garantizar presencia de personal en el área.	✓ Por periodo de trabajo.	Llamados de emergencia.

4.5.2. COMPROBACIÓN DE LO REALIZADO EN EL PLAN DE CONTINUIDAD.

El informe obtenido en los Preliminares de las Pruebas, determinará una o varias secciones del área que necesitaría más atención por parte del equipo de trabajo designado, la capacidad de operación y funcional del plan radicará en el hecho de que los resultados se hallen lo más cercanos posibles ante las pruebas sometidas y las metas trazadas.

Así, en su conjunto el proceso detalla lo siguiente:

- ✓ Identificación y designación del personal que realizará las pruebas.
- ✓ Preparación del plan de pruebas, plan que deberá ser aprobado.
- ✓ Vigilancia de la actuación del plan.
- ✓ Reportes que indiquen los resultados de las pruebas para ser analizadas.
- ✓ De existir fallas, realizar una revisión del plan.
- ✓ Si el plan está operando bien, realizar el reporte correspondiente.
- ✓ Dar inicio al seguimiento, mantenimiento y mejoramiento del plan guiado.

4.5.3. REVISIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO Y SU SUBSISTENCIA.

Se observarán los resultados y sus limitaciones en cuanto a lo esperado en el proceso de pruebas, el planteamiento de las soluciones y sus variantes mejoraran procesos en la provisión de los servicios.

Con los resultados obtenidos de la revisión del plan y los eventos ocurridos, se podrá crear niveles de pruebas que establecerán situaciones reales para la realización de tentativas, siendo detalles específicos de los eventos de riesgo en el área de IP_MPLS.

Tabla 28.

Listado de actividades de control, revisión y subsistencia del PCN.

Fecha del evento	Ítem	Observaciones
04-01-2012	001	Elaboración de calendario de vacaciones para el personal, asegurando disponibilidad de los equipos de trabajo.
10-01-2012 09:10 am	002	Daño en pc de gestión router UIO01.
12-01-1012 08:50 am	003	Perdida de conexión con bases de datos principal.
15-01-2012 01:17 pm	004	Se detecta modificación de información no programada.
15-01-2012 01:55 pm	005	Se utiliza los respaldos de configuraciones, vuelve a la normalidad.

22-01-2012	006	Se realiza upgrades masivos a los usuarios de internet.
23-01-2012	007	No todos los usuarios de internet soportan los upgrades, corrección de velocidad de usuarios, se realiza trabajos con área de planta externa.
24-01-2012	009	Se realiza pruebas de levantamiento de información para comprobar su disponibilidad y obtención de respaldos.
28-01-2012	010	Revisión de locaciones físicas del área de IP_MPLS. Se realiza informe técnico.
30-01-2012	011	Actualización de inventario de equipos, bases de datos, usuarios, contraseñas.
01-02-2012	012	Elaboración del informe mensual.
02-02-2012	013	Designación de responsabilidades, funciones y roles en el departamento de IP_MPLS.

03-02-2012	014	Capacitación y orientación de los colaboradores del área en temas de seguridad industrial, información, procedimientos y uso de equipos.

4.5.4. PRUEBAS SOBRE EL PLAN DE CONTINUIDAD DE NEGOCIO DEL ÁREA DE IP_MPLS.

Las pruebas realizadas sobre el plan de continuidad de negocio, tienen un valor detallado acerca de resultados obtenidos, permitiendo determinar nuevas alternativas ante las fallas y vulnerabilidades detectadas con su ejecución.

Si los resultados obtenidos, no fueran los requeridos o los esperados, entonces el área de IPMPLS está en la obligación de contrarrestar esos efectos considerando aspectos como:

- ✓ Instalación y pruebas con variaciones en el equipamiento.
- ✓ Revisión de los procedimientos.
- ✓ Adiestramiento del personal.
- ✓ Previsión y análisis de los procedimientos establecidos.
- ✓ Mejoramiento de los procedimientos establecidos.
- ✓ Enfoque a la normativa establecida previamente a la realización de las pruebas y sus procedimientos.
- ✓ Evitar sobre carga de responsabilidades en los colaboradores del Plan.
- ✓ Comparación de los resultados obtenidos en los procedimientos realizados.

4.5.5. CONTEXTO Y AMBIENTE DE LAS PRUEBAS PARA EL PLAN DE CONTINUIDAD DE NEGOCIO.

La ejecución de las pruebas según los lineamientos detallados y requeridos del Plan de Continuidad de Negocio, demandan de un ambiente controlado que permita obtener los mejores resultados sino los resultados esperados frente a su valoración y posterior documentación.

Se considerará situaciones y aspectos para la obtención de los resultados más cercanos, así:

- ✓ Alcance de la meta esperada ante la prueba ejecutada.
- ✓ Representación esquemática del tipo de prueba ejecutada.
- ✓ Reducir equipamiento necesario.
- ✓ Selección de los colaboradores y su disponibilidad previa.
- ✓ Lineamientos de disponibilidad para locaciones.
- ✓ Consideración de pruebas en sitio y remotas.
- ✓ Control de procesos, acciones del personal y procedimientos para suspender o dar reinicio a las pruebas ejecutadas.
- ✓ Precisión de objetivos de éxito en la realización de cada prueba.
- ✓ Detalle de resultados frente a la evaluación.

En este contexto, algunos indicadores del proceso a tomarse en cuenta podrían ser:

Tabla 29.

Indicadores de procesos para la realización de las pruebas del PCN.

CONTEXTO / ARGUMENTO	RELACIÓN
✓ Número de cambios implementados.	✓ Servicios que cumplen con los requerimientos acordados con y para los clientes.
✓ Reducción en el número de interrupciones a servicios	✓ Defectos y trabajo causado por especificaciones inexactas o evaluación de impacto pobre o incompleto.
✓ Resultados de implementar ITIL	✓ Métricas e información para toma de decisiones.
✓ Reducción de costos	✓ Eliminación de esfuerzos duplicados o innecesarios, mayor productividad de usuarios y personal IT.
✓ Reducción en el riesgo operacional	✓ Demostración del valor de las prácticas de IT al negocio

✓ Reducción en el costo de propiedad de IT	✓ Control sobre los activos tecnológicos
✓ Resultados medibles.	✓ Cumplimiento de objetivos. ✓ Tiempos de respuesta cortos

CAPÍTULO V

5. ANÁLISIS DE LOS BENEFICIOS DEL PCN Y SU PLAN DE ACCIÓN.

El realizar perfeccionamientos para adicionar e incorporar nuevas tecnologías, procesos, métodos, ideas o controles dedicados a proyectos de mejoras tecnológicas y/o administrativas dentro de la CNT, contrae el cubrimiento de sectores vulnerables dentro del departamento de IP_MPLS, lo que resulta beneficioso por la adaptabilidad del personal a las nuevas normas implementadas en la puesta en marcha del Plan de Continuidad.

Se deberá tomar en cuenta la eventualidad y/o posibilidad de que los nuevos equipamientos adquiridos tras una inversión, pueden conducir a beneficios no económicos, ya que en la CNT, una transformación a éste nivel tiene como su objetivo principal el perfeccionamiento en la provisión y prestación de los servicios o en su defecto en los procesos que conllevan a su desarrollo.

Con la realización de pruebas o análisis entre efectividad y beneficio del Plan de Continuidad, se demuestra que la CNT y su departamento de IP_MPLS, posee los potenciales necesarios con los procedimientos implantados, las nuevas tecnologías y la mejor resolución de incidentes o amenazas presentes en el proceso de provisión de servicios.

Los responsables técnicos y administrativos del departamento de IP_MPLS requieren analizar, desarrollar o aprobar los beneficios ligados directamente con la implementación de las guías descritas en el plan, deben tener determinado no solo lo concerniente con la adquisición de equipos y programas, o la eventual contratación de consultores y proveedores para la instalación del nuevo sistema, sino también, los factores administrativos y mantenimientos permanentes que además son necesarios para el área.

La realización de un análisis o estudio previo para determinar el ciclo de vida de procesos, métodos y tecnologías, arrojan como resultado que puede reutilizarse para más de un propósito, aprovechando hasta el final su funcionamiento, implementación o utilización, que al momento de su terminación será fijada en términos de efectividad junto a aquellas que deberán ser reemplazadas en plazos cortos.

5.1. LA IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO PARA LA CNT Y SU DEPARTAMENTO DE IP_MPLS.

Los efectos que cualquier embestida, agresión o incluso falla de índole tecnológica, física o humana que puede presentarse dentro del área de IP_MPLS, tanto en la CNT como en cualquier organización, siempre tienen al final una consecuencia en pérdida de clientes que a su vez viene ligada a una pérdida económica por la paralización en la provisión de sus servicios.

A menudo, la implantación de nuevas medidas para realizar control sobre las actividades, atrae consigo incomodidad en el personal, y en ocasiones se puede apreciar varios tipos de justificaciones para la no creación de disposiciones de seguridad, basándose en su costo o a la molestia que pueda involucrar una nueva reglamentación y cultura de seguridad en la organización.

Varias son las soluciones en tecnología que se pueden representar con costos elevados y que significan la eliminación de procedimientos manuales, y está claro que no siempre es aconsejable incorporar una nueva infraestructura tecnológica para obtener adicionales mejoras en la provisión de servicios a los clientes, por el contrario, con un buen planeamiento en el que se identifiquen procesos, documentación de métodos, soluciones e ideas pueden lograrse los objetivos planteados.

En definitiva, la estimación de todos los beneficios implicados en la adopción de nuevos procedimientos, procesos, métodos, lineamientos y medidas de control así como de nueva tecnología, incluyendo equipos, infraestructura, programas, sistemas de comunicación, personal, consultores externos y mantenimiento, se verán reflejados en la calidad del servicio hacia los usuarios de la Corporación Nacional de Telecomunicaciones, ya que son el verdadero capital de la empresa.

5.1.1. DETALLE DE LOS BENEFICIOS A CONSIDERAR.

- ✓ Examinar la metodología actual, su sustento e indicar el ciclo estimado de uso eficaz.
- ✓ Identificación de factores externos indispensables que viabilizarán el proyecto, como la aprobación de los métodos a establecerse y procedimientos a regir.
- ✓ Actualización de plataformas tecnológicas.
- ✓ Capacitación del personal.
- ✓ Mejoramiento o readecuación de estaciones de trabajo.
- ✓ Redundancia de la tecnología.

El programa, da lección de cómo conformar este plan, identificando las áreas que potencialmente han sido problemáticas, pudiendo determinar recomendaciones para definir un enfoque apropiado que mejorará los procesos existentes, creando un plan de actuación para la implantación de los procesos nuevos de corrección.

Este plan al ser un cúmulo de prácticas y recomendaciones del buen manejo de la información y las plataformas tecnológicas, se deberá proporcionar el seguimiento a un programa de continuidad y perfeccionamiento por parte del departamento de IP_MPLS, brindando la ayuda informativa al área, contribuyendo con la eficacia y eficiencia de sus procesos de provisión de servicios.

Un detalle de los beneficios que se pueden considerar son los siguientes elementos:

- ✓ Exactitud de los propósitos trazados por el área de IP_MPLS.
- ✓ Justificación del por qué son necesarios los procesos a seguir.
- ✓ Detalle del o los procesos reemplazados, ya sean de corto y largo plazo.
- ✓ Apropiada documentación y registro de los riesgos o problemas que pueden agudizarse al no tener una planeación adecuada.
- ✓ Detalle del funcionamiento de los nuevos estudios de las aplicaciones a implementarse.

Los tópicos que abarcan estos beneficios son:

- ✓ Las estrategias de gestión de servicio.
- ✓ Diseño y organización de los nuevos servicios provistos por la CNT a través de su departamento de IP_MPLS.
- ✓ Introducción y operación de los servicios.
- ✓ Mejoramiento en la continuidad de los servicios.

Con el cuidado de las mejores prácticas a las actividades, procesos, métodos, procedimientos y provisión de servicios de la CNT, los volúmenes de incidentes serán reducidos, la resolución de posibles eventualidades será más rápida y habrá menos trastornos para las actividades normales de la CNT.

La calidad de servicio se verá mejorada por la introducción de un agregado de procesos semejantes que pondrá en evidencia las fragilidades existentes en las actividades anteriores, fomentando en el departamento de IP_MPLS las mejoras proactivas.

Además, los plazos de resolución serán menores, acompañados de mejor control de gestión, servicios informáticos y estructurales fiables, la implantación de soluciones permanentes a problemas claramente identificados son tan sólo algunas de las maneras en que el plan contribuirá a mejorar la continuidad y calidad de sus servicios.

5.2. DISEÑO DEL PLAN DE ACCIÓN.

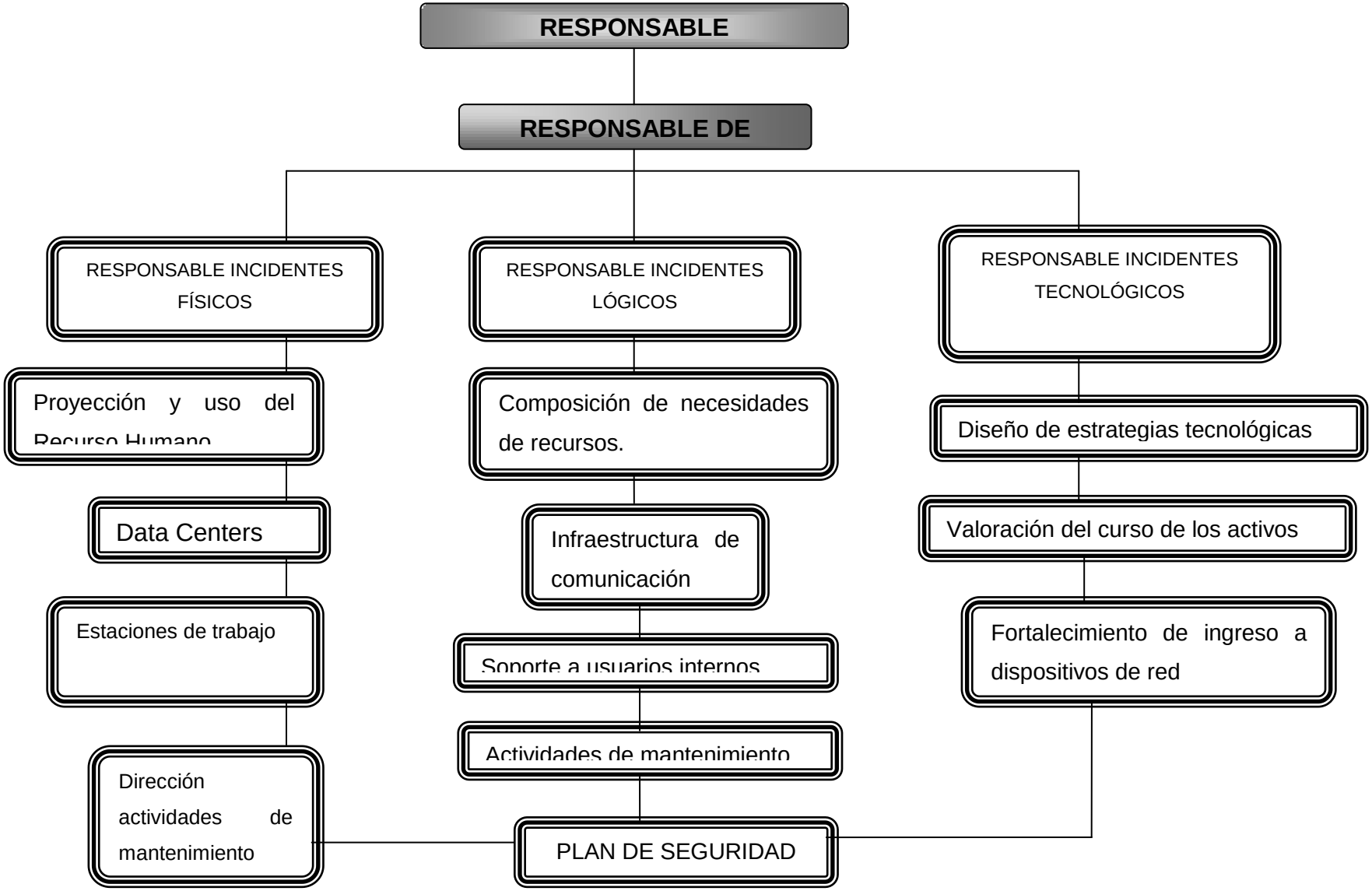
El plan de acción diseñado, asegurará que las acciones tomadas frente a una contingencia sean precisas y óptimas, minimizarán los tiempos de suspensión de los servicios y agilitarán las acciones a tomarse para prevenir consecuencias mayores.

Previamente, los administradores del área de IP_MPLS, deben haber conformado los grupos de trabajo con su respetivo líder, que sea el encargado de dirigir las acciones a tomar frente a una contingencia.

Para facilitar la efectividad del plan de acción del departamento de IP_MPLS, los canales de comunicación deberán ser adecuados y siempre estar disponibles, así como las notificaciones a las autoridades nombradas, es decir, locación, personal, jefes de grupo y gerentes.

El plan de acción, ofrecerá al personal que forma parte de los equipos designados la habilidad para contrarrestar las consecuencias, el entrenamiento propio para afrontar contingencias con la mayor rapidez y eficacia.

Tabla 30. PLAN DE ACCIÓN.



CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- ✓ El plan de continuidad de negocio aquí descrito, busca organizar los procesos, procedimientos, servicios y necesidades de la CNT con sus clientes y viceversa.
- ✓ El resultado de la implementación del plan de continuidad de negocio, será un trabajo en equipo coordinado que brinde respuestas rápidas a cualquier eventualidad de incidente.
- ✓ El desarrollo y el seguimiento del plan de continuidad de negocio en la CNT, determinará eficazmente las áreas que mantienen mayor vulnerabilidad ya sea en la prestación de servicios, administración, gestión y la toma de correctas decisiones en situaciones de riesgo.
- ✓ Brindará una mayor operatividad al personal, ya que los tiempos de paralizaciones serán reducidos por la organización y registro de la información ante eventualidades de riesgo.
- ✓ Aumento del control sobre los acuerdos de nivel de servicio SLA, disminuyendo sensiblemente penalizaciones por falta de cumplimiento de contratos.
- ✓ Detalles de registros de control homogéneos que facilitarán su comprensión al personal responsable del departamento de IP_MPLS.
- ✓ Significativa reducción de incidentes, ante la innovación y el establecimiento de soluciones eficaces enfocados a todas las actividades, procesos y provisión de los servicios del departamento de IP_MPLS.
- ✓ En la CNT y su departamento de IP_MPLS, se ha determinado que la continuidad de las operaciones ha aumentado, ya que depende directamente de la forma de gestionar los riesgos que afectan sus operaciones.

- ✓ Al igual que las plataformas tecnológicas y de software utilizadas en el departamento de IP_MPLS están en constante evolución y actualización para mejorar la provisión de servicios en la CNT, el personal que los opera cambia también los procedimientos de operación, lo que significa que riesgos que se creían mitigados vuelven a ser motivo de inquietud, lo que indica que la guía propuesta como Plan de Continuidad de Negocio también deberá evolucionar.
- ✓ El resultado obtenido en el área de IP_MPLS, después de la aplicación de la estrategia ante incidentes o amenazas, es la mejora continua, el registro de los incidentes, la recopilación de nueva y actualizada información, además, tiempo de respuesta menor ante cada uno, minimizando la probabilidad de su ocurrencia.

6.2. RECOMENDACIONES

- ✓ Conseguir el compromiso de los integrantes del equipo de trabajo del departamento de IP_MPLS es fundamental, para que participen activamente de las reuniones de aprobación de cambios.
- ✓ Para la identificación de los riesgos en el departamento de IP_MPLS en la CNT, se deberá conformar un equipo de trabajo, el cual su único objetivo será el de estandarizar los nuevos incidentes que pudieran aparecer en el futuro.
- ✓ Se deberá realizar la documentación y registro de cada uno de los cambios realizados a los procesos y a los activos que, han sido definidos como estándares a los procedimientos ya establecidos dentro del departamento de IP_MPLS, con la finalidad de lograr un mejor control de los mismos y en donde además, quedará evidenciada la realización de dichos cambios y sus responsables.
- ✓ Dentro de la documentación de los cambios realizados a los procesos y activos del área de IP_MPLS, se asegurará que los cambios son registrados y luego evaluados, autorizados, priorizados

planificados, probados e implementados de forma controlada por el equipo de trabajo responsable de los mismos.

- ✓ Los objetivos alcanzados deberán ser cuantitativos para administrar calidad y desempeño del proceso.
- ✓ Responder a los requerimientos de los clientes maximizando la continuidad y el valor de los servicios, reduciendo los incidentes o las interrupciones con una favorable acogida a las nuevas normas de control establecidas por el departamento de IP_MPLS.
- ✓ Responder favorablemente con una buena planificación, a las exigencias de los cambios de procesos de provisión de servicios y de Tecnologías de información (TI), que alinearán al servicio con las necesidades de los clientes.
- ✓ Una vez que se ha logrado una reducción importante en la cantidad de incidentes como resultado de la planificación implantada a la ejecución de cambios (autorizados y no autorizados), se lo establecerá como un proceso valido y útil para el área de IP_MPLS.
- ✓ Para la conformación de los grupos de trabajo, se identificará al personal con el nivel de conocimiento técnico y de negocio adecuado.
- ✓ Se considerará la utilización de cambios de emergencia para evitar los procesos repetitivos.
- ✓ Se debe asegurar que las mediciones y el estudio, tienen un significado o conclusión, ya que comparando lo sencillo que es contar los incidentes que eventualmente componen un cambio en los procesos, tiene más valor la identificación de las causas y detalles de esos cambios para comparar sus tendencias.

REFERENCIAS.

- ✓ ABOSO, Gustavo Eduardo y ZAPATA, María Florencia, Cibercriminalidad y Derecho Penal, Editorial BDF de Montevideo y Buenos Aires, Edición 2006
- ✓ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. http://www.cybsec.com
- ✓ Conferencia TECNOLÓGICAS. Continuidad de Negocio, Seguridad de la Información ITIL. ISEC. Quito Hotel Marriot. mayo de 2011.
- ✓ Conferencia. Gestión de Riesgos. Expositor José Antonio Mañas. Departamento de Ingeniería en Sistemas Informáticos. Universidad Politécnica de Madrid. 23 de febrero de 2010. http://www.youtube.com/watch?v=-lbbPJd_adE
- ✓ Conferencia: Business Continuity Management - Maximiliano Canosa IProt: http://www.youtube.com/watch?v=kbuQVBGmEvM
- ✓ Entrevista: Continuidad de Negocio. Alejandro Aristizabal. Docente Universidad Pontifica Bolivariana - Colombia. Consultor en Continuidad de Negocio.
- ✓ FALAGAN ROJO, M.J; CANGA ALONSO, A; FERRER PIÑOL, P; QUINTANA FERNÁNDEZ, J.M. Manual básico de prevención de riesgos laborales: Higiene industrial, seguridad y ergonomía. Sociedad Asturiana de Medicina y Seguridad en el trabajo y Fundación Médicos de Asturias. Oviedo 2000.
- ✓ FERNADEZ, Carlos M. Seguridad en sistemas informáticos. Ediciones Díaz de Santos S.A. España. 1988. Página 105.
- ✓ HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Version 1.2).
- ✓ Implementing Cisco MPLS; Student Guide; Cisco Systems Learning; 2010.
- ✓ ISEC. Conferencias de Seguridad de la Información – Continuidad de Negocio. Hotel Marriott.

- ✓ ISO. Evaluación de la seguridad de la tecnología de la información. Norma ISO 15408.
- ✓ Kauffels, Franz. Network Management: Problems, Standards and Strategies. Addison-Wesley, 1992.
- ✓ Manual CNT. Un modelo funcional para la administración de redes IP_MPLS CNT relacionado a la Seguridad.
- ✓ MERLAT, Máximo, Seguridad Informática: Los Hackers, Buenos Aires Argentina, 1999, Publicación hecha en Internet www.monografías.com
- ✓ Norma Internacional ISO/IEC 17799:2002
- ✓ P. Nobles and P. A. Horrocks, “Vulnerability of IEEE802.11 WLANs to MAC layer DoS attacks,” in Proceedings of The 2nd IEE Secure Mobile Communications Forum, Institution of Electrical Engineers, 2005.
- ✓ Planes de Contingencia. La Continuidad de Negocio en las Organizaciones. Juan Gaspar Martinez. 2004. Editorial Diaz de Santos.
- ✓ Proctor Paul E., Practical Intrusion Detection Handbook. Prentice Hall Hispanoamericana S.A. México 2005.
- ✓ RESA NESTARES CARLOS: Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea, 2005.
- ✓ RFC 1244: Site Security Handbook. J. Reynolds - P. Holbrook. Julio 1991.
- ✓ SIC. Seguridad en Informática y Comunicaciones. No 63, febrero 2005.
- ✓ SPAFFORD, Gene. "Manual de seguridad en redes". ArCERT. Argentina. 2000. http://www.arcert.gov.ar
- ✓ Stamp Mark, Information Security, Principles and Practice Wiley Interscience 2006.

REFERENCIAS DE INTERNET

- ✓ http://businesscontinuity-pe.blogspot.com/2012/07/analisis-de-impacto-al-negocio-bia.html
- ✓ http://businesscontinuity-pe.blogspot.com/2012/08/ciclo-de-vida-del-programa-de.html

- ✓ http://www3.weforum.org/docs/WEF_GCR_CompetitivenessIndexRanking_2011-12.pdf World Economic Forum (WEF).
- ✓ NIST - http://www.nist.org/ -SP 800-30 “Risk Management Guide for IT Systems”
- ✓ Guide for Applying the Risk Management Framework to Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- ✓ http://www.iso27000.es/iso27000.html#section3a
- ✓ http://www3.weforum.org/docs/WEF_GCR_CompetitivenessIndexRanking_2011-12.pdf World Economic Forum (WEF).
- ✓ http://www.etse.urv.es/ri/docs/Seguretat/UNIX/unixsec.pdf
- ✓ http://www.ezone.net/es/servicios/soluciones-de-continuidad
- ✓ http://www.itcio.es/planes-contingencia/analisis/1004786016902/plan-continuidad-negocio-debe-prioridad.1.html
- ✓ http://www.revista-ays.com/DocsNum17/PersEmpresarial/Anton.pdf criterios
- ✓ http://www.cnt.com.ec/index.php?option=com_content&view=article&id=230&Itemid=23
- ✓ http://www.conatel.gob.ec/site_conatel/index.php?option=com_content&view=article&catid=25%3Ainformacion-corporativa&id=51%3Avision&Itemid=339
- ✓ http://www.esa-security.com/web/servicios/plan.htm
- ✓ http://www.itworld.com/security/54579/survey-it-staff-would-steal-secrets-if-laid