REPÚBLICA DEL ECUADOR
Escuela Politécnica Nacional
"E SCIENTIA HOMINIS SALUS"

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del autor.

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.

- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.

- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DETERMINACIÓN Y AUDITORÍA DE PROCESOS INTERNOS DE SEGURIDAD, INCIDENTES Y PROBLEMAS DEL ÁREA DE OPERACIÓN Y MANTENIMIENTO DE LA RED IP/MPLS DE CNT E.P. MEDIANTE COBIT 4.1 Y NORMALIZACIÓN DE DICHOS PROCESOS USANDO LA GUÍA DE LAS PRÁCTICAS ITIL V.3.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

SANDY GABRIELA ACOSTA MONTERO
sandygabriela2010@gmail.com

MARJURI RAQUEL BAUTISTA MATA
raquel.marjux@gmail.com

DIRECTOR: ING. MÓNICA VINUEZA
monica.vinueza@epn.edu.ec

CODIRECTOR: ING. ANDRÉS ALMEIDA
caaamh@hotmail.com

Quito, julio 2016

DECLARACIÓN

Nosotras, Sandy Gabriela Acosta Montero y Marjuri Raquel Bautista Mata, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Sandy Gabriela Acosta Montero Marjuri Raquel Bautista Mata

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Sandy Gabriela Acosta Montero y Marjuri Raquel Bautista Mata, bajo nuestra supervisión.

_____	_____
ING. MÓNICA VINUEZA	ING. ANDRÉS ALMEIDA
DIRECTOR DEL PROYECTO	**CODIRECTOR DEL PROYECTO**

AGRADECIMIENTO

A Dios, por guiarme en este largo camino y por darme fuerza en los momentos más difíciles.

A mis padres Bolívar y Rosy por su apoyo incondicional, por ser el pilar de mi vida y enseñarme cada día con su ejemplo que todo se logra con esfuerzo, dedicación y que nada es imposible. Por tener siempre una palabra de aliento que me ayude a levantarme en cada caída y no permitir que me rinda.

A mi hermana Steffy por ser mi mejor amiga, mi apoyo gracias por tu paciencia durante las malas noches y porque siempre me diste fuerzas para seguir adelante.

A mi sobrino Thiaguito porque con tu sonrisa alegras cada día y me das fuerza para continuar.

A mi novio Cristhian, por compartir cada momento de alegría y tristeza conmigo, por no dejarme desistir cada vez que se presentaba una dificultad y recordarme por qué luchaba cada día.

A mis tías quienes siempre han estado pendientes de mí y con sus consejos, me han ayudado a seguir luchando por lograr mis objetivos. A mi compañera y amiga Marjuri, quien luchó a mi lado en todo este duro proceso, por su apoyo y motivación.

Al área O&M MPLS de la CNT E.P. en especial al ingeniero Andrés Almeida por su apoyo y guía para el desarrollo del presente proyecto. A la ingeniera Mónica Vinueza por su guía para la culminación exitosa de este proyecto.

Sandy Gabriela Acosta Montero

DEDICATORIA

A Dios, quien me dio fortaleza en estos años de duro trabajo.

A mis padres quienes son el pilar de mi vida que con su apoyo paciencia y amor me han ayudado a cumplir mis metas.

A mi hermana que siempre ha estado a mi lado y siempre ha tenido una palabra de consuelo en los momentos difíciles.

A mi pequeño Thiago que me impulsa a seguir adelante.

A Cristhian, que con su infinito amor hace que cada día sea una mejor persona.

¡Este logro es por y para ustedes!

AGRADECIMIENTO

Mis sinceros agradecimientos:

A Dios por la persona que soy, por las bendiciones y lecciones aprendidas hasta ahora en el camino de mi vida,

A mis padres Ignacio y Dolores, que lo han dado todo incondicionalmente empezando por su ejemplo hasta la última gota de sacrificio por mi persona,
A mi compañero de lucha, mi hermano Juan Carlos, quien en cada decepción, lágrima, reto, satisfacción estuvo conmigo, también agradezco a mi hermana Karen quien ha sido uno de mis motores para no perder el objetivo y como no agradecer a mi hermano Oscar de quien a pesar de los miles de kilómetros he tenido los más sabios consejos y oraciones,

A mi Ángel, por haber estado ahí en cada paso que di en la carrera, por ser mi ejemplo, mi soporte y mi amigo, Te amo,

A la Ing. Mónica Vinueza por su confianza, paciencia, y colaboración a lo largo del desarrollo de este proyecto,

A Sandy, mi compañera de tesis y amiga quien me dio aliento cuando no se veía la luz al final del túnel, lo logramos. A los colaboradores del área MPLS de CNT, por la cooperación brindada y en especial al Ing. Andrés Almeida por su predisposición y orientación para el desarrollo de este proyecto,

A mis amigos Victoria, Marisela, Jenny, Graciela y Andrés por darme la fuerza para seguir siempre hacia adelante y sin mirar atrás, Finalmente agradezco a mis compañeros de aulas y a todas las personas que me dieron aliento y creyeron en mí para cumplir con este objetivo.

Marjuri Raquel Bautista Mata

DEDICATORIA

A Dios, quien es la esencia de mi vida,

A mis padres amados Ignacio y Dolores quienes han sido mi soporte y fuerza para cumplir con mi objetivo,

A Ángel Hidalgo quien ha sido mi fuente de inspiración.

¡Esto es para ustedes!

CONTENIDO

CAPÍTULO 1 1

1 MARCO TEÓRICO 1

1.1 LEVANTAMIENTO DE PROCESOS 1

1.1.1 GESTIÓN ENFOCADA EN PROCESOS 1

1.1.2 ELEMENTOS DE UN PROCESO 2

1.1.3 CLASIFICACIÓN DE PROCESOS 3

1.1.3.1 Procesos Sustantivos 3

1.1.3.2 Procesos Complementarios 3

1.1.3.3 Procesos de soporte 3

1.1.4 PASOS PARA LEVANTAR UN PROCESO 3

1.2 GOBIERNO DE TI 4

1.2.1 COMPONENTES DE GOBIERNO DE TI 4

1.2.1.1 Alineación estratégica 5

1.2.1.2 Entrega de valor 5

1.2.1.3 Administración de riesgos 5

1.2.1.4 Administración de recursos 5

1.2.1.5 Medición del desempeño 6

1.3 COBIT 6

1.3.1 DOMINIOS DE COBIT 4.1 7

1.3.1.1 Planeación y organización 7

1.3.1.2 Adquisición e implementación 7

1.3.1.3 Entrega y soporte 8

1.3.1.4 Monitoreo y evaluación 8

1.3.2 CRITERIOS DE INFORMACIÓN DE COBIT 4.1 8

1.3.3 PROCESOS COBIT 9

1.3.3.1 DS5 Garantizar la Seguridad de los Sistemas 9

1.3.3.1.1 DS5.1 Administración de la Seguridad de TI 10

1.3.3.1.2 DS5.2 Plan de Seguridad de TI 10

1.3.3.1.3 DS5.3 Administración de Identidad 10
1.3.3.1.4 DS5.4 Administración de Cuentas del Usuario..... 10
1.3.3.1.5 DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad 11
1.3.3.1.6 DS5.6 Definición de Incidente de Seguridad 11
1.3.3.1.7 DS5.7 Protección de la Tecnología de Seguridad..... 11
1.3.3.1.8 DS5.8 Administración de Llaves Criptográficas..... 11
1.3.3.1.9 DS5.9 Prevención, Detección y Corrección de Software Malicioso 11
1.3.3.1.10 DS5.10 Seguridad de la Red..... 11
1.3.3.1.11 DS5.11 Intercambio de Datos Sensitivos 11
1.3.3.2 DS8 Administrar la Mesa de Servicio y los Incidentes. 11
1.3.3.2.1 DS8.1 Mesa de Servicios 12
1.3.3.2.2 DS8.2 Registro de Consultas de Clientes 12
1.3.3.2.3 DS8.3 Escalamiento de Incidentes..... 12
1.3.3.2.4 DS8.4 Cierre de Incidentes 12
1.3.3.2.5 DS8.5 Análisis de Tendencias..... 12
1.3.3.3 DS10 Administración de Problemas……13
1.3.3.3.1 DS10.1 Identificación y Clasificación de Problemas..... 13
1.3.3.3.2 DS10.2 Rastreo y Resolución de Problemas 13
1.3.3.3.3 DS10.3 Cierre de Problemas..... 13
1.3.3.3.4 DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas 13
1.3.4 MODELO DE MADUREZ.....14
1.3.5 MATRIZ RACI 14
1.4 ITIL……15
1.5 CICLO DE VIDA DE LOS SERVICIOS TI MEDIANTE ITIL V3 EDICIÓN 2011…… 15
1.5.1 ESTRATEGIA DEL SERVICIO 16
1.5.2 DISEÑO DEL SERVICIO 17
1.5.3 TRANSICIÓN DEL SERVICIO 17
1.5.3.1 Gestión de Cambios…….. 18

1.5.4 OPERACIÓN DEL SERVICIO 21
1.5.4.1 Funciones de la Operación del Servicio…… 22
1.5.4.2 Procesos de la Operación del Servicio ……..24
1.5.4.2.1 Gestión de Eventos 24
1.5.4.2.2 Gestión de Incidentes 27
1.5.4.2.3 Gestión de Problemas 32
1.5.4.2.4 Gestión de Consultas 35
1.5.4.2.5 Gestión de Acceso 36
1.5.5 MEJORA CONTINUA DEL SERVICIO.....38
1.5.5.1 El Ciclo de Deming……..... 39
1.5.5.2 Métricas.....39
1.5.5.3 Proceso de Mejora continua del Servicio..... 39
1.5.5.4 Relación con la fase de Operación del Servicio…..... 42
1.6 MAPEO DE LOS PROCESOS COBIT ALINEADOS A ITIL.....42

CAPÍTULO 2 46

2 AUDITORÍA DE LOS PROCESOS INTERNOS DE OPERACIÓN Y MANTENIMIENTO CON COBIT 4.1 46

2.1 SITUACIÓN ACTUAL DEL ÁREA DE OPERACIÓN Y MANTEMIENTO DE MPLS……46

2.1.1 OBJETIVO DEL ÁREA.....46

2.1.2 ESTRUCTURA DEL ÁREA O&M DE IP/MPLS 46

2.1.2.1 Gestión Técnica……46
2.1.2.2 Gestión de Proyectos y Logística…..47
2.1.2.3 O&M Backbone MPLS…… 47
2.1.2.4 O&M Core…… 47

2.1.3 OBJETIVOS DEL AREA DE OPERACIÓN Y MANTENIMIENTO MPLS 48

2.1.4 HERRAMIENTAS DE APOYO DEL ÁREA O&M de IP MPLS 49

2.1.4.1 Cisco Prime……49
2.1.4.2 Cacti…… 52
2.1.4.3 Sistema de control de Acceso ACS…… 53
2.1.4.4 BMC Remedy…… 55
2.2 DETERMINACIÓN DE LOS PROCESOS DE OPERACIÓN EN EL ÁREA O&M DE MPLS DE LA CNT E.P……..92
2.2.1 PROCESOS EXISTENTES.....92
2.2.2 PROCESOS NO EXISTENTES 93
2.3 CRITERIOS DE COBIT 4.1 APLICADOS PARA LA AUDITORÍA DE LA SITUACIÓN ACTUAL DEL ÁREA DE O&M DE MPLS DE LA CNT E.P. 56
2.4 SITUACIÓN ACTUAL DE LOS PROCESOS DEL ÁREA DE O&M DE MPLS…… 61
2.4.1 MATRIZ DE VALOR Y ASIGNACIÓN DE RECURSOS DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD 61
2.4.2 MATRIZ DE DESEMPEÑO DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD 64
2.4.3 MATRIZ DE RIESGOS DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD 70
2.4.4 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD 72
2.4.5 MODELO DE MADUREZ DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD 72
2.4.6 MATRIZ DE VALOR DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS 73
2.4.7 MATRIZ DE DESEMPEÑO DEL PROCESO DE ADMINISTRACIÓN de problemas 74
2.4.8 MATRIZ DE RIESGOS DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS 80
2.4.9 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS 81

2.4.10 MODELO DE MADUREZ DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS 82

2.4.11 MATRIZ DE VALOR DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK* 82

2.4.12 MATRIZ DE DESEMPEÑO DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK* 84

2.4.13 MATRIZ DE RIESGOS DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK* 89

2.4.14 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK* 91

2.4.15 MODELO DE MADUREZ DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK* 91

CAPÍTULO 3 94

3 NORMALIZACIÓN Y DOCUMENTACIÓN DE PROCESOS BASADOS EN LA FASE DE OPERACIÓN DEL SERVICIO DEL CICLO DE VIDA DE ITIL 94

3.1 PROCESO DE GESTIÓN DE EVENTOS..... 94

3.1.1 OBJETIVO 94

3.1.2 ALCANCE 94

3.1.3 DEFINICIONES 94

3.1.3.1 Evento..... 94

3.1.3.2 Alarma de Información..... 94

3.1.3.3 Alarma de Advertencia..... 95

3.1.3.4 Alarma de Excepción..... 95

3.1.4 RESPONSABLE 95

3.1.5 DESARROLLO DEL PROCESO DE GESTIÓN DE EVENTOS 95

3.1.5.1 Monitoreo de eventos..... 95

3.1.5.2 Definición de Eventos..... 96

3.1.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE EVENTOS 98
3.2 PROCESO DE GESTIÓN DE INCIDENTES..... 99
3.2.1 OBJETIVO 99
3.2.2 ALCANCE 99
3.2.3 DEFINICIONES 99
3.2.3.1 Incidente..... 99
3.2.3.2 Escalamiento..... 99
3.2.3.3 Impacto..... 99
3.2.3.4 Prioridad..... 100
3.2.3.5 Urgencia..... 100
3.2.3.6 Pruebas de Primer Nivel..... 100
3.2.3.7 Pruebas de Segundo Nivel..... 100
3.2.4 RESPONSABLE 100
3.2.5 DESARROLLO DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTES NOC 100
3.2.5.1 Procedimiento de registro y clasificación de incidentes..... 100
3.2.5.1.1 Identificación de Incidente 100
3.2.5.1.2 Registro del incidente 101
3.2.5.1.3 Categorización del Incidente 101
3.2.5.1.4 Priorización de un Incidente 102
3.2.5.2 Procedimiento del análisis y resolución de incidentes NOC..... 103
3.2.5.2.1 Pruebas de primer nivel 103
3.2.5.2.2 Acciones correctivas 103
3.2.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE INCIDENTES NOC 104
3.2.7 DESARROLLO DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTES MPLS 105
3.2.7.1 Recepción del ticket..... 105
3.2.8 DIAGRAMA DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTES MPLS 105

3.2.9 DESARROLLO DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTE CRÍTICO 106
3.2.10 DIAGRAMA DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTE CRÍTICO 107
3.2.11 DESARROLLO DEL PROCEDIMIENTO DE CIERRE DE INCIDENTES 108
3.2.11.1 Notificación de la solución…….....108
3.2.12 DIAGRAMA DEL PROCEDIMIENTO DE CIERRE DE INCIDENTES 108
3.3 PROCESO DE GESTIÓN DE PROBLEMAS……..109
3.3.1 OBJETIVO 109
3.3.2 ALCANCE 109
3.3.3 DEFINICIONES.....109
3.3.3.1 Problema…….....109
3.3.3.2 Error conocido…….....109
3.3.3.3 Base de datos de error conocido……...109
3.3.4 RESPONSABLE 109
3.3.5 DESARROLLO DEL PROCESO DE GESTIÓN DE PROBLEMAS.....110
3.3.5.1 Registro de problemas……..……110
3.3.5.2 Investigación y diagnóstico de problemas…….....110
3.3.5.3 Acciones correctivas……111
3.3.5.4 Solución del problema ……111
3.3.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE PROBLEMAS.....111
3.4 PROCESO DE GESTIÓN DE CONSULTAS……...112
3.4.1 OBJETIVO 112
3.4.2 ALCANCE 112
3.4.3 RESPONSABLE 113

3.4.4 DESARROLLO DEL PROCESO DE GESTIÓN DE CONSULTAS 113
3.4.4.1 Recepción de la consulta……113
3.4.4.2 Registro y Validación de la consulta……113
3.4.4.3 Categorización de la consulta……113
3.4.4.4 Priorización de la consulta……..114
3.4.4.5 Autorización de la consulta……..114
3.4.4.6 Revisión de consulta……114
3.4.4.7 Ejecución de la consulta……..114
3.4.4.8 Cierre de la consulta……114
3.4.5 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE CONSULTAS 115
3.5 PROCESO DE GESTIÓN DE ACCESOS……116
3.5.1 OBJETIVO 116
3.5.2 ALCANCE 116
3.5.3 RESPONSABLE 116
3.5.4 DEFINICIONES.....116
3.5.4.1 Confidencialidad……...116
3.5.4.2 Disponibilidad……116
3.5.4.3 Integridad……116
3.5.5 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE ACCESOS.....117
3.5.5.1 Recepción de la solicitud de acceso……....117
3.5.5.2 Verificación de la solicitud de acceso……..117
3.5.5.3 Autorización de la solicitud de acceso……..117
3.5.5.4 Ejecución de acceso……...117
3.5.5.5 Notificación de acceso……..118
3.5.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE ACCESO 118
3.6 PROCESO DE GESTIÓN DE CAMBIOS……119

3.6.1 OBJETIVO 119
3.6.2 ALCANCE 119
3.6.3 DEFINICIONES.....119
3.6.3.1 Cambio……...119
3.6.3.2 Cambio Normal……119
3.6.3.3 Cambio Standard……119
3.6.3.4 Cambio Emergente……..119
3.6.3.5 RFC (Request For change) ……...120
3.6.3.6 Registro de cambios……120
3.6.3.7 Propuesta de cambio……120
3.6.3.8 Plan de recuperación (*rollback*) ……120
3.6.4 RESPONSABLE 120
3.6.5 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS NORMAL 120
3.6.5.1 Recepción de propuestas del cambio……...120
3.6.5.2 Creación de RFC……121
3.6.5.3 Aprobación del RFC……121
3.6.5.4 Asignación de recursos……..122
3.6.5.5 Implementación del Cambio……...122
3.6.6 DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS NORMAL 123
3.6.7 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EMERGENTE 124
3.6.7.1 Planificación y asignación de recursos……124
3.6.7.2 Autorización del cambio……..124
3.6.7.3 Implementación del cambio……124
3.6.8 DIAGRAMA DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EMERGENTE 125
3.6.9 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS ESTÁNDAR 125
3.6.9.1 Revisión y Análisis del cambio……126

3.6.9.2 Autorización del cambio……..126
3.6.9.3 Notificación e Implementación del Cambio……..126
3.6.10 DIAGRAMA DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EMERGENTE 127
3.7 EJEMPLOS DE APLICACIÓN DE LOS PROCESOS PLANTEADOS AL ÁREA DE O&M IP/MPLS……..127
3.7.1 EJEMPLO 1 127
3.7.1.1 Paso 1 (Gestión de eventos) …….....127
3.7.1.2 Paso 2 (Gestión de eventos) ……..…....128
3.7.1.3 Paso 3 (Gestión de eventos) ……128
3.7.1.4 Paso 4 (Gestión de eventos) ……128
3.7.1.5 Paso 5 (Gestión de eventos) ……128
3.7.1.6 Paso 6 (Gestión de incidentes NOC) ……....128
3.7.1.7 Paso 7 (Gestión de incidentes NOC) ……..…..129
3.7.1.8 Paso 8 (Gestión de incidentes MPLS) ……129
3.7.1.9 Paso 9 (Gestión de incidentes MPLS) ……129
3.7.1.10 Paso 10 (Gestión de cambio emergente) ……..129
3.7.1.11 Paso 11 (Gestión de cambio emergente) ……..129
3.7.1.12 Paso 12 (Gestión de cambio emergente) ……..129
3.7.1.13 Paso 13 (Gestión de incidentes MPLS) ……130
3.7.1.14 Paso 14 (Gestión de incidentes NOC) ……...130
3.7.1.15 Paso 15 (Gestión de incidentes NOC) ……...130
3.7.1.16 Paso 16 (Gestión de incidentes NOC) ……..130
3.7.1.17 Paso 17 (Gestión de Problemas) ……130
3.7.1.18 Paso 18 (Gestión de Problemas) ……131
3.7.1.19 Paso 19 (Gestión de Problemas) ……131
3.7.1.20 Paso 20 (Gestión de Problemas) ……131
3.7.1.21 Paso 21 (Gestión de cambios normal) ……...131
3.7.1.22 Paso 22 (Gestión de cambios normal) ……...134
3.7.1.23 Paso 23 (Gestión de cambios normal) ……...134
3.7.1.24 Paso 24 (Gestión de cambios normal) ……...134
3.7.1.25 Paso25 (Gestión de cambios normal) ……134

3.7.1.26 Paso 26(Gestión de cambios normal) ……134
3.7.1.27 Paso 27 (Gestión de cambios normal) ……...134
3.7.1.28 Paso 28 (Gestión de cambios normal) ……...135
3.7.2 EJEMPLO 2 135
3.7.2.1 Paso 1 (Gestión de incidentes NOC) ……135
3.7.2.2 Paso 2 (Gestión de incidentes NOC) ……135
3.7.2.3 Paso 3 (Gestión de incidentes NOC) ……135
3.7.2.4 Paso 4 (Gestión de incidentes NOC) ……135
3.7.2.5 Paso 5 (Gestión de incidentes NOC) ……136
3.7.2.6 Paso 6 (Gestión de incidentes NOC) ……136
3.7.2.7 Paso 7 (Gestión de incidentes NOC) ……136
3.7.2.8 Paso 8. (Gestión de incidentes NOC) ……136
3.7.3 EJEMPLO 3 136
3.7.3.1 Paso 1 (Gestión de Acceso) ……137
3.7.3.2 Paso 2 (Gestión de Acceso) ……137
3.7.3.3 Paso 3 (Gestión de Acceso) ……137
3.7.3.4 Paso 4 (Gestión de Acceso) ……137
3.7.3.5 Paso 5 (Gestión de Acceso) ……137
3.7.4 EJEMPLO 4 138
3.7.4.1 Paso 1 (Gestión de Consultas) ……138
3.7.4.2 Paso 2 (Gestión de Consultas) ……138
3.7.4.3 Paso 3 (Gestión de Cambio Estándar) ……...138
3.7.4.4 Paso 4 (Gestión de Consultas) ……139
3.7.4.5 Paso 5 (Gestión de Consultas) ……139
3.7.5 EJEMPLO 5 139
3.7.5.1 Paso 1 (Gestión de Eventos) ……...139
3.7.5.2 Paso 2 (Gestión de Eventos) ……...139
3.7.5.3 Paso 3 (Gestión de Eventos) ……...139
3.7.5.4 Paso 4 (Gestión de Eventos) ……...139
3.7.5.5 Paso 5 (Gestión de Eventos) ……...140
3.7.5.6 Pase 6. (Gestión de Incidentes) ……..140
3.7.5.7 Paso 7 (Gestión de Incidentes NOC) ……140

3.7.5.8 Paso 8 (Gestión de Incidentes MPLS) ……...141
3.7.5.9 Paso 9. (Gestión de Incidentes MPLS) ……..141
3.7.5.10 Paso 10 (Gestión de Incidentes MPLS) ……141
3.7.5.11 Paso 11. (Gestión de Incidentes MPLS) ……141
3.7.5.12 Paso 12 (Gestión de Incidentes MPLS) ……141

CAPÍTULO 4 142

4 PLAN DE MEJORA CONTINUA DE LOS PROCESOS DEL ÁREA DE O&M DE CNT E.P. 142

4.1 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE EVENTOS… 142

4.1.1 METAS 142

4.1.2 INDICADORES DE RENDIMIENTO 142

4.1.3 ANÁLISIS DE DATOS 143

4.1.4 RECOMENDACIONES DE MEJORA CONTINUA 144

4.2 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE INCIDENTES…… 145

4.2.1 METAS 145

4.2.2 INDICADORES DE RENDIMIENTO 145

4.2.3 ANÁLISIS DE DATOS 146

4.2.4 RECOMENDACIONES DE MEJORA CONTINUA 147

4.3 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE PROBLEMAS ……...148

4.3.1 METAS 148

4.3.2 INDICADORES DE RENDIMIENTO 148

4.3.3 ANÁLISIS DE DATOS 149

4.3.4 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE PROBLEMAS 149

4.4 MEJORA CONTINUA DE GESTIÓN DE ACCESOS……150

4.4.1 METAS 150

4.4.2 INDICADORES DE RENDIMIENTO 150
4.4.3 ANÁLISIS DE DATOS.....151
4.4.4 RECOMENDACIONES DE MEJORA CONTINUA.....153
4.5 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE CONSULTAS……153
4.5.1 METAS.....153
4.5.2 INDICADORES DE RENDIMIENTO 153
4.5.3 ANÁLISIS DE DATOS.....154
4.5.4 RECOMENDACIONES DE MEJORA CONTINUA.....154
4.6 MEJORA CONTINUA DE CAMBIOS……154
4.6.1 METAS.....154
4.6.2 INDICADORES DE RENDIMIENTO 155
4.6.3 ANÁLISIS DE DATOS.....155
4.6.4 RECOMENDACIONES DE MEJORA CONTINUA.....156

CAPÍTULO 5.....157
5 CONCLUSIONES Y RECOMEDACIONES 157
5.1 CONCLUSIONES…….....157
5.2 RECOMENDACIONES……159
6 REFERENCIAS BIBLIOGRÁFICAS.....162

ANEXOS.....165

ÍNDICE DE FIGURAS

Figura 1.1 Elementos de un proceso 2
Figura 1.2 Componentes de Gobierno de TI 4
Figura 1.3 Dominios de COBIT 4.1 7
Figura 1.4 Procesos del dominio de Entrega y Soporte de COBIT 4.1 9
Figura 1.5 Ciclo de vida ITIL y sus elementos de trabajo 16
Figura 1.6 Actividades de la gestión de Problemas Reactiva 34
Figura 1.7 Actividades de la Gestión de Acceso 37
Figura 1.8 Siete pasos del proceso de mejora 40
Figura 2.1 Organigrama del área O&M de la Plataforma IP MPLS 47
Figura 2.2 Elementos de red 50
Figura 2.3 Vista gráfica integral de la topología de Azogues 50
Figura 2.4 Vista de las alarmas generadas en Cisco Prime Network Events 51
Figura 2.5 Vista de los elementos de red agregados en la herramienta 52
Figura 2.6 Monitoreo del tráfico de un enlace mediante la herramienta Cacti 52
Figura 2.7 Vista de la pantalla de inicio de la herramienta ACS 53
Figura 2.8 Usuarios creados en el ACS 53
Figura 2.9 Grupos de Usuarios definidos en el ACS 54
Figura 2.10 Tiempo de vida de las contraseñas 55
Figura 2.11 Vista de los tickets pendientes de resolución 55
Figura 2.12 Matriz de Riesgo 59
Figura 2.13 Criterios de Información del proceso de Administración de Seguridad según COBIT 4.1 65
Figura 2.14 Recursos asignados por COBIT 4.1 del proceso de Administración de Seguridad 65
Figura 2.15 Criterios de Información del proceso de Administración de Problemas según COBIT 4.1..... 75
Figura 2.16 Recursos asignados por COBIT 4.1 del proceso de Administración de problemas..... 75
Figura 2.17 Criterios de Información del proceso de Administración de Incidentes y *Service Desk* según COBIT 4.1..... 84

Figura 2.18 Recursos asignados por COBIT 41 del proceso de Administración de Incidentes y *Service Desk* 84
Figura 3.1 Diagrama del Proceso de Gestión de eventos 98
Figura 3.2 Procedimiento de Gestión de Incidentes NOC 104
Figura 3.3 Procedimiento de resolución de incidentes MPLS 106
Figura 3.4 Procedimiento de Resolución de Incidente Crítico 107
Figura 3.5 Procedimiento de Cierre de Incidentes 108
Figura 3.6 Diagrama de flujo del proceso de Gestión de Problemas 112
Figura 3.7 Proceso de Gestión de Consultas 115
Figura 3.8 Proceso de gestión de acceso 118
Figura 3.9 Procedimiento de gestión de cambios normal 123
Figura 3.10 Diagrama del procedimiento de gestión de cambios emergente 125
Figura 3.11 Procedimiento de Gestión de cambios estándar 127
Figura 3.12 Ejemplo de alarma crítica 128
Figura 3.13 Pruebas de primer nivel en los equipos A y B 136
Figura 3.14 Gráfico de caída de tráfico en el CACTI 140
Figura 4.1 Porcentaje de aparición de alertas en la herramienta ACS 152
Figura 4.2 Cambios y Mantenimientos Preventivos 156

ÍNDICE DE TABLAS

Tabla 1.1 Cálculo de la Prioridad 30
Tabla 1.2 Tiempos de resolución de Incidentes 30
Tabla 1.3 COBIT 4.1 alineado a ITIL V3 45
Tabla 2.1 División en regiones de la red MPLS..... 48
Tabla 2.2 Representación y significado de alarmas en Cisco Prime..... 51
Tabla 2.3 Áreas de enfoque del gobierno de TI alineadas al marco de trabajo COBIT 4.1 56
Tabla 2.4 Criterios de Información de COBIT 4.1..... 57
Tabla 2.5 Recursos de TI según COBIT 4.1..... 57
Tabla 2.6 Porcentaje de calificación de desempeño 58
Tabla 2.7 Probabilidad de ocurrencia de un incidente 58
Tabla 2.8 Impacto sobre el servicio en caso de que ocurra el incidente 59
Tabla 2.9 Valoración de Riesgo 60
Tabla 2.10 Criterios para calificación del nivel de madurez 61
Tabla 2.11 Roles de la matriz RACI 61
Tabla 2.12 Matriz de disparadores de valor del proceso de seguridad 64
Tabla 2.13 Ejemplo 1 de calificación de nivel de cumplimiento..... 66
Tabla 2.14 Ejemplo 2 de calificación de nivel de cumplimiento..... 68
Tabla 2.15 Matriz de desempeño de los procesos de control de seguridad..... 69
Tabla 2.16 Matriz de Riesgo del proceso de administración de seguridad 71
Tabla 2.17 Matriz RACI del proceso de Administración de Seguridad..... 72
Tabla 2.18 Nivel de Madurez del proceso de administración de seguridad 73
Tabla 2.19 Matriz de valor del proceso de problemas..... 74
Tabla 2.20 Ejemplo 1 de calificación de nivel de cumplimiento..... 76
Tabla 2.21 Ejemplo 2 de calificación de nivel de cumplimiento..... 78
Tabla 2.22 Matriz de desempeño de los procesos de control de problemas..... 79
Tabla 2.23 Matriz de Riesgo del proceso de administración de Problemas 80
Tabla 2.24 Matriz RACI del Proceso de Administración de Problemas..... 81
Tabla 2.25 Nivel de Madurez del proceso de administración de problemas 82
Tabla 2.26 Matriz de valor del proceso de incidentes y *service desk*..... 83

Tabla 2.27 Ejemplo 1 de calificación de nivel de cumplimiento Administración incidentes y *service desk* 86
Tabla 2.28 Ejemplo 2 de calificación de nivel de cumplimiento Administración incidentes y *service desk* 87
Tabla 2.29 Matriz de desempeño de los procesos de control de incidentes y *service desk* 88
Tabla 2.30 Matriz de Riesgo del proceso de administración de incidentes y *service desk* 90
Tabla 2.31 Matriz RACI del proceso de administración de incidentes y *service desk* 91
Tabla 2.32 Modelo de Madurez del proceso de administración de incidentes y *service desk* 92
Tabla 3.1 Alarmas Cisco Prime 96
Tabla 3.2 Significancia del evento correspondiente a las alarmas de Cisco Prime 96
Tabla 3.3 Correlación de alarmas Cisco Prime 97
Tabla 3.4 Criterios de categorización del incidente 101
Tabla 3.5 Matriz Urgencia Impacto 102
Tabla 3.6 Tiempo de solución en base a la prioridad 103
Tabla 3.7 Servicios afectados durante el mantenimiento 132
Tabla 3.8 Resumen de actividades durante el mantenimiento 133
Tabla 3.9 Matriz de pruebas y validaciones 133
Tabla 3.10 Roles y responsables en el mantenimiento 134
Tabla 4.1 Porcentaje de intentos fallidos de acceso a la red 152

RESUMEN

El presente proyecto tiene como objetivo conocer el estado actual de los procesos internos del área de operación y mantenimiento de las plataformas IP MPLS de la Corporación Nacional de Telecomunicaciones CNT E.P., la cual es una empresa dedicada a entregar servicios de telecomunicaciones, para después normalizar los procesos auditados mediante las prácticas de ITIL V3.

En el primer capítulo se presenta el estudio de los componentes de un proceso y su levantamiento, también se analiza los dominios de garantía de seguridad de sistemas (DS5), administración de incidentes y consultas (DS8) y administración de problemas (DS10) del marco de trabajo COBIT 4.1, adicionalmente se describen los procesos y componentes de las etapas de operación y mejora continua del servicio del ciclo de vida de las prácticas ITIL.

En el segundo capítulo se detalla la situación actual del área y se muestran los resultados obtenidos de la auditoría mediante matrices de desempeño, valor, riesgo y responsabilidades, en base a las cuales se obtiene el nivel de madurez de cada proceso aplicando los dominios estudiados en el capítulo 1 del marco de trabajo COBIT 4.1.

En el tercer capítulo, se normalizan los procesos obtenidos de la auditoría y se crean aquellos que son necesarios para complementar la fase de operación del servicio, seguidamente se presentan los diagramas de flujo guía de cada proceso basados en las prácticas ITIL v3.

En el cuarto capítulo, se presenta el plan de mejora continua, mismo que detalla las metas a alcanzar con sus correspondientes indicadores que permitirán medir el desempeño de cada proceso y ser analizados para mejorar el rendimiento de los mismos.

Finalmente en el quinto capítulo se detallan las conclusiones y recomendaciones obtenidas durante el desarrollo del presente proyecto.

PRESENTACIÓN

Las tecnologías de la información actualmente representan una parte esencial para el desarrollo de las empresas, por lo cual para su gestión es indispensable proyectar una guía de procesos, en los cuales fundamentarse para brindar servicios sin perder de vista los objetivos del negocio.

Para una organización que ofrece servicios de telecomunicaciones el área de operaciones es una de las más importantes ya que de ésta depende la prestación efectiva de los servicios. Para cumplir con el máximo índice de disponibilidad es necesario gestionar de forma oportuna los eventos para evitar y disminuir incidentes que afecten la operación normal del servicio y al mismo tiempo encontrar la causa raíz de éstos para tomar una acción que brinde una solución definitiva sin perder de vista la gestión de accesos a los elementos de red para guardar la seguridad de la información además de cumplir con las consultas de las áreas dependientes.

Dado que el área de operación y mantenimiento de las plataformas IP MPLS de la Corporación Nacional de Telecomunicaciones CNT E.P. requiere un plan que permita la organización de sus procesos para optimizar la calidad de los servicios es necesario aplicar un marco de trabajo referencial y buenas prácticas que brinden una guía para cumplir con este objetivo.

COBIT 4.1 es un marco de trabajo que brinda una guía para medir el nivel de madurez de los procesos y determinar las falencias que deben solventarse para corregirlas, por este motivo se lo ha utilizado para conocer el estado actual del área de O&M, para posteriormente aplicar el conjunto de prácticas ITIL las cuales permiten plantear procesos que darán lugar a la mejora de la calidad de los servicios.

Por lo descrito anteriormente, se estructuran los procesos de operación de manera clara y eficaz enfocada en los objetivos de la organización para llevar un control adecuado de éstos, lo cual permitirá que el personal del área O&M tenga

un conocimiento claro de las actividades que deben realizar y sus responsabilidades para brindar una cultura de utilización de procesos que mejorará la eficiencia de trabajo.

CAPÍTULO 1

MARCO TEÓRICO

En este capítulo se presentará un breve estudio de los componentes de un proceso y cómo éste debe ser levantado.

También se revisará COBIT[1] 4.1, principalmente se analizarán los dominios de Garantía de Seguridad de Sistemas (DS5) y Administración de problemas (DS10) pues estos serán utilizados para realizar la auditoría que permitirá determinar la situación actual del área de Operación y Mantenimiento de la red IP[2]/MPLS[3] de la Corporación Nacional de Telecomunicaciones CNT E.P.

Posteriormente, se realizará una revisión de las prácticas ITIL[4] haciendo énfasis en las fases de Operación y Mejora Continua del Servicio de ITIL v3 edición 2011 ya que éstas serán utilizadas para la normalización de los procesos obtenidos mediante la auditoría.

1.1 LEVANTAMIENTO DE PROCESOS

Un proceso es un conjunto de procedimientos que se encuentran interrelacionados y se desarrollan cronológicamente para la consecución de una serie de objetivos, estos se forman por tareas que especifican cómo ejecutar un trabajo [1].

1.1.1 GESTIÓN ENFOCADA EN PROCESOS

La gestión enfocada en procesos tiene como objetivo relacionar las actividades y recursos necesarios para facilitar que la organización cubra las necesidades del cliente y sus expectativas prestando los servicios ofrecidos de manera eficaz y eficiente [2].

---

[1] COBIT (*Control Objectives for Information Systems and related Technology*)
[2] IP (*Internet Protocol*)
[3] MPLS (*MultiProtocol Label Switching*)
[4] ITIL (*Information Technology Infrastructure Library*)

1.1.2 ELEMENTOS DE UN PROCESO [2]

En la **Figura 1.1** se observan los elementos de un proceso

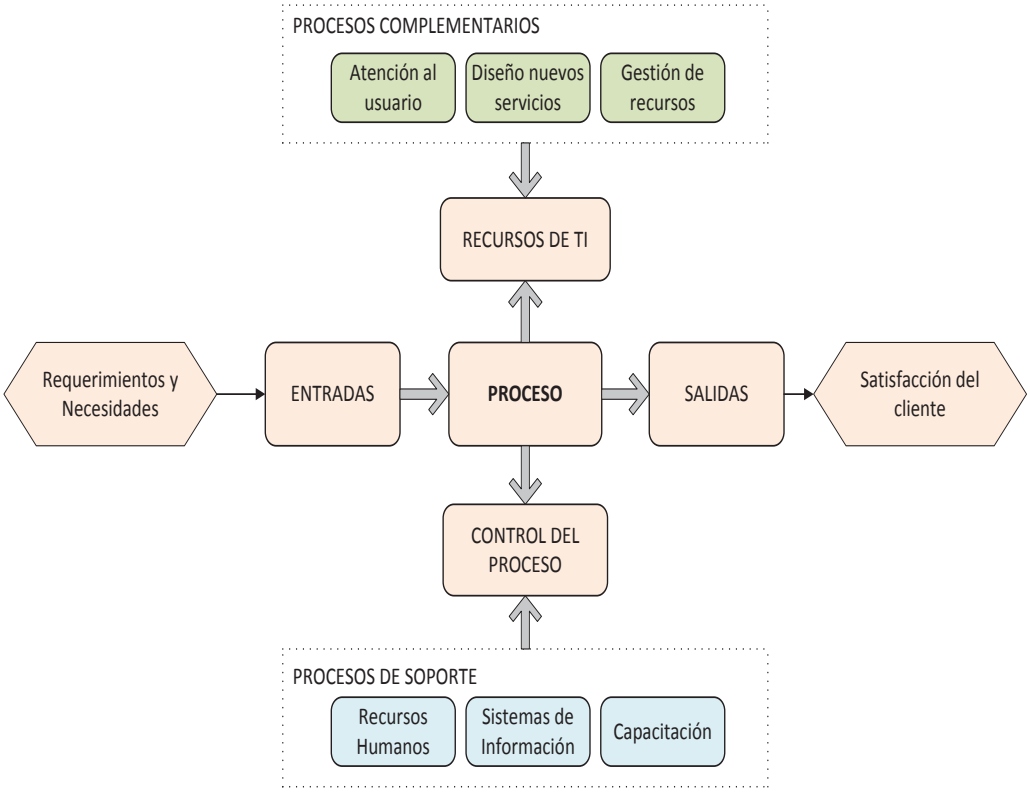


Figura 1.1 Elementos de un proceso [2]

Entradas.- Requisitos y necesidades iniciales del destinatario final para comenzar con el desarrollo del proceso.

Salidas.- Producto o servicio destinado para el cliente interno o externo. Frecuentemente la salida de un proceso corresponde a la entrada del siguiente, lo cual permite complementar cada etapa.

Control del proceso.- Se basa en indicadores y metodologías aplicados a los procedimientos establecidos de manera eficiente para lograr el objetivo del proceso.

Recursos.- Medios e insumos necesarios para desarrollar el proceso.

1.1.3 CLASIFICACIÓN DE PROCESOS [2]

1.1.3.1 Procesos sustantivos

Conjunto de actividades mutuamente relacionadas que interactúan directamente para satisfacer las necesidades del cliente o usuario, sin estos procesos existiría ausencia del servicio.

Estos procesos son esenciales en la formulación de la visión institucional y proporcionan directrices a todos los demás procesos.

1.1.3.2 Procesos complementarios

Permiten desplegar las estrategias y objetivos de la organización para agregar valor al proceso inicial. Guardan relación directa con los usuarios y tienen impacto sobre su satisfacción.

1.1.3.3 Procesos de soporte

Gestionan los recursos para la ejecución de los procesos sustantivos y complementarios.

1.1.4 PASOS PARA LEVANTAR UN PROCESO [2]

A continuación se detallan los pasos principales para el levantamiento de un proceso:

- Formación del equipo y planificación del trabajo.
- Identificación de usuarios de los procesos y sus necesidades.
- Identificación del objetivo y alcance del proceso.
- Identificación del (os) responsable (s) del proceso.
- Identificación de los procedimientos y actividades.
- Priorización y aprobación de los procesos.
- Difusión de los procesos.
- Aplicación y control de los procesos.
- Mejoramiento continuo de los procesos.

1.2 GOBIERNO DE TI [3]

ITGI[5] fue creado por ISACA[6] en 1998 con el propósito de ofrecer una guía de trabajo a las organizaciones a través de la asistencia a los dirigentes corporativos en su responsabilidad para lograr que TI apoye en forma exitosa en la misión y los objetivos de la empresa, mediante investigaciones en gobierno de TI.

El gobierno de TI tiene como objetivo principal alinear las operaciones de TI de la organización con sus estrategias y metas de negocio, de tal manera que las metas comerciales se logren a través del desarrollo y mantenimiento de un control efectivo de TI.

El gobierno de TI consta de estructuras y procesos que aseguran que la organización de TI pueda sostener y ampliar los objetivos y estrategias de la organización.

1.2.1 COMPONENTES DE GOBIERNO DE TI [4]

En la Figura 1.2 se presentan los componentes del gobierno de TI:

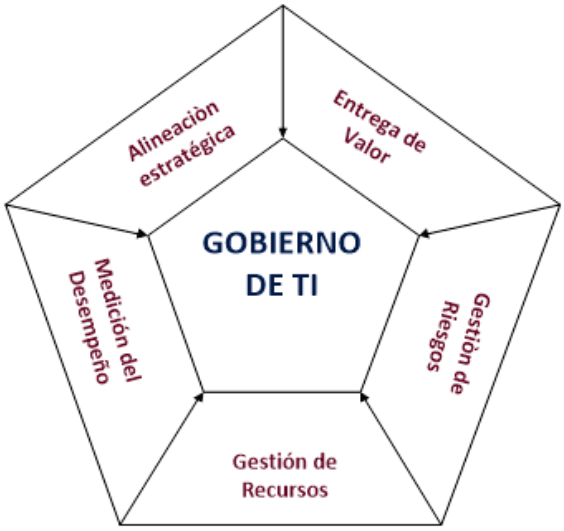


Figura 1.2 Componentes de Gobierno de TI [3]

[5] ITGI (*IT Governance Institute*)
[6] ISACA (*Information Systems Audit and Control Association*)

A continuación se muestran las definiciones utilizadas por COBIT para los componentes del gobierno de TI:

1.2.1.1 Alineación estratégica

Se enfoca en garantizar el vínculo entre los planes de las entidades de negocio y de TI; además tiene como objetivos principales definir, mantener y validar la propuesta de valor de TI, y en alinear las operaciones de TI con las operaciones de la empresa.

1.2.1.2 Entrega de valor

Este componente se refiere a ejecutar la propuesta de valor a lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la alineación estratégica, concentrándose en optimizar los costos y en brindar el valor intrínseco de TI.

1.2.1.3 Administración de riesgos

Requiere conciencia de la existencia de riesgos por parte de los altos ejecutivos de la empresa, para este motivo es necesario comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

1.2.1.4 Administración de recursos

Se trata de la inversión óptima por parte de la organización para una correcta capacidad técnica, así como de la administración adecuada de los recursos críticos de TI los cuales son:

- Aplicaciones.
- Información.
- Infraestructura.
- Personas.

1.2.1.5 Medición del desempeño

Rastrea y monitorea la estrategia de implementación, la finalización del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio para lograr las metas que se puedan medir más allá del registro convencional. Un gobierno efectivo de TI debe asegurar que TI se acople a los objetivos del negocio, maximice las inversiones del negocio en TI, y gestione apropiadamente las oportunidades y los riesgos relacionados a TI.

1.3 COBIT [3]

COBIT promueve un marco de control de gobierno de TI autorizado y reconocido internacionalmente, mismo que tiene como propósito concentrarse en la información que se necesita para apoyar los objetivos y metas del negocio mediante el uso de los elementos de tecnología de la información [5].

Inicialmente COBIT fue desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) en respuesta a una necesidad percibida de un marco para el control interno del gobierno de TI, en 1998 la segunda edición añade guías para gestionar los procesos. Después en el 2000 el ITGI lanzó la tercera edición de COBIT; consecuentemente la cuarta edición se publicó en 2005 y su edición en 2007 fue presentado como COBIT 4.1.

La quinta edición de COBIT fue publicada en el año 2012, se desarrolló mediante la consolidación e integración de COBIT 4.1, VAL IT[7] y RISK IT[8].

En el desarrollo del presente proyecto la investigación se enfoca en COBIT 4.1 con el objetivo de medir el nivel de madurez de los procesos internos del área de operación y mantenimiento de la red IP MPLS de la Corporación Nacional de Telecomunicaciones CNT E.P. y se plantearán metas orientadas al servicio mas no al negocio, por lo cual no se aplicarán los factores añadidos a COBIT 5.

---

[7] VAL IT (*Value of Infomation Technology*): marco enfocado en el manejo de la cartera de inversiones de TI.
[8] RISK IT (*Risk of Information Technology*): marco de trabajo enfocado en la gestión de riesgos de negocio relacionados con TI.

En la Figura 1.3 se pueden observar los cuatro dominios que contempla COBIT 4.1:

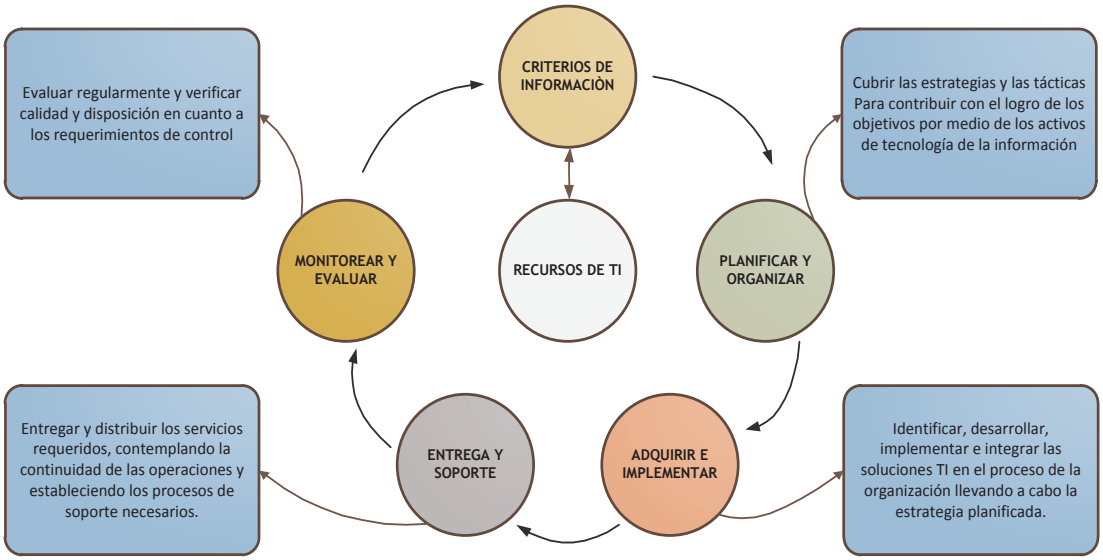


Figura 1.3 Dominios de COBIT 4.1 [3]

1.3.1 DOMINIOS DE COBIT 4.1

1.3.1.1 Planeación y organización

Este dominio cubre la planeación de estrategias y tácticas con el propósito de que la tecnología de información pueda contribuir al logro de los objetivos del negocio.

La visión de planeamiento estratégico de la organización requiere ser comunicada y administrada desde diferentes perspectivas. Adicionalmente, se debe establecer una organización y una infraestructura tecnológica que vaya de la mano de los objetivos trazados inicialmente.

1.3.1.2 Adquisición e implementación

Para llevar a cabo la organización y planeación de las estrategias de TI, las soluciones deben ser identificadas adquiridas o desarrolladas, así como implementadas e integradas dentro del proceso del negocio. Contempla también, los cambios y el mantenimiento de sistemas existentes, para garantizar continuidad en el ciclo de vida.

1.3.1.3 Entrega y soporte

Este dominio se enfoca en la prestación y distribución de los servicios requeridos, abarca las operaciones para brindar los mismos, tomando en cuenta la seguridad en los sistemas y la continuidad de las operaciones.

Adicionalmente incluye el procesamiento de los datos el cual es ejecutado por los sistemas de aplicación, frecuentemente clasificados según las necesidades del área donde se emplean y administran.

Con el fin de proveer servicios a los usuarios, este dominio define que deben establecerse los procesos de soporte necesarios y darles la prioridad adecuada para ser atendidos.

1.3.1.4 Monitoreo y evaluación

Una vez levantados todos los procesos necesitan ser evaluados y monitoreados periódicamente a través del tiempo para verificar su calidad y eficacia en cuanto a los requerimientos de control.

Además este dominio sugiere a la administración sobre la necesidad de asegurar procesos de control independientes, los cuales son provistos por auditorías internas y externas u obtenidas de fuentes alternativas.

1.3.2 CRITERIOS DE INFORMACIÓN DE COBIT 4.1

Los criterios definidos para satisfacer los objetivos del negocio según COBIT son:

- Efectividad.
- Eficiencia.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Cumplimiento.
- Confiabilidad.

1.3.3 PROCESOS COBIT

Los procesos de COBIT 4.1 requieren de un conjunto de objetivos de control que establezcan un puente entre los riesgos, controles, aspectos técnicos del negocio y soporten sus procesos [6].

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar mediante la implementación de procedimientos de control específicos dentro de una actividad de TI.

El control debe incluir prácticas, procedimientos, políticas y estructuras organizacionales.

En la aplicación de este marco de trabajo, es importante asegurar que todos los individuos involucrados en la administración, uso, diseño, desarrollo, mantenimiento u operación de sistemas de información actúen con eficiencia.

En la **Figura 1.4** se resaltan los procesos del dominio de entrega y soporte a ser estudiados y aplicados en el desarrollo de este proyecto.

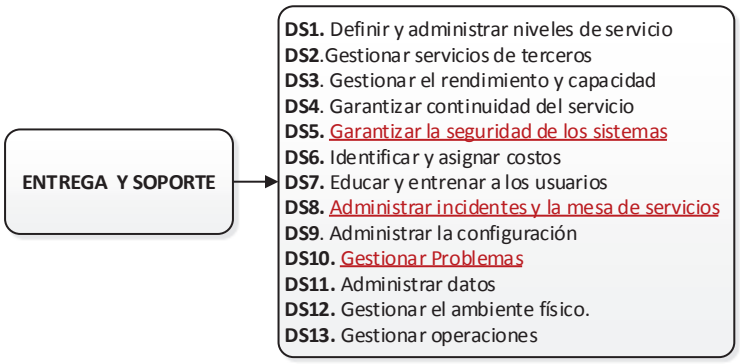


Figura 1.4 Procesos del dominio de Entrega y Soporte de COBIT 4.1 [3]

1.3.3.1 DS5 Garantizar la Seguridad de los Sistemas [3] [7]

Este proceso es creado en base a la necesidad de administrar la seguridad de los elementos de TI fundamentales para el negocio manteniendo la integridad de la información.

Para cumplir con este proceso, COBIT sugiere como parte fundamental establecer y mantener los roles y responsabilidades de TI.

También pide realizar una correcta gestión de seguridad mediante un monitoreo regular y toma de acciones correctivas sobre posibles incidentes identificados que afecten a la seguridad causando la indisponibilidad del servicio.

COBIT denomina como una efectiva administración de seguridad al proceso que protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

A continuación se describen los objetivos de control del proceso DS5.

1.3.3.1.1 *DS5.1 Administración de la Seguridad de TI*

Gestionar la seguridad de TI en un nivel eficiente y apropiado para la organización que se encuentre alineado con los objetivos del negocio.

1.3.3.1.2 *DS5.2 Plan de Seguridad de TI*

Garantizar un plan completo basado en políticas y procedimientos de seguridad tomando en cuenta los riesgos y requerimientos del negocio.

1.3.3.1.3 *DS5.3 Administración de Identidad*

Asegurar que se asignen a todos los usuarios derechos de acceso relacionados con las actividades de la organización para que se autentiquen de manera única bajo la administración del responsable de este procedimiento, tomando en cuenta el tiempo que el usuario opere en el sistema.

1.3.3.1.4 *DS5.4 Administración de Cuentas de Usuario*

Establecer un conjunto de procedimientos para emitir, modificar, suspender, y cerrar cuentas de todos los usuarios relacionados con la operación de la organización así como también la administración de privilegios de dichas cuentas basados en políticas de seguridad establecidas.

1.3.3.1.5 *DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad*

Monitorear de manera proactiva la operación de seguridad para garantizar que se cumple con el nivel inicialmente aprobado y detectar actividades inusuales para luego corregirlas.

1.3.3.1.6 *DS5.6 Definición de Incidente de Seguridad*

Caracterizar los incidentes de seguridad potenciales para que sean tratados por el proceso de gestión de incidentes y problemas.

1.3.3.1.7 *DS5.7 Protección de la Tecnología de Seguridad*

Proteger la integridad de la información contenida en la tecnología.

1.3.3.1.8 *DS5.8 Administración de Llaves Criptográficas*

Implementar llaves criptográficas y su proceso de administración para garantizar la protección contra divulgación y modificaciones no autorizadas.

1.3.3.1.9 *DS5.9 Prevención, Detección y Corrección de Software Malicioso*

Establecer parámetros para proteger la integridad de los sistemas de TI y prevenir los daños causados por cualquier tipo de malware.

1.3.3.1.10 *DS5.10 Seguridad de la Red*

Controlar los flujos de información de entrada y salida de la red apoyados en técnicas de seguridad como por ejemplo los dispositivos de seguridad.

1.3.3.1.11 *DS5.11 Intercambio de Datos Sensitivos*

Controlar el intercambio de datos para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

1.3.3.2 DS8 Administrar la Mesa de Servicio y los Incidentes.

El objetivo de este dominio es brindar un soporte efectivo según lo requieran los usuarios y en el tiempo adecuado. Para esto es importante diseñar procesos para

la ejecución de consultas y resolución de incidentes definiendo tareas para las actividades de: escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución.

1.3.3.2.1 *DS8.1 Mesa de Servicios*

Establecer la función de mesa de servicio para cumplir con los requerimientos de servicio y solicitudes de información de los usuarios, para lograr este objetivo deben existir procedimientos de monitoreo y escalamiento basados en los SLAs[9] establecidos.

1.3.3.2.2 *DS8.2 Registro de Consultas de Clientes*

Establecer un sistema que permita la administración ligada a los procesos de incidentes, solicitudes de servicio, consultas, administración de problemas, administración de cambios administración de capacidad y administración de disponibilidad.

1.3.3.2.3 *DS8.3 Escalamiento de Incidentes*

Establecer un proceso que detalle criterios de escalamiento basados en las limitaciones del SLA en caso de que no puedan ser resueltos por la mesa de servicios.

1.3.3.2.4 *DS8.4 Cierre de Incidentes*

Establecer procedimientos de seguimiento de la resolución de los incidentes. Se debe registrar la causa raíz que ocasionó el incidente y las acciones tomadas para solucionarlo.

1.3.3.2.5 *DS8.5 Análisis de Tendencias*

Presentar informes de las actividades realizadas en el *service desk* para medir el desempeño e identificar problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

---

[9] SLA (*Service Level Agreement*): es un documento que se define para entablar la relación de la provisión del servicio con el cliente.

1.3.3.3 DS10 Administración de Problemas

Identificar y clasificar problemas para luego ser analizados con el objetivo de encontrar la causa raíz que los ocasiona y su solución para luego ser utilizadas en la mejora continua del servicio.

1.3.3.3.1 *DS10.1 Identificación y Clasificación de Problemas*

Establecer procesos y definir pasos para clasificar e identificar problemas que surgen como parte de la gestión de incidentes. Dentro del proceso se tomará en cuenta criterios de categorización y priorización especificados en los incidentes.

1.3.3.3.2 *DS10.2 Rastreo y Resolución de Problemas*

Para cumplir con un proceso eficiente de Identificación y clasificación de problemas y brindar soluciones sostenibles se deben considerar:

- Todos los elementos de configuración asociados
- Problemas e incidentes sobresalientes
- Errores conocidos y sospechados
- Seguimiento de las tendencias de los problemas.

Se debe monitorear continuamente el impacto de los problemas y errores conocidos sobre los servicios que se brinda a los usuarios para tomar acciones según la medida del impacto.

1.3.3.3.3 *DS10.3 Cierre de Problemas*

Detallar el procedimiento para cerrar los problemas después de confirmar una solución haciendo uso de un error conocido.

1.3.3.3.4 *DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas*

Integrar los procesos de administración de cambios, configuración y problemas para administrar incidentes y problemas de forma correcta. Se debe monitorear

los tiempos aplicados para brindar soluciones y minimizarlos mejorando los procesos involucrados en la solución.

1.3.4 MODELO DE MADUREZ

El marco de trabajo COBIT provee un Modelo de Madurez para el control y evaluación de la capacidad sobre los procesos de TI de tal forma que la administración tenga:

- Una medida coherente de dónde está la organización.
- Fundamentos para decidir eficientemente planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.
- Una herramienta para medir el progreso con respecto al objetivo.

También se necesita analizar, en base a los impulsores de riesgo y de valor, cuáles mecanismos de control se debe aplicar [7].

1.3.5 MATRIZ RACI

La matriz de asignación de responsabilidades es una herramienta versátil donde se específica el grado de responsabilidad de los recursos (personas, grupos, roles) asignados para relacionar entregables o actividades con respecto al proyecto.

De esta manera se asegura que cada uno de los componentes del alcance esté asignado a un individuo o equipo de trabajo. Se denomina matriz RACI, por las cuatro letras con las que se codifica el tipo de relación con un proceso que tiene cada agente:

Responsible / Responsable (R).- Se refiere al asignado a cumplir con la tarea o actividad.

Accountable / Persona a cargo (A).- Es la persona responsable de hacer que se cumpla la tarea y se la haga de forma correcta.

Consulted / Consultado (C).- Los recursos con este rol son las personas con las que hay que consultar datos o decisiones con respecto a la actividad o proceso que se define.

Informed / Informado (I).- A estas personas se les informa las decisiones tomadas, resultados que se producen, estados del servicio y grados de ejecución

1.4 ITIL [8]

ITIL[10] es un marco de trabajo de mejores prácticas para la gestión de servicios[11] de TI[12] que describe procesos, funciones y estructuras para la mayoría de áreas de gestión de Servicios. Este marco de trabajo permite a las organizaciones diseñar e implementar sus propios procesos y procedimientos. Se ha desarrollado desde su creación hasta convertirse en el método más aceptado para la gestión de servicios alrededor del mundo.

1.5 CICLO DE VIDA DE LOS SERVICIOS TI MEDIANTE ITIL V3 EDICIÓN 2011 [8]

La estructura de gestión de servicios TI[13] se basa en el ciclo de vida de los servicios, esto permite brindar una clara visión del servicio desde su diseño hasta su abandono, tomando en cuenta los procesos detallados y sus funciones. Este ciclo de vida consta de cinco fases, que son:

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

[10] ITIL (*Information Technology Infrastructure Library*)
[11] Servicio: es un medio para entregar valor a los clientes, brindándoles el resultado esperado sin que tengan que asumir los costos y riesgos correspondientes.
[12] TI (*Tecnología de Información*)
[13] Servicio de TI: es un servicio ofrecido por un proveedor de servicios TI, el servicio TI se compone de la combinación de tecnología de información, personas y proceso.

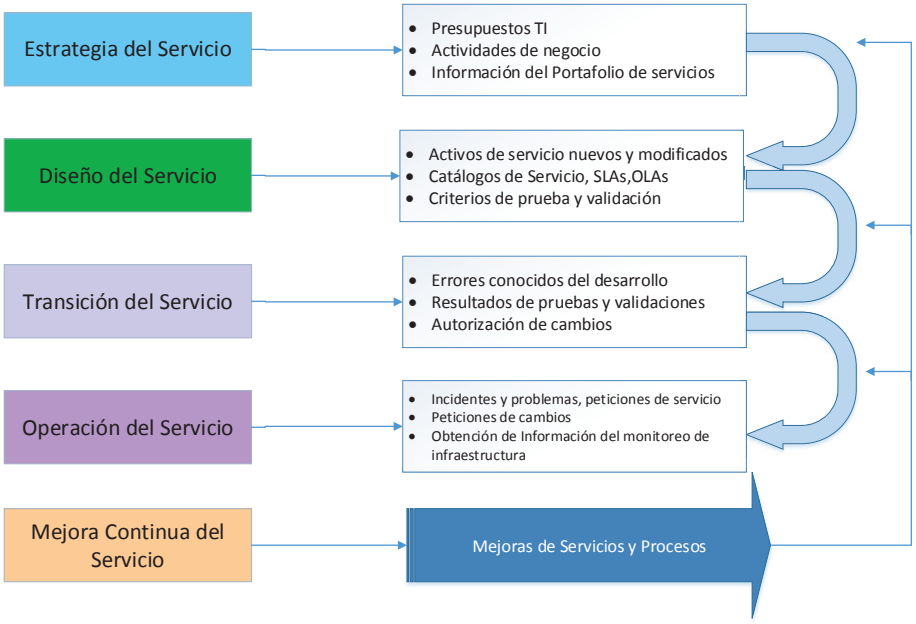


Figura 1.5 Ciclo de vida ITIL y sus elementos de trabajo [8]

De las cinco fases del ciclo de vida ITIL listadas, serán estudiadas detalladamente, la Operación y la Mejora continua del Servicio, pues éstas se utilizarán para el desarrollo del presente proyecto ya que se aplican en las actividades realizadas en el área de Operación y Mantenimiento de la red IP MPLS de la Corporación Nacional de Telecomunicaciones CNT E.P.

Las fases de Estrategia Diseño y Transición del servicio, serán revisadas de forma general.

1.5.1 ESTRATEGIA DEL SERVICIO [8]

La etapa de estrategia del servicio determina las necesidades, prioridades e importancia relativa de los servicios, también se encarga de definir la perspectiva, posición, planes y patrones que un proveedor de servicios de TI[14] debe ejecutar para cumplir con las exigencias de negocio de la organización, además proporciona una guía de cómo enfocar la gestión de servicios como un activo estratégico.

[14] Proveedor de Servicios TI: es una organización que brinda servicios TI a uno o más clientes que pueden ser internos o externos

Los procesos definidos en la Estrategia del servicio son:

- Gestión de la estrategia de los servicios TI.
- Gestión del portafolio de servicios.
- Gestión financiera de servicios TI.
- Gestión de la demanda.
- Gestión de la relación de negocio.

Estos procesos trabajan en conjunto para permitir que una organización incremente el valor de sus servicios.

1.5.2 DISEÑO DEL SERVICIO [8]

El propósito de ésta fase es diseñar los servicios TI en conjunto con las prácticas de gobierno de TI, procesos y políticas para poner en marcha la introducción de nuevos servicios utilizando entornos compatibles que garanticen la calidad en la prestación del servicio y la satisfacción del cliente. Los procesos definidos en la fase de Diseño del Servicio son los siguientes:

- Coordinación del diseño.
- Gestión del catálogo de servicios.
- Gestión de nivel del servicio.
- Gestión de la disponibilidad.
- Gestión de la capacidad.
- Gestión de la continuidad de servicios TI.
- Gestión de la seguridad de información.
- Gestión de proveedores.

1.5.3 TRANSICIÓN DEL SERVICIO [9]

Esta etapa se enfoca en la transición entre las etapas de diseño y operación del servicio. La transición del servicio es fundamental ya que si existen errores técnicos o funcionales y no se encuentran durante esta fase, afectará gravemente al negocio o a la infraestructura TI y será más costoso dar solución durante la

operación del servicio. Los procesos definidos en la fase de Transición del Servicio son los siguientes:

- Planificación y soporte a la transición.
- Gestión de cambios[15].
- Gestión de la configuración y activos de servicio.
- Gestión de entregas y despliegues.
- Validación y pruebas del servicio.
- Evaluación del cambio.
- Gestión del conocimiento.

1.5.3.1 Gestión de Cambios [9]

Este proceso se encarga de controlar el ciclo de vida de los cambios para garantizar que cuando éstos se realicen, se mantenga la continuidad de los servicios.

Se realizan cambios por las siguientes razones:

- Mejorar los servicios.
- Brindar solución a errores conocidos[16].
- Aumentar servicios.

La gestión de cambios debe garantizar que los cambios:

- No perjudiquen la calidad del servicio TI.
- Se justifiquen.
- Se registren, clasifiquen y documenten.
- Sean probados.
- Se puedan deshacer mediante procesos de recuperación (*rollback*)[17] en caso de no ser exitosos.

[15] Cambio: es la adición, modificación o remoción de algo que puede causar un efecto en los servicios TI.
[16] Error conocido: es un problema cuya causa ha sido determinada y documentada

La gestión de cambios se enfoca en los siguientes objetivos:

- Responder a los requerimientos del cliente mientras se maximiza el valor del negocio reduciendo incidentes que provoquen interrupciones del servicio.
- Responder las solicitudes de cambios que alinean los servicios con las necesidades del negocio.
- Asegurar que los cambios sean registrados y evaluados.
- Garantizar que los cambios autorizados se prioricen, planifiquen, documenten, implementen, prueben y se revisen de manera controlada.

Actividades.- las actividades definidas por ITIL dentro del proceso de gestión de cambios son:

- Creación de RFC[18].
- Registro de RFC.
- Revisión inicial para filtrar RFCs.
- Evaluación de RFC (gestor de cambios[19] y comité asesor de cambios).
- Autorización del cambio (gestor de cambios).
- Coordinación de cambios y pruebas.
- Autorización del despliegue del cambio.
- Coordinación del despliegue de cambios.
- Implementación del cambio.
- Revisión de cambios.
- Cierre del registro de cambios.

Modelos de Cambios.- son los cambios que previamente se han clasificado analizado y autorizado para asignar actividades a cada modelo lo que permita implementar efectivamente las RFC planteadas. Los modelos de cambios deben incluir:

---

[17] *Rollback*: Es la reversión de una operación que devuelve a los sistemas a su estado previo.
[18] RFC (*Request for change*): es una propuesta formal que incluye detalles de los cambios que serán realizados.
[19] Gestor de Cambios: es la persona responsable del proceso de Gestión de Cambios

- Los pasos a seguir para gestionar los cambios.
- Roles y responsabilidades.
- Escalas de tiempo y umbrales para acciones.
- Procedimientos de escalamiento[20].
- Plan de recuperación.

ITIL define los siguientes modelos de cambios:

- ***Normal,*** es un cambio que sigue todos los pasos del proceso de cambios, estos serán definidos por el impacto y complejidad, por esta razón se deben escalar a la persona adecuada para realizarlos.

- ***Standard,*** es un cambio pre autorizado, de bajo riesgo, es común y debe seguir un procedimiento. Este cambio incluye reseteo de passwords o aprovisionamiento de equipos para un empleado nuevo.

  Para implementar los cambios estándar, no se requiere el planteamiento de un RFC (*Request For Change*) y se usan diferentes mecanismos para resolverlos, como la petición de servicios.

- ***Emergencia,*** es un cambio que se debe realizar tan pronto como sea posible.

Clasificación de Cambios.- luego de que el cambio se ha aprobado, es necesario asignar la prioridad e impacto al RFC.

El impacto permite determinar la dificultad del cambio, esto se utiliza para la asignación de recursos.

La prioridad se utiliza para diferenciar la importancia entre RFCs y como estos deben ser tratados, se establecen los siguientes niveles de prioridad:

[20] Escalamiento: Es un proceso que se utiliza cuando el Centro de servicios no es capaz de dar soluciones en primera instancia y requiere solicitar el apoyo de un especialista más experimentado.

- ***Baja,*** este cambio puede ser de actualizaciones de software, se puede realizar en conjunto con otros cambios.

- ***Normal,*** estos cambios se realizan si no interfieren a cambios prioritarios, pueden ser menores, significativos y mayores.

- ***Alta,*** estos cambios se asocian a errores conocidos que causan la interrupción de los servicios, por lo cual se deben realizar inmediatamente.

- ***Urgente,*** estos cambios se aplican cuando se requiere resolver problemas que deterioran gravemente la calidad del servicio.

Plan de recuperación.- ningún cambio se debería realizar sin tomar en cuenta las condiciones que podrían causar que este falle, por esto es necesario contar con un plan de recuperación (*rollback*), el mismo que volverá todo a su estado original, especialmente los datos y software; sin embargo, debido a que no todos los cambios son reversibles, es necesario tomar en cuenta una solución alternativa.

1.5.4 OPERACIÓN DEL SERVICIO [10]

El propósito de la etapa de Operación del servicio es coordinar y poner en marcha los procesos necesarios para gestionar y entregar servicios, asegurando que se cumplan los niveles acordados entre la organización y los clientes.

Una vez que los servicios se han puesto en marcha, dentro de esta fase se realiza el monitoreo, control y revisión de los mismos, en caso de que las cosas no vayan bien, debe existir un proceso robusto que permita registrar la falla, resolverla y asegurar que no vuelva a ocurrir.

El personal involucrado en esta etapa, debe contar con procesos y herramientas que les brinden una visión global del funcionamiento del servicio, éstas también deben permitir la detección de fallas que ponen en riesgo la calidad del servicio.

Esta fase del ciclo de vida del servicio es crítica pues de nada servirá tener procesos bien definidos e implementados, si no se lleva un correcto control y gestión de los mismos.

Los objetivos de la Operación del servicio son:

- Prestar eficaz y eficientemente los servicios TI.
- Minimizar el impacto de las interrupciones del servicio.
- Asegurar el acceso a los servicios únicamente a usuarios autorizados.

1.5.4.1 Funciones[21] de la Operación del Servicio [10]

Las funciones TI establecen los roles y responsabilidades para la prestación y soporte de servicios. Las funciones especificadas dentro de este ciclo de vida son:

***Service Desk*[22]**.- Proporciona un único punto de contacto entre los servicios y los usuarios, se encarga de gestionar incidentes, peticiones de servicio y la comunicación con el usuario. Las actividades del *service desk* son:

- Registrar los incidentes[23] y solicitudes importantes asignando prioridades y categorías.
- Proveer investigación y diagnóstico a los incidentes.
- Resolver incidentes o solicitudes de servicio siempre y cuando sea posible.
- Escalar incidentes o solicitudes de servicio dentro de tiempos establecidos cuando estos no pueden ser resueltos por la mesa de servicios.
- Mantener a los usuarios informados de los avances.
- Cerrar todos los eventos resueltos y solicitudes.

La mesa de servicios utiliza diferentes herramientas, sistemas y tecnología para brindar un soporte eficiente y efectivo para los usuarios, como por ejemplo: sistemas computarizados para monitoreo, servicios de voz, entre otros.

---

[21] Función: hace referencia a roles o personas que ejecutan una actividad, un proceso o ambos.
[22] *Service Desk* (mesa de servicios)
[23] Incidente: es una interrupción imprevista del servicio TI o reducción de la calidad del servicio.

Para evaluar el desempeño de la mesa de servicios y se establecen las siguientes métricas:

- El número de llamadas entrantes.
- Taza de resolución.
- Costo promedio del tratamiento de incidentes o solicitudes.
- Número de bases de conocimiento creadas.
- Tiempos de solución.
- Satisfacción del cliente.

Gestión Técnica.- provee habilidades técnicas detalladas y los recursos necesarios para dar soporte a la operación continua de los servicios de TI.

En organizaciones pequeñas, esta gestión se puede realizar a través de un solo departamento, pero en organizaciones grandes, se dividen en varios departamentos técnicos especializados.

Gestión de Operaciones TI.- es la función responsable de las actividades de mantenimiento de operaciones para la gestión de la infraestructura TI, su objetivo es asegurar que se cumplan los niveles acordados de servicio, consta de dos sub funciones que son:

- ***Control de Operaciones TI,*** se encarga de las actividades de mantenimiento de la infraestructura para asegurar que las tareas operativas se cumplan. Provee un monitoreo centralizado conocido como centro de operaciones de red (NOC).

- ***Gestión de Instalaciones***, gestiona el entorno físico TI, estos son usualmente los centros de datos.

Gestión de Aplicaciones.- esta función es responsable de gestionar aplicaciones que se utilizan en la operación del servicio a lo largo de su ciclo de vida (requerimientos, diseño, desarrollo, despliegue, operación y optimización).

1.5.4.2 Procesos de la Operación del Servicio [10]

Los procesos definidos por ITIL para la fase de operación del servicio son los siguientes:

1.5.4.2.1 *Gestión de Eventos* [10]

Este proceso está diseñado para gestionar eventos[24] a lo largo de su ciclo de vida, esto incluye la detección, entendimiento y determinación de una acción apropiada de control.

La gestión de eventos se basa en monitoreo operacional y de control, tiene dos tipos de herramientas que permiten:

- ***Monitoreo activo,*** sondea los elementos de configuración para determinar su estado y disponibilidad. Cualquier excepción detectada, generará una alerta.

- ***Monitoreo pasivo,*** detecta y correlaciona alertas.

Los objetivos de la gestión de eventos son:

- Detectar los cambios de estado significantes
- Determinar una acción de control apropiada para eventos.

Las actividades definidas en la Gestión de Eventos son las siguientes:

Ocurre un evento.- Los eventos ocurren constantemente, pero no todos son detectados o registrados, es por eso que es necesario definir qué tipo de eventos se deben detectar.

Notificación del evento.- La mayoría de elementos de configuración se diseñan para comunicar la siguiente información:

[24] Evento: es un cambio de estado que tiene significancia para la gestión de un servicio TI. Los eventos requieren personal de operaciones TI para tomar acciones en caso de que se convierta en un incidente.

- Un dispositivo es monitoreado por una herramienta de gestión para obtener datos específicos, es decir se realiza un sondeo.
- El elemento de configuración genera una notificación cuando se presentan ciertas condiciones.

Detección del evento.- Una vez que se ha generado la notificación del evento, será detectado por un agente que corre sobre el mismo sistema, o se transmite directamente a una herramienta de gestión diseñada para leer e interpretar el significado del evento.

Registro del evento.- El evento puede ser registrado mediante un registro de eventos o simplemente ser una entrada en el sistema de logs[25] del dispositivo o aplicación que genere el evento.

Primer nivel de correlación y filtrado de eventos.- El filtrado consiste en decidir cuáles eventos serán notificados y detectados por la herramienta de monitoreo.

Si es ignorado, se almacena en el archivo de logs del dispositivo. Aquí se decide el significado del evento que puede ser de tres tipos:

- ***Informativos***, indican que algo ha ocurrido, por ejemplo, que un usuario[26] ha ingresado a un equipo.

- ***Advertencia***, se presentan si algo inusual ha ocurrido, requiere de monitoreo, en este caso se resolverá solo. Así por ejemplo, cuando sube el procesamiento de un equipo.

- ***Excepciones***, se presentan cuando la operación no es normal, por lo tanto se requiere tomar acciones pues puede causar interrupción de la operación normal de los servicios, por ejemplo: caída de protocolos.

[25] Log: es el registro de eventos.
[26] Usuario: es la persona que utiliza los servicios TI diariamente.

Segundo nivel de correlación de eventos.- si el evento es una advertencia, se debe analizar para determinar su significancia y las acciones que deben ser tomadas para tratarlo.

¿Se requiere tomar una acción?.- Si el segundo nivel de correlación de eventos identifica un evento, se debe brindar una respuesta:

- **Auto respuesta,** algunos eventos presentan una respuesta definida y automática, por ejemplo: reiniciar un dispositivo, cambiar un parámetro de configuración.

- **Alerta e intervención humana,** si el evento requiere de intervención humana, es necesario escalarlo. El propósito de la alerta es direccionar el evento a la persona con las habilidades apropiadas para tratarlo y evitar que llegue al nivel incidente.

Las entradas de la gestión de eventos son:

- Requerimientos operacionales y de nivel de servicio asociados con eventos.
- Alarmas, alertas[27], y umbrales para reconocimiento de eventos.
- Roles y responsabilidades para identificación y notificación de eventos hacia los encargados de manejarlos.
- Procedimientos de identificación, registro, escalamiento y notificación.

Las salidas de la gestión de eventos son:

- Eventos notificados y escalados a los responsables de tomar acciones.
- Eventos que indican que ha ocurrido un incidente.

Indicadores de desempeño.- se definen los siguientes:

[27] Alerta: es una notificación que indica que algo ha cambiado, se ha sobrepasado un umbral, o ha ocurrido una falla

- Número de eventos en comparación de incidentes.
- Porcentaje de eventos que requieren intervención humana y si estos se solventan.
- Porcentaje de eventos que se convierten en incidentes y requieren cambios.
- Porcentaje de eventos generados por problemas existentes o errores reconocidos.
- Porcentaje de eventos que provocan la degradación del servicio.

1.5.4.2.2 *Gestión de Incidentes* [10]

Es el proceso responsable de gestionar cualquier evento que cause interrupción del servicio, su propósito es restaurar el servicio rápidamente y minimizar el impacto en las operaciones del negocio, esto con el propósito de garantizar que se cumplan los niveles de servicio acordados.

Los incidentes deben ser identificados por el personal técnico, detectados por las herramientas de monitoreo y reportados telefónicamente al *service desk*. Se definen los siguientes objetivos:

- Asegurar que los procedimientos estandarizados sean utilizados eficientemente.
- Realizar un adecuado análisis para brindar una respuesta rápida y que al resolverse se genere una documentación detallada.
- Alinear las actividades de gestión de incidentes con el negocio.
- Mantener la satisfacción del cliente con la calidad de los servicios TI.

Plazos.- se deben establecer plazos para la resolución de incidentes, estos se basan en el nivel de prioridad de los mismos.

Modelos de Incidentes.- debido a que muchos de los incidentes no son nuevos y se relacionan con alguno ocurrido anteriormente, es necesario establecer un modelo de incidente estándar para predefinir los pasos a seguir para resolverlo.

Estos modelos deben incluir:

- Los pasos a seguir para gestionar el incidente
- El orden cronológico para seguir estos pasos con sus dependencias
- Las responsabilidades asignadas a cada persona
- Las precauciones que se deben tomar para resolver el incidente (obtener *backups*[28] de los datos, archivos de configuración, entre otros).
- Plazos y umbrales para completar las acciones
- Procesos de escalamiento (a quien se debe contactar y cuándo)

Incidentes Críticos.- cuando se presentan incidentes que pueden ocasionar un impacto grande a la organización, se deben utilizar procedimientos diferentes para su resolución.

En estos incidentes se deben definir plazos más cortos y mayor urgencia para brindar una respuesta apropiada que permita la resolución de incidentes. Será necesario determinar la causa del incidente, entonces se verá envuelta con la gestión de problemas[29].

Seguimiento del estado de Incidentes.- se debe dar un seguimiento a los incidentes a lo largo de su ciclo de vida para realizar un correcto reporte del estado de incidentes. Los estados por los que atraviesa un incidente son:

- ***Abierto*****,** se identifica el incidente sin asignar un recurso para su resolución.

- ***En progreso*****,** el incidente se encuentra en proceso de análisis y resolución

- ***Resuelto*****,** el incidente se ha resuelto, pero aún no se ha validado la restauración del servicio con el cliente.

- ***Cerrado*****,** se valida la restauración del servicio

[28] *Backup*: es un respaldo de información o sistemas que permite su recuperación en caso de pérdidas.
[29] Problema: es la causa no identificada de una serie de incidentes

Las actividades definidas para la Gestión de Incidentes son:

Identificación del Incidente.- las fuentes desde las cuales se puede identificar el incidente son:

- Clientes y usuarios finales
- Personal de TI
- Mecanismos automáticos, incluyendo los utilizados en la gestión de eventos.
- Proveedores externos

Registro del incidente.- todos los incidentes deben ser registrados, sin excepción, con un número único referencial, debe incluir la fecha y la hora en la que se generó así como el tiempo de solución y su hora de cierre en cuanto se ha validado con el cliente. Se debe registrar toda la información relevante del incidente, incluyendo su prioridad y categorización.

Categorización del incidente.- como parte del registro inicial del incidente, es necesario categorizarlo, de esta manera se almacena el tipo exacto de incidente, esto es importante para determinar la frecuencia de estos, y establecer pautas para ser usadas en la gestión de problemas.

Es importante tener claro que una solicitud de servicio no es un incidente.

Priorización de Incidentes.- otro aspecto importante dentro del registro de incidentes es su priorización, esto determinará como se gestionará el incidente. Para calcular la prioridad se utiliza la siguiente fórmula:

$$\boldsymbol{Prioridad = Impacto + Urgencia}$$

Dónde:

- ***Impacto*****,** es el grado de afectación de usuarios. Se toman en cuenta los siguientes factores para determinar el impacto de un incidente:

- Número de usuarios afectados
- Número de servicios afectados
- Daño a la reputación de la empresa.
- Tipo de usuarios afectados

- ***Urgencia*****,** es el tiempo de resolución del incidente. Para calcular la urgencia de resolución de un incidente, es necesario asociarla con el impacto.

La Tabla 1.1 muestra la matriz de impacto vs urgencia, para obtener la prioridad.

		Urgencia		
		Alto	Medio	Bajo
Impacto	Alto	1	2	3
	Medio	2	3	4
	Bajo	3	4	5

Tabla 1.1 Cálculo de la Prioridad [10]

Se definen los tiempos para la resolución de incidentes dependiendo de la priorización, estos se muestran en la **Tabla 1.2**.

Prioridad	**Descripción**	**Tiempo de resolución**
1	Crítica	1 hora
2	Alta	8 horas
3	Media	24 horas
4	Baja	48 horas
5	Programada	Programado

Tabla 1.2 Tiempos de resolución de Incidentes [10]

Diagnóstico Inicial.- previo a la resolución de un incidente, se realiza un análisis, el cual permitirá determinar las acciones a tomar. Esto generalmente, lo realiza el personal del *service desk*.

Escalamiento de Incidentes.- cuando el personal del *service desk* requiere ayuda de otros grupos para resolver el incidente, lo escala. Se deben establecer reglas de escalamiento para orientarlo a los grupos adecuados y garantizar que esto se realice solo cuando sea necesario.

Investigación y Diagnóstico.- se deben incluir las siguientes acciones.

- Identificar el error.
- Reconocer el orden cronológico de los eventos.
- Confirmar las consecuencias del incidente detectado, incluyendo el número de usuarios afectados.
- Distinguir los eventos que desencadenaron el incidente.
- Buscar guía que ayude a resolver el incidente.

Resolución de incidentes y recuperación del servicio.- cuando se ha identificado la resolución para un incidente, esta se debe aplicar y probar; las acciones que se tomarán y el personal que las realizará variarán dependiendo de la naturaleza de la falla.

Incluso cuando se ha restaurado el servicio, es necesario realizar varias pruebas para asegurar que ha recuperado su funcionamiento normal. Sin importar las acciones que se tomen, o quien las realice, el registro de incidentes debe ser actualizado con todos los detalles e información relevante.

El grupo que se encargue de la resolución, deberá reportar las acciones al *service desk* para que se encargue del cierre del incidente.

Cierre de Incidentes.- cuando se han resuelto los incidentes, el *service desk* debe revisar que estos se hayan resuelto por completo para proceder a cerrarlos. Se debe revisar lo siguiente:

- Categorización.
- Satisfacción del usuario.

- Documentación de incidentes.
- ¿Es un problema recurrente?
- Cierre Formal.

Indicadores de Desempeño.- se definen los siguientes [10]:

- Separación de incidentes en cada etapa.
- Porcentaje de incidentes resueltos por el *service desk* sin necesidad de escalarlos.
- Porcentaje de incidentes resueltos remotamente, sin la necesidad de una visita.
- Número de incidentes críticos para cada servicio TI.
- Porcentaje de respuestas satisfactorias de encuestas.
- Número de incidentes asignados y categorizados incorrectamente.

1.5.4.2.3 *Gestión de Problemas* [8] [10]

Es el proceso responsable de gestionar el ciclo de vida de los problemas. ITIL define un problema como la causa raíz de los incidentes. Hay dos formas de gestionar problemas:

- ***Gestión de problemas reactiva****,* se concentra en resolver problemas generados por uno o varios incidentes.

- ***Gestión de problemas proactiva****,* se concentra en la identificación y solución de problemas y errores conocidos para evitar futuras incidencias.

Los objetivos de la gestión de problemas son:

- Prevenir la ocurrencia de problemas e incidentes.
- Eliminar incidentes recurrentes.
- Minimizar el impacto de incidentes que no se pueden prevenir.
- Solicitar cambios cuando sea necesario para mejorar el servicio.

Incidentes vs Problemas [8].-

La gestión de Problemas e Incidentes no se utiliza simultáneamente: la gestión de incidentes será llamada primero, si la situación requiere que se llame a la gestión de problemas, se lo hace. ITIL identifica estas situaciones:

- La gestión de incidentes no puede relacionar a un incidente con problemas y errores conocidos existentes.
- El análisis de los incidentes registrados, indica que puede existir un problema.
- Ha ocurrido un incidente crítico, por lo cual es necesario identificar la causa raíz.
- Otras funciones TI identifican la existencia de un problema.
- El *service desk* ha resuelto un incidente, pero no ha determinado la causa y tiene la sospecha de que puede ocurrir nuevamente.

Si no se realiza una distinción entre problemas e incidentes se corren los siguientes riesgos:

- Se puede extender la duración de cortes de servicio si dentro de las actividades de resolución de incidentes se incluye la búsqueda de la causa raíz en lugar de tomar acciones directas para restaurar el servicio.
- Se cerrarán los registros de incidentes sin incluir las acciones para prevenir recurrencia, por lo que algunos incidentes continuarán interrumpiendo los servicios y serán resueltos muchas veces.

Gestión de Problemas Reactiva [8].-

Las actividades presentadas en la gestión de problemas son similares a las realizadas en la gestión de incidentes, son las siguientes:

- Detección de problemas.
- Registro de problemas.
- Categorización y priorización de problemas.
- Investigación y diagnóstico de problemas.

- Solución de problemas.
- Levantamiento del registro de errores conocidos.
- Resolución de problemas.
- Revisión de problemas críticos y errores detectados.

En la **Figura 1.6** se muestran las actividades de la gestión de problemas reactiva donde se verifica que tiene como entrada a eventos e incidentes.

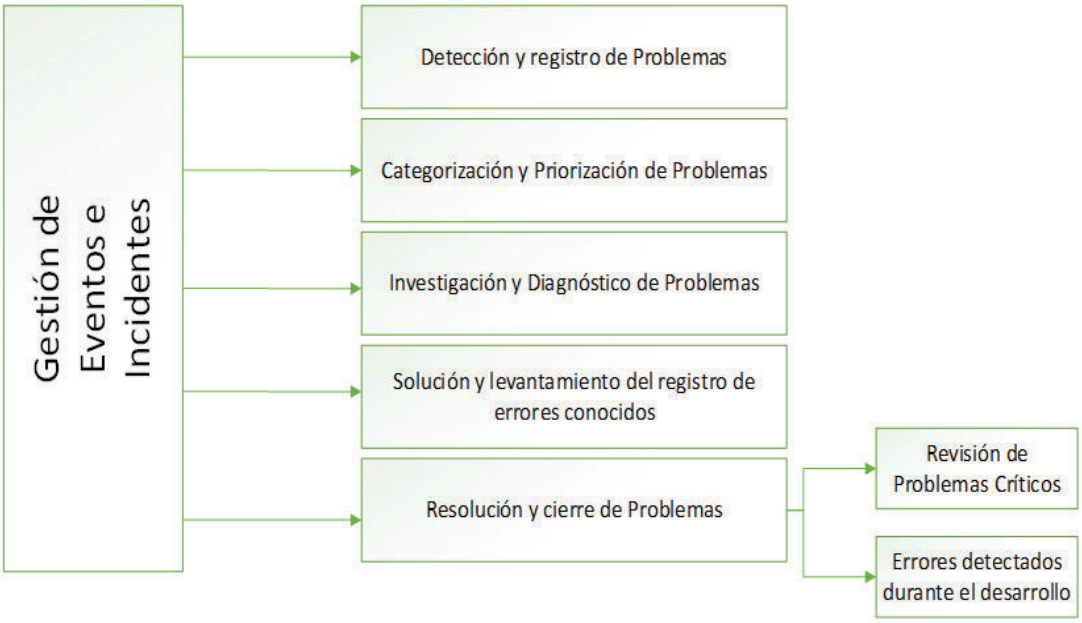


Figura 1.6 Actividades de la gestión de Problemas Reactiva [10]

Gestión de Problemas Proactiva.- cuenta con las siguientes actividades:

- ***Análisis de Tendencias,*** se encarga de la revisión de reportes de otros procesos e identificación de problemas recurrentes.

- ***Acciones preventivas,*** se realiza un análisis de los mantenimientos preventivos que se deben llevar a cabo para prevenir incidentes que impacten el funcionamiento normal del servicio.

Indicadores de Desempeño.- se definen los siguientes [8]:

- El número de errores conocidos agregados a la base de datos de errores conocidos.
- Tiempo de resolución de incidentes relacionados con errores conocidos.
- Número total de problemas.
- Número de reincidencias de problemas para cada servicio.
- Número de problemas críticos.
- Porcentaje de resoluciones exitosas de problemas críticos.
- Numero de problemas asignados incorrectamente.
- Número de problemas que han sobrepasado el tiempo de resolución.

1.5.4.2.4 *Gestión de Consultas* [10]

Este proceso se encarga de gestionar las peticiones de servicio[30] de los usuarios. Las consultas que generalmente se toman en cuenta en este proceso son: cambios de hardware, adición de usuarios, cambios de claves o reseteo de *passwords.* Los objetivos definidos para la Gestión de consultas son:

- Mantener la satisfacción del cliente y usuarios mediante una correcta gestión de sus peticiones.
- Proveer un canal para los usuarios y sus peticiones de servicio que requieren una autorización previa.
- Asistir con información general.

Modelos de peticiones.- Se definen los modelos de peticiones para documentar lo siguiente:

- Las actividades realizadas para cumplir el requerimiento.
- Los roles y responsabilidades.
- Tiempos de escalamiento.

Las actividades definidas por ITIL para la gestión de peticiones son [8]:

[30] Peticiones de servicio: descripción de diferentes tipos de demandas realizadas por los usuarios de los servicios TI.

- ***Menú de opciones,*** se deben emplear mecanismos que permitan a los usuarios generar las peticiones de servicio. Esto se debe realizar con el apoyo de aplicaciones web.

- ***Aprobación Financiera,*** es necesaria una aprobación financiera previa para aquellas peticiones que impliquen una inversión

- ***Otras Aprobaciones,*** en ocasiones son necesarias aprobaciones adicionales, dependiendo de la solicitud realizada.

- ***Cumplimiento,*** el cumplimiento varía dependiendo de las características de la petición de servicio. Algunas se cumplirán únicamente utilizando mecanismos automáticos, otras serán realizadas por el *service desk* o será necesario escalar a los grupos especializados.

- ***Cierre,*** una vez que se ha cumplido la solicitud, se debe cerrar el requerimiento después de la confirmación del usuario.

Indicadores de Desempeño.- se definen los siguientes:

- El tiempo empleado para realizar cada tipo de petición
- El número de peticiones cumplidas dentro de los tiempos acordados
- El número de peticiones aprobadas para su aprovisionamiento

1.5.4.2.5 *Gestión de Acceso* [10]

Es el proceso diseñado para brindar permisos de acceso a los usuarios autorizados para utilizar servicios especificados en el Catálogo de Servicios y evitar el acceso a los usuarios no autorizados.

Se encarga de la ejecución de las políticas de seguridad, con lo cual permite gestionar la confidencialidad e integridad de los datos de la organización.
Los objetivos de la gestión de acceso son:

- Dar respuesta eficiente ante solicitudes de acceso o restricción a los servicios, cambio de derechos de acceso.
- Supervisar que los derechos de acceso a los servicios sean utilizados apropiadamente.

Actividades.- En la **Figura 1.7** se muestran las actividades de la gestión de acceso[8].

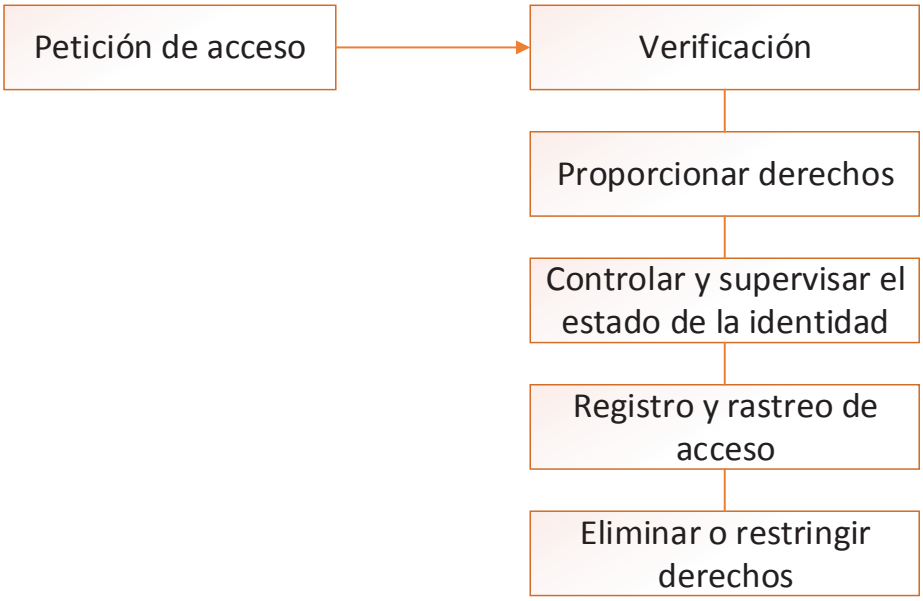


Figura 1.7 Actividades de la Gestión de Acceso [8]

- ***Petición de acceso,*** se puede recibir de diferentes fuentes como el sistema de recursos humanos (cuando hay cambio de personal), un RFC, una solicitud mediante la gestión de peticiones.

- ***Verificación,*** se deben verificar las peticiones de acceso desde dos perspectivas.

    - Que el usuario que solicita el acceso sea quien dice ser, para lo cual es necesario el nombre de usuario y contraseña.
    - Que los motivos para la solicitud son legítimos, requiere más verificaciones como por ejemplo: una autorización.

- ***Proporcionar derechos,*** la gestión de acceso ejecuta las políticas definidas mas no se especifica quién tiene acceso y a qué servicios. .Una vez que se han verificado los usuarios, se proporcionan derechos de acceso a los servicios, estos, se basan en los diferentes roles definidos y en las políticas establecidas.

- ***Controlar y supervisar el estado de la Identidad,*** los cambios de derechos se asocian al ciclo de vida de un empleado dentro de la organización, se toman en cuenta los siguientes: cambios de empleo, despidos, ascensos, transferencias, acciones disciplinarias.

- ***Registro y rastreo de acceso,*** la gestión de acceso es responsable de asegurar que los derechos proporcionados sean utilizados adecuadamente, eliminar o restringir derechos.

1.5.5 MEJORA CONTINUA DEL SERVICIO [11]

Como parte del ciclo de vida del servicio ITIL, la mejora continua tiene el propósito de alinear los servicios TI con las necesidades cambiantes del negocio, mediante la identificación e implementación de mejoras sobre los servicios soportados por los procesos TI.

La base de la mejora continua del servicio se enfoca en el seguimiento y evaluación de procesos reformándolos para así alinearlos a la misión y visión del negocio.

Los objetivos de la Mejora Continua del Servicio son:

- Revisar, analizar, priorizar y realizar recomendaciones sobre las oportunidades de mejora sobre todos los procesos en cada etapa del ciclo de vida ITIL.
- Identificar e implementar actividades para mejorar la calidad de los servicios TI

- Mejorar la relación costo-efectividad de los servicios TI sin sacrificar la satisfacción del cliente.
- Entender qué será medido, por qué es medido, y cuál debería ser un resultado exitoso.

1.5.5.1 El Ciclo de Deming [11]

Constituye la base de los procesos de mejora continua:

Plan (Planear).- definir objetivos y especificar cómo cumplirlos

Do (Hacer).- implementar el plan y medir su desempeño

Check (Chequear).- verificar que se han cumplido los objetivos

Act (Actuar).- corregir las fallas detectadas y mejorar los procesos utilizados.

1.5.5.2 Métricas [8]

La organización TI debe definir un conjunto de métricas para determinar si se han alcanzado las metas propuestas y verificar el rendimiento de los procesos involucrados. Se definen tres métricas:

- **Tecnológicas,** miden disponibilidad, capacidad y rendimiento de la infraestructura y aplicaciones.

- **Procesos,** miden el rendimiento y calidad de procesos de gestión de TI.

- **Servicios,** se encargan de la evaluación de servicios.

1.5.5.3 Proceso de Mejora continua del Servicio [11]

Es el proceso responsable de definir los pasos requeridos para identificar, definir, analizar e implementar mejoras.

El rendimiento del proveedor de servicios TI es medido continuamente por este proceso y las mejoras se convierten en procesos o servicios TI para incrementar la eficiencia y eficacia.

Este proceso está formado por siete pasos mediante los cuales se elaboran Planes de Mejora Continua del Servicio para optimizar procesos. Los siete pasos de este proceso se muestran en la **Figura 1.8**.

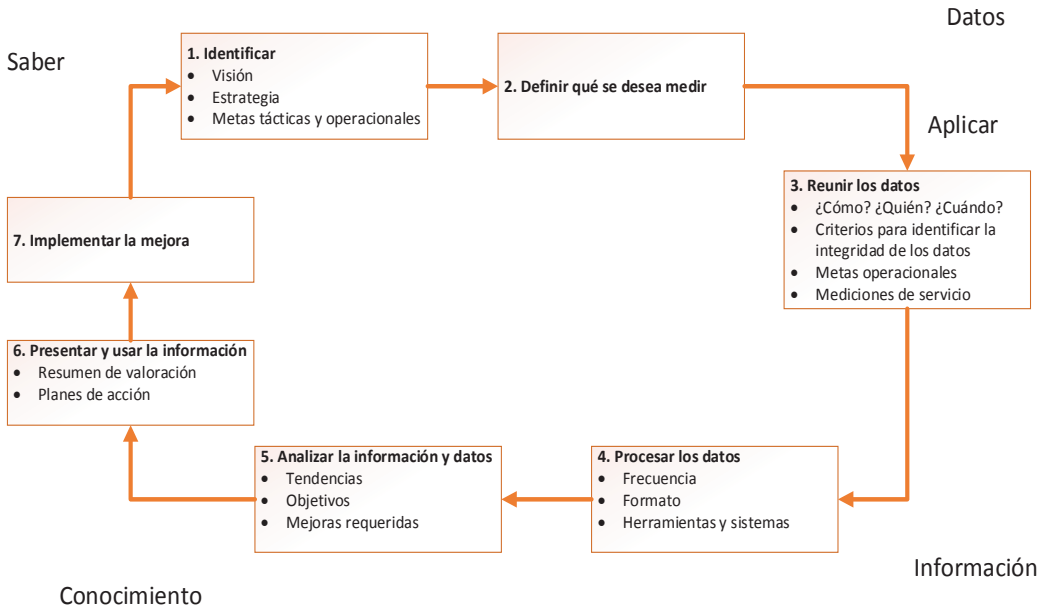


Figura 1.8 Siete pasos del proceso de mejora [11]

Identificar la estrategia para la mejora.- identificar la visión general, necesidades del negocio, la estrategia y las metas tácticas y operacionales.

Definir qué se medirá.- se debe identificar la situación actual de la empresa y también a dónde se desea llegar incluyendo la metodología para conseguirlo. Se deben definir los procesos que son asequibles a la organización, para esto se tiene en cuenta lo siguiente:

- Procesos de medida existentes.
- Informes.

- Flujos de trabajo.
- Protocolos y procedimientos utilizados actualmente.

Recopilar los datos.- para responder la pregunta ¿Lo logramos? Se debe primero recopilar los datos (esto se hace desde la operación de servicios). Los datos se obtienen de diferentes fuentes basadas en metas y objetivos definidos.

Procesar los datos.- se procesan los datos para transformarlos en información, la misma que será analizada más adelante, se deben realizar las siguientes tareas:

- Analizar SLAs vigentes para determinar la información útil para evaluar que estos se cumplan.
- Establecer procedimientos para procesar datos e incluir la frecuencia con que se realizarán.
- Determinar recursos necesarios.
- Definir el personal a cargo.
- Establecer una estructura de la información a ser entregada.

Analizar la información y datos.- se transforma la información en conocimiento para determinar qué se mejorará. Se debe comprobar:

- Cumplimiento de SLAs.
- Servicios eficientes.
- Cumplimiento de procedimientos.
- Cumplimiento de objetivos por parte de los servicios TI.

Presentar y usar la información.- se utiliza la información adquirida previamente para tomar decisiones, para esto se deben presentar informes al personal responsable de la gestión de los servicios TI.

Implementar la mejora.- el conocimiento obtenido se utiliza para optimizar, mejorar, corregir servicios y procesos.

Finalmente se detectan fallas e implementan soluciones. Al seguir este paso, la organización establece una nueva línea base y el ciclo empieza de nuevo.

1.5.5.4 Relación con la fase de Operación del Servicio [11]

La etapa de Mejora Continua es dependiente de la Operación del servicio ya que obtiene la información de esta para optimizar los procesos y actividades para la prestación de los servicios.

Los informes que se generan en la Operación del servicio deben contener la siguiente información:

- Incidencias que afecten la calidad del servicio.
- Soluciones a los problemas detectados.
- Peticiones de usuarios.

1.6 MAPEO DE LOS PROCESOS COBIT ALINEADOS A ITIL

En la **Tabla 1.3** se muestra la alineación de los procesos de COBIT a ITIL, esto para los procesos utilizados en el presente proyecto.

DS5 Garantizar la seguridad de los sistemas		
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**
DS5.1 Gestión de la seguridad de TI	• Ubicar la gestión de seguridad a alto nivel para cumplir con las necesidades del negocio	• SD 4.6 Gestión de seguridad de la información • SO 5.13 Gestión de seguridad de la información y la operación del servicio
DS5.2 Plan de Seguridad de TI	• Traducción de requerimientos de negocio, riesgo y cumplimiento en un plan de seguridad	• SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura a alto nivel, sin detalle)
DS5.3 Gestión de identidad	• Identificación de todos los usuarios y su actividad	• SO 4.5 Gestión de acceso

DS5 Garantizar la seguridad de los sistemas		
DS5.4 Gestión de cuentas de usuario	• Gestión del ciclo de vida de las cuentas de usuario y privilegios de acceso	•SO 4.5 Gestión de acceso •SO 4.5.5.1 Peticiones de acceso •SO 4.5.5.2 Verificación •SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	• Pruebas proactivas de la implementación de seguridad • Acreditación oportuna • Reporte oportuno de eventos inusuales	• SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio
DS5.6 Definición de incidente de seguridad	• Definición y clasificación de las características de los incidentes de seguridad	• SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes
DS5.7 Protección de la tecnología de seguridad	• Resistencia a la manipulación	• SO 5.4 Gestión y soporte de servidores
DS5.8 Gestión de llaves criptográficas	• Gestión del ciclo de vida de llaves criptográficas	NA
DS5.9 Prevención, detección y corrección de software malicioso	• Parches de actualización, control de virus y protección de malware	NA
DS5.10 Seguridad de la red	• Controles para autorizar acceso y flujos de información desde y hacia las redes	NA
DS5.11 Intercambio de datos sensitivos	• Ruta confiable y controles de autenticación, constancia de recepción y no repudio	NA

DS10 Gestionar problemas		
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**
DS10.1 Identificación y clasificación de problemas	• Clasificación de problemas; asignación al personal de soporte	• SO 4.4.5.1 Detección de problemas • SO 4.4.5.3 Clasificación de problemas • SO 4.4.5.4 Priorización de problemas
DS10.2 Seguimiento y resolución de problemas	• Pistas de auditoría, seguimiento y análisis de causa raíz de todos los problemas • Inicio de soluciones para abordar las causas de origen	• SO 4.4.5.2 Log de problemas • SO 4.4.5.5 Investigación y diagnóstico de problemas • SO 4.4.5.6 Soluciones provisionales • SO 4.4.5.7 Registro de errores conocidos • SO 4.4.5.8 Resolución de problemas
DS10.3 Cierre de problemas	• Procedimientos de cierre después de la eliminación del error o enfoques alternos	• SO 4.4.5.9 Cierre de problemas • SO 4.4.5.10 Revisión de problemas mayores
DS10.4 Integración de la gestión de configuración, incidentes y problemas	• Integración para habilitar una gestión efectiva de problemas	NA
DS8 Gestionar la mesa de servicios y los incidentes		
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**
DS8.1 Mesa de servicios	• Interface de usuario • Gestión de llamadas • Clasificación y priorización de incidentes basadas en servicios.	• SO 4.1 Gestión de eventos • SO 4.2 Gestión de incidentes • SO 6.2 Mesa de servicios
DS8.2 Registro de consultas de clientes	• Registro y seguimiento de todas las llamadas, incidentes, solicitudes de servicio y necesidades de información	• SO 4.1.5.3 Detección de eventos • SO 4.1.5.4 Filtrado de eventos • SO 4.1.5.5 Significado de los eventos • SO 4.1.5.6 Correlación de eventos

DS8 Gestionar la mesa de servicios y los incidentes		
DS8.2 Registro de consultas de clientes		• SO 4.1.5.7 Trigger • SO 4.2.5.1 Identificación de incidentes • SO 4.2.5.2 Log de incidentes • SO 4.2.5.3 Clasificación de incidentes • SO 4.2.5.4 Priorización de incidentes • SO 4.2.5.5 Diagnóstico inicial • SO 4.3.5.1 Selección por menú
DS8.3 Escalamiento de incidentes	• Escalamiento de incidentes de acuerdo a los límites del nivel de servicio.	• SO 4.1.5.8 Selección de respuestas • SO 4.2.5.6 Escalamiento de incidentes • SO 4.2.5.7 Investigación y diagnóstico • SO 4.2.5.8 Resolución y recuperación • SO 5.9 Soporte de estaciones de trabajo
DS8.4 Cierre de incidentes	• Registro de los incidentes resueltos y no resueltos	• SO 4.1.5.10 Cerrar eventos • SO 4.2.5.9 Cierre de incidentes
DS8.5 Reportes y análisis de tendencias	• Reportes de desempeño de servicio y tendencias de los problemas recurrentes	• SO 4.1.5.9 Revisar acciones • CSI 4.3 Mediciones del servicio (aproximada)

Tabla 1.3 COBIT 4.1 alineado a ITIL V3 [12]

CAPÍTULO 2

AUDITORÍA DE LOS PROCESOS INTERNOS DE OPERACIÓN Y MANTENIMIENTO CON COBIT 4.1

Una vez realizado el estudio del marco de trabajo COBIT, en el presente capítulo se describe la situación actual del área de O&M[31] de MPLS basados en una auditoría con los criterios de COBIT 4.1, los resultados se presentan por medio de matrices de desempeño, riesgos, valor y responsabilidades, con las cuales se obtienen los resultados para la determinación del nivel de madurez de los procesos internos del área. Finalmente, se indican los procesos que serán normalizados mediante ITIL en el capítulo 3.

2.1 SITUACIÓN ACTUAL DEL ÁREA DE OPERACIÓN Y MANTEMIENTO DE MPLS

2.1.1 OBJETIVO GENERA DEL ÁREA

Mantener, gestionar, operar y aprovisionar la red a nivel nacional, para garantizar la disponibilidad en los servicios, incrementar la optimización y efectividad de la red [13].

2.1.2 ESTRUCTURA DEL ÁREA O&M DE IP/MPLS [13]

El área está dividida en dos niveles dentro de los cuales existen grupos coordinados por un responsable y trabajan en conjunto para cumplir con las funciones del área. En la **Figura 2.1** se presenta el organigrama actual correspondiente al área O&M de las plataformas IP MPLS.

2.1.2.1 Gestión Técnica

Se responsabiliza de la gestión de eventos, incidentes, accesos y de cambios. Además se encarga de gestionar instalaciones y mantenimientos preventivos.

---

[31] O&M: acrónimo de Operación y Mantenimiento.

2.1.2.2 Gestión de Proyectos y Logística

Tiene la función de administrar presupuestos, logística, turnos, pasantías e inventarios.

2.1.2.3 O&M Backbone MPLS

Se encarga de realizar el aprovisionamiento, solución de incidentes, soporte de la red y atención de órdenes de trabajo. También se encargan de ejecutar los mantenimientos preventivos y correctivos.

2.1.2.4 O&M Core

Es el responsable de la administración de las plataformas Core móvil, del Peering de enlaces internacionales y del backbone de internet. También se encarga de la resolución de incidentes que se presenten en este nivel.

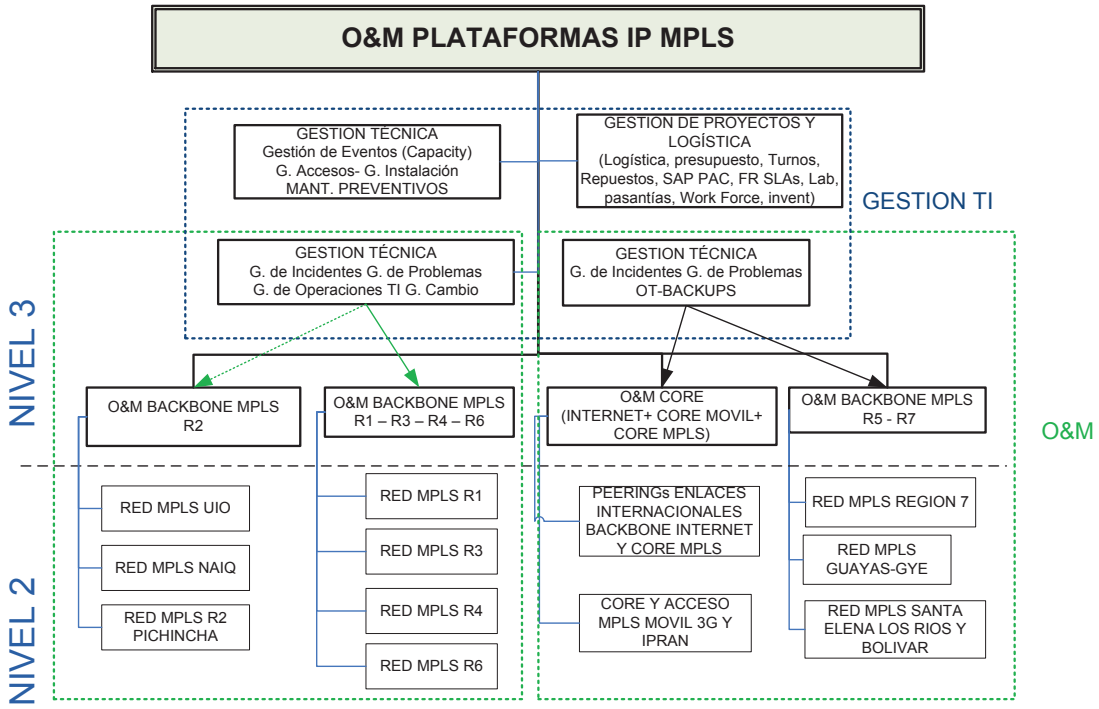


Figura 2.1 Organigrama del área O&M de la Plataforma IP MPLS [14]

Para administrar de forma sencilla la red nacional MPLS, CNT la divide en regiones, éstas se describen en la **Tabla 2.1**.

REGIÓN	PROVINCIAS
R1	Imbabura, Esmeraldas, Carchi, Sucumbíos
R2	Pichincha, Napo, Orellana
R3	Tungurahua, Pastaza, Cotopaxi, Chimborazo
R4	Santo Domingo, Galápagos, Manabí
R5	Guayas, Santa Elena, Los Ríos, Bolívar
R6	Azuay, Cañar, Morona Santiago
R7	El Oro, Loja, Zamora Chinchipe

Tabla 2.1 División en regiones de la red MPLS [14]

2.1.3 OBJETIVOS DEL ÁREA DE O&M MPLS [13]

- Ejecutar el mantenimiento preventivo y correctivo de la plataforma IP MPLS en coordinación con los grupos O&M Provinciales, en base a la normativa y manuales correspondientes a cada sistema.

- Administrar usuarios y accesos de la plataforma IP MPLS que están en operación.

- Realizar aprovisionamiento y activación de servicios de la plataforma IP MPLS.

- Generar, respaldar y responder por la confidencialidad de la información de la plataforma IP MPLS, según la normativa y manuales correspondientes.

- Actualizar el inventario de materiales, bienes, repuestos, plataformas IP MPLS, equipos de medición, herramientas y recursos asignados al área.

- Dar soporte en proyectos de ampliación de la plataforma IP MPLS.

- Ejecutar todas las acciones necesarias para garantizar la disponibilidad de la plataforma IP MPLS.

- Elaborar planes, políticas o directrices para la operación y mantenimiento de la plataforma IP MPLS.

- Coordinar la ejecución de cambios, migraciones y mantenimientos preventivos (rutinas, respaldos, etc.) de la plataforma IP MPLS, a nivel nacional.

- Cumplir y hacer cumplir los planes de operación y mantenimiento para la mejora continua de servicios y recursos de la plataforma IP MPLS, con las diferentes áreas de la Gerencia de Operación & Mantenimiento y los grupos O&M.

- Ejecutar todas las tareas en el ámbito de su competencia con respecto a la implantación del nuevo sistema transaccional.

- Controlar los procesos de su competencia que se encuentren desconcentrados en las Agencias Regionales y Provinciales.

- Monitorear y controlar indicadores operativos de los procesos a su cargo.

- Definir e implantar proyectos de mejora de procesos en el ámbito de su competencia.

- Brindar soporte y emitir criterios formales respecto a los procesos de su competencia.

- Cumplir las disposiciones legales, reglamentarias y demás normativas.

2.1.4 HERRAMIENTAS DE APOYO DEL ÁREA O&M DE IP MPLS

Para la gestión de la red IP MPLS el área O&M cuenta con las siguientes herramientas de monitoreo, control de acceso y gestión.

2.1.4.1 Cisco Prime [15]

Es una herramienta de monitoreo que ofrece un conjunto de herramientas visuales para la gestión de la red y servicios. Las herramientas son las siguientes:

- ***Cisco Prime Network Vision***, permite el monitoreo constante de los estados de red y servicios a través de mapas, así como verificación de conectividad de los mismos. En la **Figura 2.2** y **Figura 2.3** se presentan ejemplos de los elementos de red y topologías que permite visualizar esta herramienta.

Figura 2.2 Elementos de red [16]

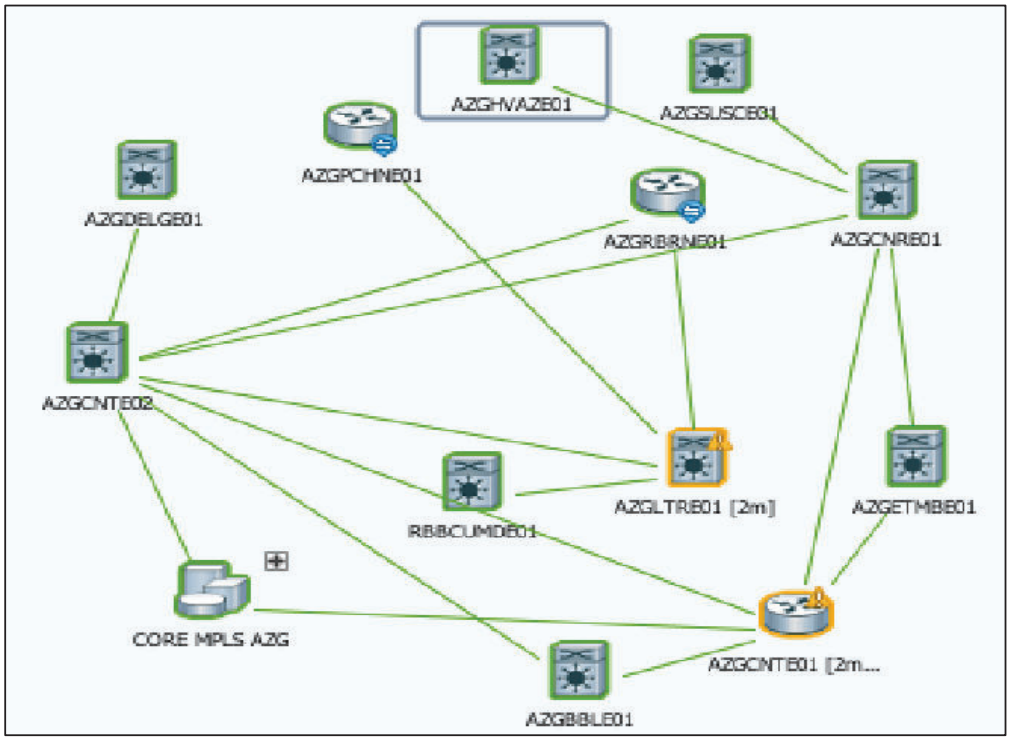


Figura 2.3 Vista gráfica integral de la topología de Azogues [17]

- ***Cisco Prime Network Events***, permite la visualización y recuperación de la información detallada de los diferentes eventos del sistema. En la **Figura 2.4** se presenta un ejemplo de las alarmas que se presentan en esta herramienta.

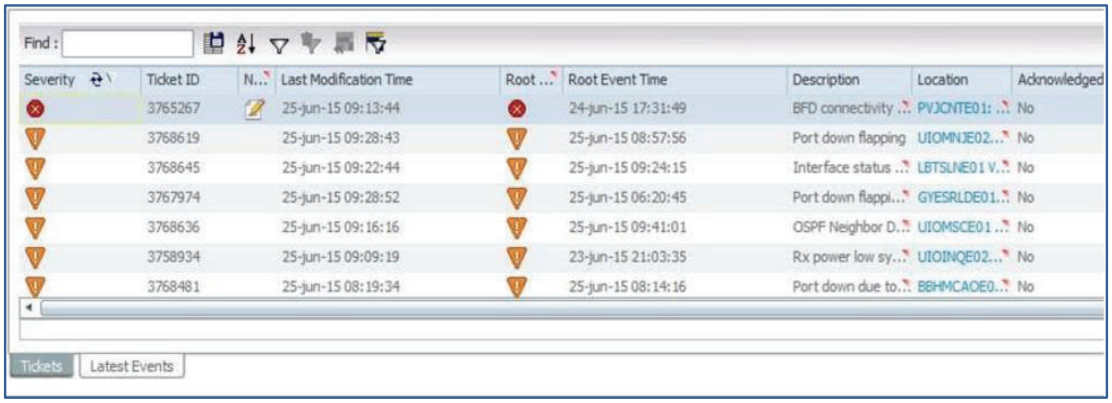


Figura 2.4 Vista de las alarmas generadas en Cisco Prime Network Events [18]

En la **Tabla 2.2** se describe el significado de las alarmas que se presentan en la herramienta Cisco Prime.

Ícono	Color	Significado de alarma
	Rojo	Critica
	Naranja	Mayor
	Amarillo	Menor
	Celeste	Advertencia
	Verde	Servicio estable

Tabla 2.2 Representación y significado de alarmas en Cisco Prime

- ***Cisco Prime Network Administration***, permite administrar cada uno de los servidores (Gateway, Units) y los elementos de red incluidos en los mismos.

En la **Figura 2.5** se presenta un elemento de red agregado y los posibles comandos que pueden ser ejecutados.

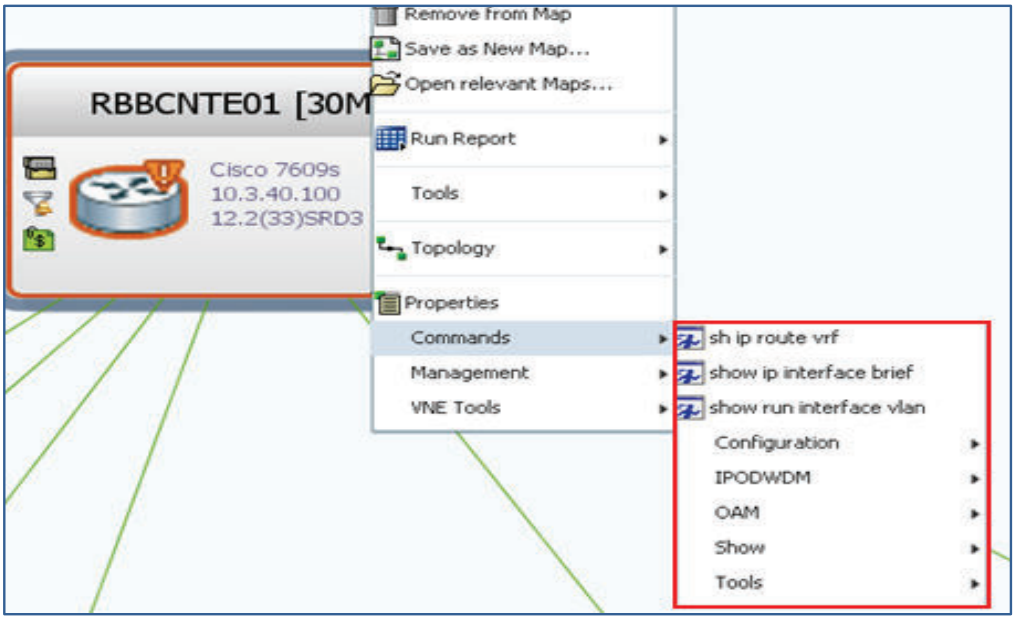


Figura 2.5 Vista de los elementos de red agregados en la herramienta [19]

2.1.4.2 Cacti

Esta herramienta permite monitorizar el desempeño y utilización de los recursos, además sirve de apoyo para archivar y presentar estadísticas de redes y servidores. En la **Figura 2.6** se muestra el ejemplo del tráfico de un enlace graficado mediante el cacti, donde se observa un consumo normal con un máximo de 8 Gbps.

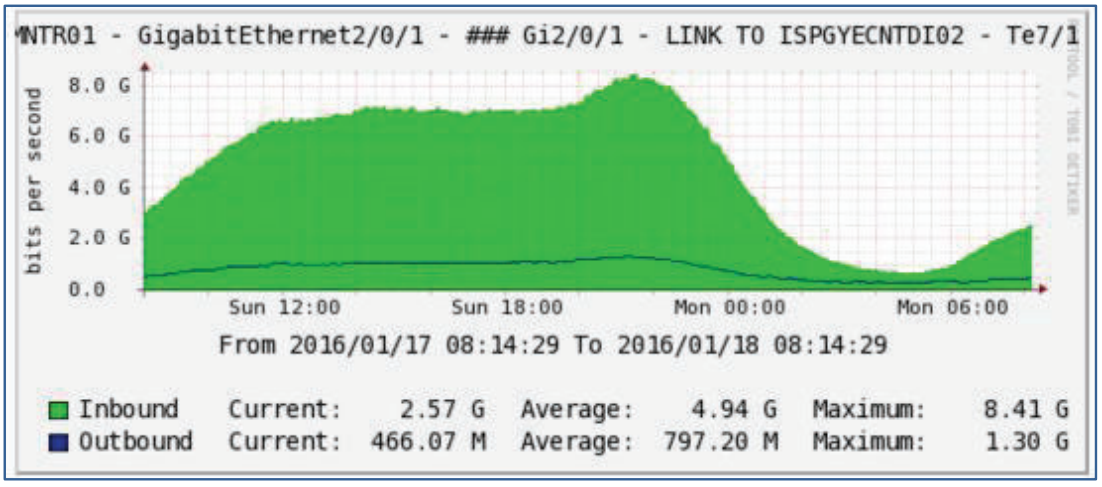


Figura 2.6 Monitoreo del tráfico de un enlace mediante la herramienta Cacti [20]

2.1.4.3 Sistema de control de Acceso ACS [21]

Es una herramienta de control de acceso cuyo sistema centralizado permite controlar el acceso remoto a los dispositivos de la red y ofrece el servicio AAA (Auditoría, Autorización, Autenticación). En la **Figura 2.7** se presenta la pantalla de inicio del ACS.

Figura 2.7 Vista de la pantalla de inicio de la herramienta ACS [22]

- ***Privilegios de acceso a los dispositivos de red***, para llevar el control de los privilegios, se definen diferentes grupos de usuarios dependiendo de las funciones que desempeñen dentro del área.

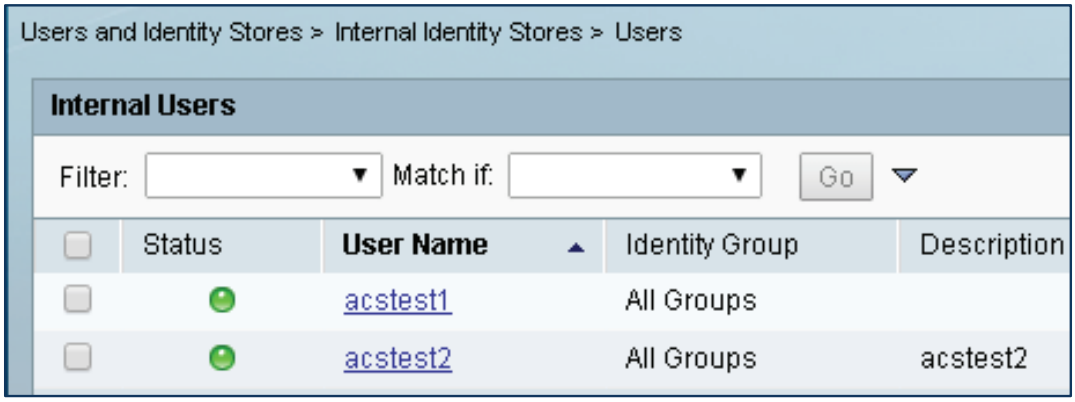


Figura 2.8 Usuarios creados en el ACS [22]

En la **Figura 2.8** se muestra un ejemplo de usuarios creados, estos se han asociado *All Groups* que es un perfil que tiene privilegios para aplicar un conjunto de comandos permitidos y en la **Figura 2.9** se muestra un ejemplo de los usuarios añadidos al perfil *All Groups.*

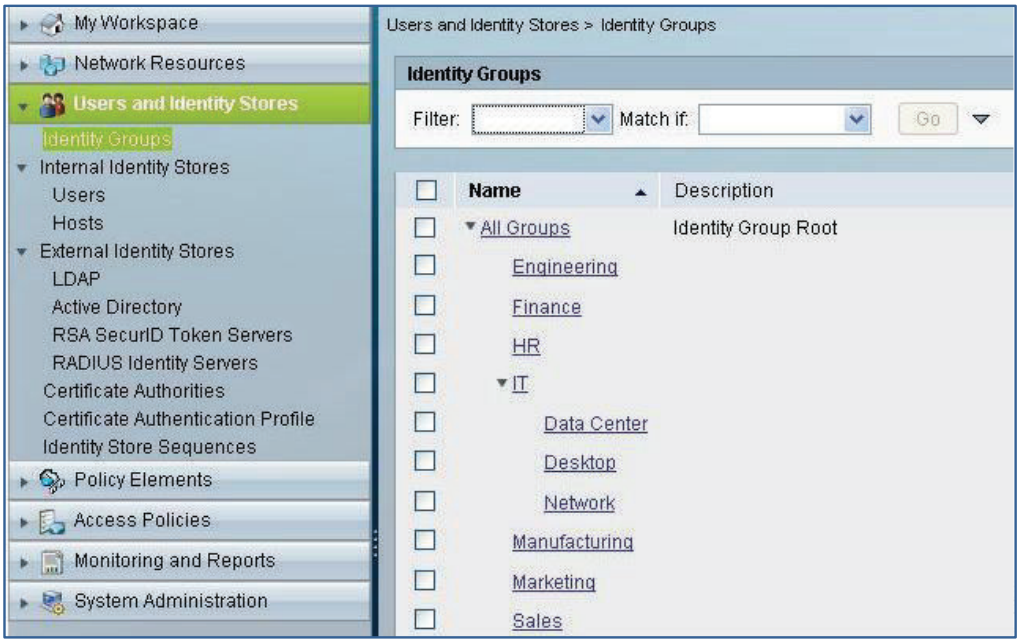


Figura 2.9 Grupos de Usuarios definidos en el ACS [22]

- ***Creación de equipos,*** para la creación de los equipos dentro de la herramienta es necesario asociarlos a dos grupos clasificados por localización (regiones) y por tipo (acceso, distribución y núcleo).

- ***Políticas de seguridad de acceso,*** se definen políticas de seguridad con parámetros que deben cumplir los usuarios para acceder a los equipos, estas son:

    - Tiempo de caducidad de contraseñas.
    - Símbolos.
    - Palabras no permitidas.
    - Número de intentos para ingreso.
    - Longitud mínima de la contraseña.
    - El número máximo de conexiones por usuario.

En la **Figura 2.10** se presenta el formulario en el cual se establece el tiempo de vida de las contraseñas y el tiempo con el cual se anticipa al usuario para el cambio de las mismas.

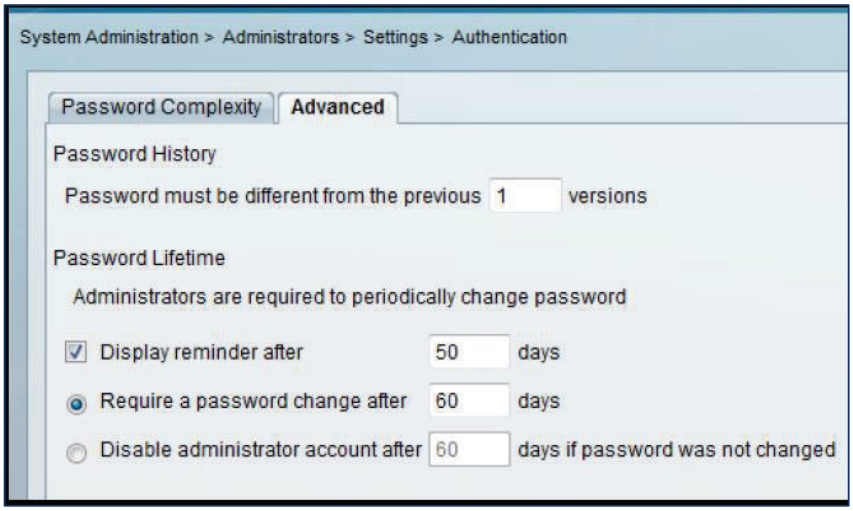


Figura 2.10 Tiempo de vida de las contraseñas [22]

2.1.4.4 BMC Remedy [23]

Es una herramienta gestora de tickets que funciona como un punto de contacto para las solicitudes de usuarios e incidentes. Los flujos de trabajo de esta herramienta permiten realizar el seguimiento de las incidencias desde su inicio hasta la correlación con problemas. En la **Figura 2.11** se presenta un ejemplo de los tickets gestionados por la herramienta descrita, el ticket señalado tiene asignada una prioridad baja y está en proceso de solución.

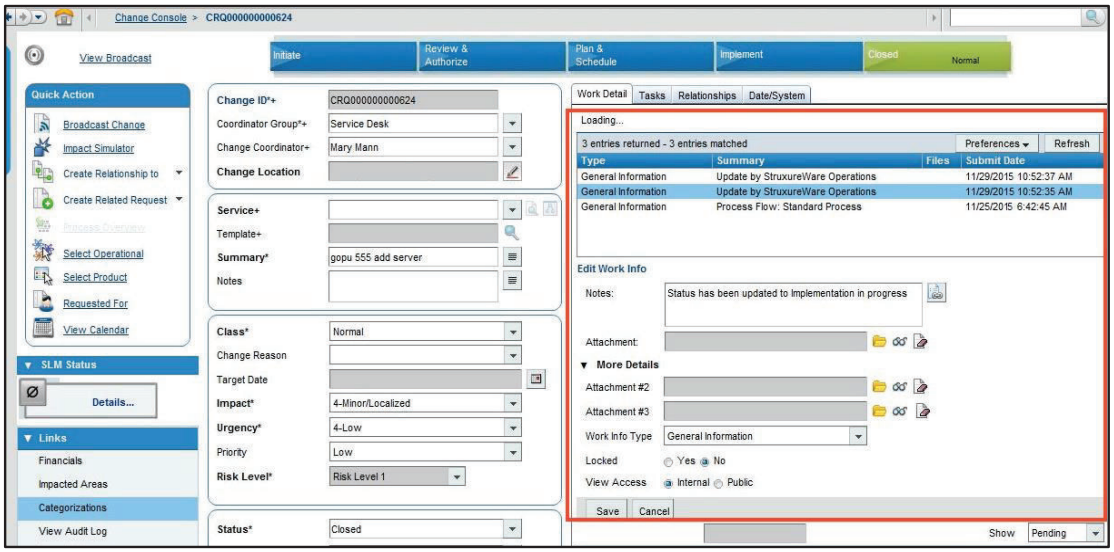


Figura 2.11 Vista de los tickets pendientes de resolución [24]

2.2 CRITERIOS DE COBIT 4.1 APLICADOS PARA LA AUDITORÍA DE LA SITUACIÓN ACTUAL DEL ÁREA DE O&M DE MPLS DE LA CNT E.P.

En la **Tabla 2.3** se presentan las áreas sugeridas por COBIT a ser analizadas para obtener el nivel de madurez de los procesos existentes, se asigna criterios P = Primario y S = Secundario para definir el nivel de importancia sobre el enfoque de cada área.

	MODELOS DE MADUREZ
ALINEAMIENTO ESTRATÉGICO	No aplica
ENTREGA DE VALOR	P
GESTIÓN DE RIESGOS	S
GESTIÓN DE RECURSOS	P
MEDICIÓN DEL DESEMPEÑO	S

Tabla 2.3 Áreas de enfoque del gobierno de TI alineadas al marco de trabajo COBIT 4.1 [3]

Para realizar el análisis enfocado a las áreas sugeridas por COBIT se desarrollarán matrices correspondientes a los procesos existentes del área, como son: matriz de valor y asignación de recursos, desempeño, riesgo, asignación de responsabilidades y finalmente se aplicará el modelo de madurez.

En la **Tabla 2.4** se muestran los criterios de información con su significado aplicados a los disparadores de valor definidos mediante COBIT 4.1 para los procesos de estudio del presente proyecto.

Efectividad	Tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
Eficiencia	Consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
Confidencialidad	Se refiere a la protección de información sensitiva contra revelación no autorizada.

Integridad	Está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
Disponibilidad	Se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
Cumplimiento	Tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
Confiabilidad	Se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Tabla 2.4 Criterios de Información de COBIT 4.1 [3]

Los recursos de TI referidos por COBIT se describen en la **Tabla 2.5** y se indicará en la matriz de valor cuáles de éstos han sido asignados para cumplir con los disparadores de cada proceso según la situación actual.

RECURSOS DE TI	
Aplicación	Sistemas que procesan información automáticos y manuales
Información	Representan los datos en todas sus formas que sean utilizados por el negocio.
Infraestructura	Tecnología e instalaciones donde se procesan las aplicaciones.
Personas	Personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información.

Tabla 2.5 Recursos de TI según COBIT 4.1 [3]

Debido a que COBIT define 6 niveles de cumplimiento, se emplea el factor de suma 20% para la calificación de cada nivel, se excluye el nivel NO CUMPLE ya que tiene un valor 0%. A continuación se presenta la fórmula para la obtención del factor de suma:

Ecuación 2-1: $$\mathrm{f} = \frac{p}{n}\%$$

$$f = \frac{100}{5} = 20\ \%$$

Donde **f** = Factor de cumplimiento, p = Porcentaje total (100), y n = Número de niveles de cumplimiento (5).

Nivel de Cumplimiento	Calificación
NO CUMPLE	0-19%
CUPLE LEVEMENTE	20-39%
CUMPLE PARCIALMENTE	40-59%
CUMPLE MAYORITARIAMENTE	60-79%
CUMPLE CASI TOTALMENTE	80-99%
CUMPLE TOTALMENTE	100%

Tabla 2.6 Porcentaje de calificación de desempeño

En la **Tabla 2.6** se presentan los porcentajes de calificación a ser aplicados para medir el desempeño de los procesos del área de O&M de MPLS en base a la auditoría realizada.

Para la obtención del desempeño total de cada proceso, se obtendrá el promedio de la calificación del nivel de cumplimiento sobre los procesos de control.

Ecuación 2-2: $$r = \frac{c}{n_p}$$

Donde, n_p = número de procesos de control, **c** = calificación del nivel de cumplimiento, y **r** = rendimiento.

En la **Tabla 2.7** se presenta la descripción de la probabilidad de riesgo de ocurrencia de un incidente con los valores asignados.

Probabilidad		
1	**Rara vez**	Poca probabilidad de ocurrencia
2	**Ocasional**	Sospecha, con baja probabilidad de ocurrencia
3	**Probable**	Sospecha, con alta probabilidad de ocurrencia
4	**Muy Probable**	Plena sospecha, con probabilidad de ocurrencia

Tabla 2.7 Probabilidad de ocurrencia de un incidente [3]

En la **Tabla 2.8** se presenta el impacto sobre el servicio en caso de ocurrir el incidente con su respectiva valoración.

Impacto		
1	**Menor**	Efectos menores, no significativos
2	**Moderado**	Efectos moderados, pero significativos
3	**Mayor**	Efectos Mayores y significativos
4	**Extremo**	Grandes consecuencias sobre los servicios TI

Tabla 2.8 Impacto sobre el servicio en caso de que ocurra el incidente [3]

Con los valores de la **Tabla 2.7** y **Tabla 2.8** se procede a realizar el producto entre la probabilidad y el impacto para obtener la matriz de riesgo representada en la **Figura 2.12**.

Ecuación 2-3 $$Riesgo = \text{Impacto} * \text{Probabilidad}$$

Ejemplo: $$Riesgo = \text{Ocasional}(2) * \text{Extremo}(4)$$

$$Riesgo = 2 * 4 = 8$$

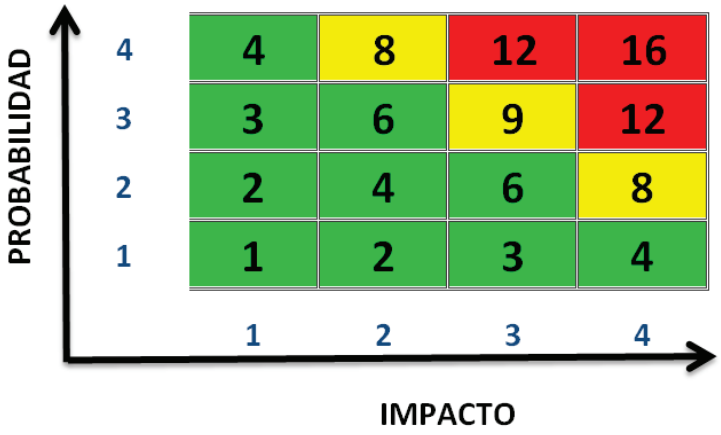


Figura 2.12 Matriz de Riesgo [25]

En la **Tabla 2.9** se describe la valoración del riesgo una vez obtenido el producto de la probabilidad y el impacto, los valores que implican cada uno de los riesgos definidos se visualizan en la **Figura 2.12**.

RIESGO	
Bajo	Baja pérdida o Daño. Puede ser susceptible de una amonestación o sanción moderada de la autoridad competente, no causa indemnización por perjuicios ni pérdida de clientes o disminución de ingresos por desprestigio, mala imagen o publicidad negativa.
Medio	Pérdida o daño medio. Puede ser susceptible de una sanción más estricta de la autoridad competente, de índole monetaria. Poca o media probabilidad de procesos penales, baja o media probabilidad de indemnización por perjuicios, poca o media probabilidad de pérdida de clientes, disminución de ingresos por desprestigio, mala imagen o publicidad negativa.
Alto	Alta pérdida o daño. Puede ser susceptible de cuantiosas multas de la autoridad competente y estrictas sanciones de suspensión, inhabilitación o remoción de administrador, oficial de cumplimiento y otros funcionarios. Alta probabilidad de procesos penales y pérdida de clientes; disminución de ingresos por desprestigio, mala imagen o publicidad negativa. Puede poner en peligro la solvencia de la entidad

Tabla 2.9 Valoración de Riesgo [26]

En la **Tabla 2.10** se observan los 6 niveles de madurez existentes tomados de COBIT 4.1, mismos que serán utilizados para medir la madurez de los procesos analizados en la situación actual del área aplicada en el presente proyecto.

0	No Existente	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1	Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2	Repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3	Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4	Administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada
5	Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Tabla 2.10 Criterios para calificación del nivel de madurez [3]

En la **Tabla 2.11** se describen los roles de la matriz de asignación de responsabilidades.

Rol		Descripción
R	Responsable	Responsable por el trabajo
A	A quién se rinde Cuentas	Aprueba el trabajo y es responsable
C	Consultado	Posee información y capacidad para concluir un trabajo
I	Informado	Debe ser informado de los resultados y el progreso de un trabajo

Tabla 2.11 Roles de la matriz RACI [3]

2.3 SITUACIÓN ACTUAL DE LOS PROCESOS DEL ÁREA DE O&M DE MPLS

Los resultados de la auditoría se reflejan a través de un conjunto de matrices que registran indicadores cualitativos y cuantitativos obtenidos de la aplicación de mediciones en base a los criterios de COBIT 4.1.

2.3.1 MATRIZ DE VALOR Y ASIGNACIÓN DE RECURSOS DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD

Tomando la guía *Assurance* de Cobit 4.1 [26] se han definido los disparadores de valor del proceso de administración de seguridad del dominio de entrega y soporte para acoplarlos a los procedimientos del área de O&M IP MPLS de la CNT E.P. según sus objetivos y la auditoría aplicada.

Posteriormente se califican los criterios de información con P= Primario y con S = Secundario mientras que los campos vacíos se consideran criterios menos importantes según lo actualmente aplicado por el área de O&M, adicionalmente se marcan los recursos utilizados para los disparadores mencionados.

De lo indicado anteriormente, se obtiene la matriz de valor de la **Tabla 2.12**.

DISPARADORES DE VALOR		CRITERIOS DE INFORMACIÓN							RECURSOS DE TI			
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS
DS5.1	Proteger los activos de TI críticos			P	P	P		P	✓	✓	✓	
	Plantear estrategias de seguridad de TI alineadas a las necesidades de negocio	P	P				S		✓			✓
	Implementar y mantener prácticas de seguridad consistentes con las leyes y reglamentos aplicables	P		S	P		P	S	✓	✓	✓	
DS5.2	Cumplir un plan de seguridad de TI que mantenga la satisfacción de los requerimientos de negocio y cubra los riesgos a que está expuesta la empresa.			S	S	P	P	P	✓	✓	✓	
	Administrar las inversiones en seguridad de TI de una manera consistente para habilitar el plan de seguridad	P	P				S			✓	✓	

DISPARADORES DE VALOR		CRITERIOS DE INFORMACIÓN							RECURSOS DE TI			
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS
DS5.2	Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.		S	P	S	P	P		✓	✓	✓	✓
	Los usuarios deben estar conscientes del plan de seguridad de TI			P		P	P		✓	✓	✓	✓
DS5.3	Aplicar efectivamente los cambios de seguridad			P	P	P	P	P	✓	✓	✓	✓
	Investigar adecuadamente actividades de acceso indebido			P	P	S	S	P	✓	✓	✓	✓
DS5.4	Gestionar cuentas de usuario consistentemente.	P	P	P	S	P	P	P	✓	✓	✓	✓
	Aplicar reglas y regulaciones para todo tipo de usuarios	P	P	P	P	P	S	P	✓	✓	✓	✓
	Detectar oportunamente los incidentes de seguridad				S		S		✓		✓	✓
	Proteger los sistemas informáticos y los datos confidenciales de los usuarios no autorizados	S	P	P	P	P	P	P	✓	✓	✓	✓
DS5.5	Asignar a personal con experiencia en pruebas de seguridad y vigilancia de los sistemas de TI			S			P		✓			✓
	Detectar brechas de seguridad proactivamente						P			✓		✓
DS5.6	Detectar incidentes de seguridad proactivamente			S			P		✓		✓	✓
	Generar informes de fallos de seguridad en un nivel definido y documentado			S	S	P	P		✓		✓	✓
	Comunicar los incidentes de seguridad			P		S	P			✓		✓
DS5.7	Mantener confiabilidad de la información		S	P	P	P	S	P		✓		✓
	Mantener los activos corporativos seguros		S	P	P	P		P	✓			✓
DS5.8	Definir y documentar la administración de claves	S	S	P	P	P	P	P	✓	✓	✓	✓

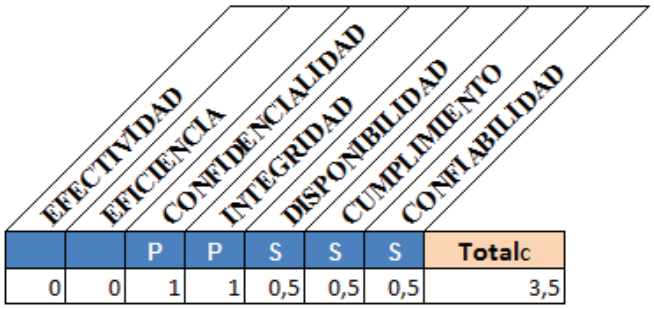
DISPARADORES DE VALOR		CRITERIOS DE INFORMACIÓN							RECURSOS DE TI			
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS
DS5.8	Manejar claves de forma segura	S	S	P	P	P	P	P	✓	✓	✓	✓
	Envío seguro de claves	S	S	P	S		S	S				✓
DS5.9	Asegurar los sistemas de seguridad mediante protección proactiva de malware			P	P		S		✓			✓
	Asegurar la integridad de los sistemas			S	P	P	S	P	✓		✓	✓
	Detectar oportunamente problemas de seguridad						P		✓			✓
DS5.10	Proteger la tecnología de seguridad corporativa	P		P	P		S	P	✓		✓	✓
	Administrar la seguridad de red consistentemente			P	P	P	P	P	✓		✓	✓
DS5.11	Disponer de medios de comunicación confiables											
	Intercambiar información confiablemente						S					✓
	Salvaguardar la integridad de sistemas y datos						S				✓	✓

Tabla 2.12 Matriz de disparadores de valor del proceso de seguridad

2.3.2 MATRIZ DE DESEMPEÑO DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD

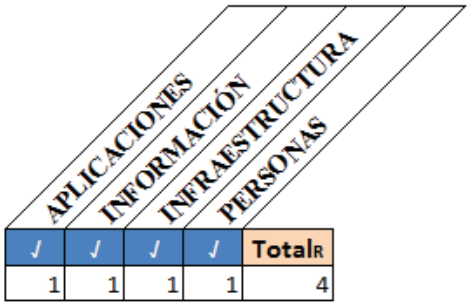
Una vez desarrollada la matriz de valor indicada en la **Tabla 2.12**, se procede con la medición del desempeño de los procesos de control de administración de seguridad DS5, para esto en la **Figura 2.13** y **Figura 2.14** se presentan los criterios y recursos que se deben asignar acorde a COBIT 4.1, en base a los cuales se ha realizado la comparación y se ha determinado el nivel de cumplimiento de los disparadores de valor correspondientes a los objetivos de control de este proceso.

Para medir el nivel de cumplimiento se asignarán valores a los criterios primario P= 1, secundario S=0,5 y para cada recurso se fijará ✓= 1. Esto se presenta en la Figura 2.13 y Figura 2.14 donde $Total_c$ es la suma de los valores asignados a los criterios de información y $Total_R$ corresponde valor total de recursos asignados.



EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	
		P	P	S	S	S	Totalc
0	0	1	1	0,5	0,5	0,5	3,5

Figura 2.13 Criterios de Información del proceso de Administración de Seguridad según COBIT 4.1 [3]



APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
✓	✓	✓	✓	TotalR
1	1	1	1	4

Figura 2.14 Recursos asignados por COBIT 4.1 del proceso de Administración de Seguridad [3]

Se sumará el valor total de los criterios de información con el de los recursos utilizados y este resultado corresponderá al 100%, con lo cual de acuerdo a lo especificado por COBIT indicará que el proceso de control se cumple totalmente. Es importante aclarar que los criterios y recursos que han sido utilizados por el área y no se alinean a los sugeridos por COBIT tendrán un valor de 0.

Ecuación 2-4

$$V_T = Total_c + Total_R$$

$$V_T = 3{,}5 + 4$$

$$V_T = 7{,}5 = 100\%$$

Para el proceso de administración de seguridad de acuerdo a lo especificado por COBIT el valor total que debe cumplir cada proceso de control es 7,5.

Para una mejor compresión, se detallarán dos ejemplos indicados a continuación.

Ejemplo 1: En el proceso de Administración de Identidad se tienen dos disparadores de valor. El primer disparador tiene como objetivo aplicar efectivamente los cambios de seguridad, para esto el área O&M IP MPLS toma como primarios los criterios de confidencialidad, integridad, disponibilidad, cumplimiento y confiablidad, además se verifica que los recursos asignados para este disparador son aplicaciones, información, infraestructura y personas.

El objetivo del segundo disparador es investigar adecuadamente las actividades de acceso indebido, para esto el área de operación y mantenimiento toma como primarios los criterios de confidencialidad, integridad y confiablidad y como secundarios la disponibilidad y cumplimiento, además se verifica que los recursos asignados para este disparador son aplicaciones, información, infraestructura y personas.

DISPARADOR DE VALOR	CRITERIOS DE INFORMACIÓN							RECURSOS DE TI				TOTAL V_T
	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
Aplicar efectivamente los cambios de seguridad			P	P	P	P	P	✓	✓	✓	✓	7,5
	0	0	1	1	0,5	0,5	0,5	1	1	1	1	
Investigar adecuadamente actividades de acceso indebido			P	P	S	S	P	✓	✓	✓	✓	7,5
	0	0	1	1	0,5	0,5	0,5	1	1	1	1	

Tabla 2.13 Ejemplo 1 de calificación de nivel de cumplimiento

Se debe promediar cada uno de los valores totales obtenidos de los disparadores para conocer el valor total del proceso de control V_P.

Ecuación 2-5 $$V_P = \frac{\sum V_T}{n_d}$$

Donde n_d es el número de disparadores de cada proceso de control.

$$V_P = \frac{7{,}5 + 7{,}5}{2}$$

$$V_P = \frac{15}{2} = 7{,}5$$

Cálculo del porcentaje total:

$$Cumplimiento = \frac{7{,}5 * 100\%}{7{,}5} = 100\% \approx Cumple\ Totalmente$$

Con el análisis descrito anteriormente, y en base a la **Tabla 2.6** se concluye que se abarcan los criterios de información y se asignan los recursos necesarios a los disparadores de administración de identidad por lo que se cumple totalmente con el proceso DS5.3 alineado a las necesidades del área.

Ejemplo 2: En el proceso de intercambio de datos sensitivos se tienen dos disparadores de valor. El primer disparador tiene como objetivo disponer de medios de comunicación confiables, para esto el área O&M IP MPLS toma como primarios los criterios de disponibilidad y cumplimiento, además se verifica que los recursos asignados para este disparador son información, y personas.

El segundo disparador tiene como objetivo intercambiar información confiablemente, para esto el área de operación y mantenimiento toma como criterio secundario la disponibilidad, además se verifica que se asigna a las personas como recurso para este disparador.

El tercer disparador tiene como objetivo salvaguardar la integridad de sistemas y datos, para esto el área toma como criterio primario la disponibilidad y como

secundario el cumplimiento, además los recursos utilizados son infraestructura, información, y personas.

DISPARADOR DE VALOR	CRITERIOS DE INFORMACIÓN							RECURSOS DE TI				TOTAL V_T
	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
Disponer de medios de comunicación confiables												0
	0	0	0	0	0	0	0	0	0	0	0	
Intercambiar información confiablemente						S					✓	1,5
	0	0	0	0	0	0,5	0	0	0	0	1	
Salvaguardar la integridad de sistemas y datos						S				✓	✓	2,5
	0	0	0	0	0	0,5	0	0	0	1	1	

Tabla 2.14 Ejemplo 2 de calificación de nivel de cumplimiento

Se debe promediar cada uno de los valores totales obtenidos de los disparadores para conocer el valor total del proceso de control V_P en base a la Ecuación 2-5.

$$V_P = \frac{\sum V_T}{n_d}$$

Donde n_d es el número de disparadores de cada proceso de control.

$$V_P = \frac{0 + 1{,}5 + 2{,}5}{3}$$

$$V_P = \frac{4}{3}$$

$$V_P = 1{,}33$$

Cálculo del porcentaje total:

$$Cumplimiento = \frac{1{,}33 * 100\%}{7{,}5} = 17{,}78\% \approx Cumple\ Levemente$$

Con el análisis realizado, y en base a la **Tabla 2.6** se concluye que para este proceso el área cumple levemente con los criterios básicos principales sugeridos por el marco de trabajo COBIT.

En la **Tabla 2.15** se muestran todos los porcentajes de cumplimiento asignados a los procesos de control en base a la **Tabla 2.6** con respecto a la administración de seguridad del área basados en la auditoria.

PROCESOS CONTROL DE SEGURIDAD DE TI		NO CUMPLE	CUMPLE LEVEMENTE	CUMPLE PARCIALMENTE	CUMPLE MAYORITARIAMENTE	CUMPLE CASI TOTALMENTE	CUMPLE TOTALMENTE	%
DS5.1	Administración de Seguridad TI				x			60
DS5.2	Plan de seguridad TI				x			68
DS5.3	Administración de Identidad						x	100
DS5.4	Administración de Cuentas de Usuario					x		80
DS5.5	Vigilancia y monitoreo			x				43,3
DS5.6	Definición de Incidentes de Seguridad			x				55,5
DS5.7	Protección de la Tecnología de Seguridad				x			70
DS5.8	Administración de Claves Criptográficas					x		82,2
DS5.9	Prevención, Detección y Corrección de Software Malicioso			x				44,4
DS5.10	Seguridad de Red					x		83,3
DS5.11	Intercambio de Datos Sensitivos		x					17,78

Tabla 2.15 Matriz de desempeño de los procesos de control de seguridad.

Para la obtención del valor total del desempeño del proceso de administración de seguridad se aplicará la Ecuación 2-2 en la cual se suman los porcentajes de cada proceso de control y se divide para el total de procesos con el propósito de obtener el valor promedio.

$$r = \frac{c}{n_p}$$

$$r = \frac{704{,}48}{11}$$

$$r = 64{,}04\%$$

Por lo tanto, se tiene que el desempeño del proceso de administración de seguridad del área alcanza un 64,24%.

2.3.3 MATRIZ DE RIESGOS DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD

Utilizando la guía *Assurance* de Cobit 4.1 [26] se obtienen los disparadores sobre los que se analiza el riesgo en base a la probabilidad de ocurrencia y el impacto que produciría sobre los servicios ofrecidos por el área O&M MPLS, esto se realizará tomando los valores obtenidos en la matriz de riesgo de la **Figura 2.12**.

PROCESO DE ADMINISTRACIÓN DE SEGURIDAD	PROBABILIDAD				IMPACTO				RIESGO
	1	2	3	4	1	2	3	4	
Disparadores de Riesgo	Rara vez	Ocasional	Probable	Muy probable	Menor	Moderado	Mayor	Extremo	
Falta de gobernanza de la seguridad de TI		x					x		6
Objetivos de negocio y de TI desalineados			x				x		9
Activos de datos e información sin protección.	x							x	4
Falta de conocimiento del plan de seguridad				x		x			8
Medidas de seguridad comprometidas por los interesados y usuarios		x					x		6
Cambios no autorizados en hardware y software	x							x	4
Requisitos de seguridad no especificados para todo el sistema.				x		x			8
Violación de la seguridad		x						x	8
Información comprometida del sistema.		x						x	8
Brechas de seguridad		x					x		6
Falta de cumplimiento de las políticas de seguridad			x				x		9
Incidentes de seguridad no resueltos de manera oportuna		x					x		6

PROCESO DE ADMINISTRACIÓN DE SEGURIDAD	PROBABILIDAD				IMPACTO				RIESGO
	1	2	3	4	1	2	3	4	
Disparadores de Riesgo	**Rara vez**	**Ocasional**	**Probable**	**Muy probable**	**Menor**	**Moderado**	**Mayor**	**Extremo**	
Afectación de la seguridad a causa del cierre inoportuno de cuentas no utilizadas.	x						x		3
Uso inadecuado de cuentas de usuarios que comprometen la seguridad de la organización	x							x	4
Violaciones de seguridad no detectadas	x							x	4
Registros de seguridad poco fiables	x					x			2
Divulgación de activos corporativos e información a personas no autorizadas.	x							x	4
Exposición de información	x							x	4
Claves mal utilizadas por personas no autorizadas	x							x	4
Registro de usuarios no verificados que comprometen el sistema de seguridad	x						x		3
Sistemas y datos propensos a ataques		x					x		6
Contra medidas Ineficientes		x				x			4
Detección inoportuna del incumplimiento de las normas de seguridad	x						x		3
Información sensible expuesta		x						x	8
Conexiones externas a sitios remotos no autorizadas	x					x			2

Tabla 2.16 Matriz de Riesgo del proceso de administración de seguridad

Para la obtención del riesgo del proceso de administración de seguridad al que se encuentra expuesta el área, se obtendrá el promedio de los valores de riesgo obtenidos en la **Tabla 2.16**.

Donde, $\boldsymbol{d_r}$ = número de disparadores de riesgo, $\boldsymbol{s_r}$ = suma total del riesgo y $\boldsymbol{r_e}$ = riesgo estimado.

Ecuación 2-6:

$$r_e = \frac{\boldsymbol{s_r}}{\boldsymbol{d_r}}$$

$$r_e = \frac{133}{25} = r_e = 5{,}32 \approx 5$$

En base al resultado obtenido, se estima que este proceso se encuentra en un riesgo bajo de acuerdo a la matriz de la **Figura 2.12**.

2.3.4 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD

Como parte del análisis se verifican los roles (**Tabla 2.11**) de las actividades de este proceso y se los alinea con las funciones dentro de la estructura del área esto se lo detalla mediante la Matriz RACI en la **Tabla 2.18**.

ACTIVIDADES	GERENTE MPLS	GESTOR TÉCNICO	GESTOR DE PROYECTOS Y LOGÍSTICA
Definir y mantener un plan de seguridad de TI	I	R/A	C/I
Definir, establecer y operar un proceso de administración de identidad (cuentas)	I	R/A	C/I
Monitorear incidentes de seguridad, reales y potenciales	I	R/A	I
Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios		R	
Realizar evaluaciones de vulnerabilidades de manera regular	I	R/A	I

Tabla 2.17 Matriz RACI del proceso de Administración de Seguridad

2.3.5 MODELO DE MADUREZ DEL PROCESO DE ADMINISTRACIÓN DE SEGURIDAD

En base a los resultados obtenidos en las matrices de valor, recursos, desempeño y riesgos se pudo concluir que existen procedimientos estandarizados mediante la norma ISO 27000 que están documentados y han sido difundidos, no solo dentro del área sino a nivel de empresa, sin embargo, se verifica que no se realiza medición continua del proceso para el planteamiento de mejoras y tampoco se cumple en su totalidad con el objetivo de control del proceso de administración de seguridad planteado por COBIT 4.1.

En la **Tabla 2.18** se presenta el nivel de madurez definido para este proceso, el cual se obtiene en base a lo mencionado anteriormente y lo especificado en el modelo de la **Tabla 2.10**.

MODELO DE MADUREZ	
Proceso:	**PROCESO DE ADMINISTRACIÓN DE SEGURIDAD**
Objetivo de Control:	La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.
RIESGO	BAJO
DESEMPEÑO	64,04%
MADUREZ	**3**

Tabla 2.18 Nivel de Madurez del proceso de administración de seguridad

2.3.6 MATRIZ DE VALOR DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS

En base a la guía de *Assurance* de Cobit 4.1 [26] se han definido los disparadores de valor del dominio de administración de problemas y se han alineado a los existentes en el área de O&M IP MPLS con la información obtenida de la auditoría.

Después se califican los criterios de información con P= Primario y con S = Secundario mientras que los campos vacíos se consideran criterios menos importantes según lo actualmente aplicado por el área de O&M.

Adicionalmente se marcan con un visto los recursos utilizados para los disparadores mencionados. Esta calificación se presenta en la **Tabla 2.19**.

DISPARADORES DE VALOR		CRITERIOS DE INFORMACIÓN							RECURSOS DE TI			
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS
DS10.1	Brindar herramientas de soporte para el rendimiento del *service desk* orientado a problemas.									✓		✓
	Administrar proactivamente los problemas										✓	✓
	Manejar eficiente y efectivo de problemas		S				S					✓
	Resolver oportunamente problemas e incidentes	S	S				P		✓		✓	✓
	Mejorar la calidad de servicios TI					S	P				✓	✓
DS10.2	Resolver apropiadamente los problemas de acuerdo a los niveles de servicio acordados						P			✓	✓	✓
	Minimizar el tiempo para detección y resolución de problemas					P	S			✓	✓	
DS10.3	Resolver consultas dentro del plazo acordado						P	P	✓	✓	✓	
	Mejorar la satisfacción de clientes y usuarios						P			✓	✓	
	Tener la capacidad de aplicar las lecciones aprendidas al abordar problemas similares en el futuro						S			✓	✓	
DS10.4	Documentar y notificar los problemas de incidentes						S		✓		✓	
	Gestionar de forma eficaz los servicios		S				P				✓	✓

Tabla 2.19 Matriz de valor del proceso de problemas

2.3.7 MATRIZ DE DESEMPEÑO DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS

Una vez desarrollada la matriz de valor indicada en la Tabla 2.19, se procede con la medición del desempeño de los procesos de control de administración de problemas DS10 aplicados a las actividades del área de O&M IP MPLS.

Para esto, en la **Figura 2.15** y **Figura 2.16** se presentan los criterios y recursos que deben asignarse respectivamente acorde a COBIT 4.1, en base a los cuales se ha realizado la comparación y se ha determinado el nivel de cumplimiento de los disparadores de valor correspondientes a los objetivos de control.

Para medir el nivel de cumplimiento se asignarán valores a los criterios primario P= 1, secundario S=0,5 y para cada recurso se fijará ✓= 1. Esto se presenta en la Figura 2.15 y Figura 2.16 donde $Total_c$ es la suma de los valores asignados a los criterios de información y $Total_R$ corresponde valor total de recursos asignados.

EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	
P	P			S			$Total_C$
1	1	0	0	0,5	0	0	2,5

Figura 2.15 Criterios de Información del proceso de Administración de Problemas según COBIT 4.1 [3]

APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
✓	✓	✓	✓	$Total_R$
1	1	1	1	4

Figura 2.16 Recursos asignados por COBIT 4.1 del proceso de Administración de problemas [3]

Se sumará el valor total de los criterios de información con el de los recursos utilizados y este resultado corresponderá al 100%, con lo cual de acuerdo a lo especificado por COBIT indicará que el proceso de control se cumple totalmente. Es importante aclarar que los criterios y recursos que han sido utilizados por el área y no se alinean a los sugeridos por COBIT tendrán un valor de 0.

$$V_T = Total_c + Total_R$$
$$V_T = 2{,}5 + 4 = 6{,}5 = 100\%$$

Para el proceso de administración de problemas de acuerdo a lo especificado por COBIT el valor total que debe cumplir cada proceso de control es 6,5.

Para una mejor compresión, se describen dos ejemplos indicados a continuación.

Ejemplo 1: En el proceso rastreo y resolución de Problemas (DS10.2) se tienen dos disparadores de valor. El primer disparador tiene como objetivo resolver apropiadamente los problemas de acuerdo a los niveles de servicio acordados, para esto el área toma como primario el criterio de cumplimiento, además se verifica que los recursos asignados para este disparador información, infraestructura y personas.

El objetivo del segundo disparador es Minimizar el tiempo para detección y resolución de problemas, para esto el área de operación y mantenimiento toma como primarios el criterio de disponibilidad y como secundario el de cumplimiento, además se verifica que los recursos asignados para este disparador son información e infraestructura.

DISPARADOR DE VALOR	CRITERIOS DE INFORMACIÓN							RECURSOS DE TI				TOTAL V_T
	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
Resolver apropiadamente los problemas de acuerdo a los niveles de servicio acordados						P			✓	✓	✓	3
	0	0	0	0	0	0	0	0	1	1	1	
Minimizar el tiempo para detección y resolución de problemas					P	S			✓	✓		2,5
	0	0	0	0	0,5	0	0	0	1	1	0	

Tabla 2.20 Ejemplo 1 de calificación de nivel de cumplimiento

Se debe promediar cada uno de los valores totales obtenidos de los disparadores para conocer el valor total del proceso de control V_P en base a la Ecuación 2-5.

$$V_P = \frac{\sum V_T}{n_d}$$

Donde n_d es el número de disparadores de cada proceso de control.

$$V_P = \frac{3 + 2{,}5}{2}$$

$$V_P = \frac{5{,}5}{2} = 2{,}75$$

Cálculo del porcentaje total:

$$Cumplimiento = \frac{2{,}75 * 100\%}{6{,}5} = 42{,}31\% \approx Cumple\ Parcialmente$$

Con el análisis descrito anteriormente, se realiza una comparación con los criterios sugeridos por COBIT 4.1 y se concluye que no se toman los criterios de información y tampoco se asignan los recursos necesarios para rastrear y solucionar los problemas por lo que se cumple parcialmente con el proceso DS10.2

Ejemplo 2: En el proceso de integración de configuración, incidentes y administración de problemas (DS10.4) se tienen dos disparadores de valor, el primero tiene como objetivo documentar y notificar los problemas, para esto el área O&M IP MPLS toma como secundario el criterio de cumplimiento, además se verifica que los recursos asignados para este disparador aplicaciones e infraestructura.

El objetivo del segundo disparador es Minimizar el tiempo para detección y resolución de problemas, para esto el área de operación y mantenimiento toma como primario el criterio de cumplimiento y como secundario el de eficiencia, además se verifica que los recursos asignados para este disparador son infraestructura y personas.

DISPARADOR DE VALOR	CRITERIOS DE INFORMACIÓN							RECURSOS DE TI				TOTAL V_T
	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
Documentar y notificar los problemas de incidentes						S		✓		✓		2
	0	0	0	0	0	0	0	1	0	1	0	
Gestionar de forma eficaz los servicios		S				P				✓	✓	2,5
	0	0,5	0	0	0	0	0	0	0	1	1	

Tabla 2.21 Ejemplo 2 de calificación de nivel de cumplimiento

Se debe promediar cada uno de los valores totales obtenidos de los disparadores para conocer el valor total del proceso de control V_P.

$$V_P = \frac{\sum V_T}{n_d}$$

Donde n_d es el número de disparadores de cada proceso de control.

$$V_P = \frac{2 + 2{,}5}{2}$$

$$V_P = \frac{4{,}5}{2}$$

$$V_P = 2{,}25$$

Cálculo del porcentaje total:

$$Cumplimiento = \frac{2{,}25 * 100\%}{6{,}5}$$

$$Cumplimiento = 34{,}62\% \approx Cumple\ Levemente$$

Con el análisis realizado, y en base a la **Tabla 2.6** se concluye que para este proceso el área cumple levemente con los criterios básicos principales sugeridos por el marco de trabajo COBIT.

Con el análisis realizado anteriormente, se compara con los criterios de información y los recursos que se deben asignar a este proceso sugeridos por COBIT 4.1 y se concluye que no se toman los criterios de información y tampoco se asignan los recursos necesarios para rastrear y solucionar los problemas por lo que se cumple levemente con el proceso DS10.4.

En la **Tabla 2.22** se muestran los porcentajes de cumplimiento asignados a los procesos de control en base a la **Tabla 2.19** con respecto a la administración de problemas del área basados en la auditoria.

	PROCESOS CONTROL DE PROBLEMAS	NO CUMPLE	CUMPLE LEVEMENTE	CUMPLE PARCIALMENTE	CUMPLE MAYORITARIAMENTE	CUMPLE CASI TOTALMENTE	CUMPLE TOTALMENTE	%
DS10.1	Identificación y Clasificación de Problemas		**x**					35,38
DS10.2	Rastreo y Resolución de Problemas			**x**				42,31
DS10.3	Cierre de problemas		**x**					35,38
DS10.4	Integración de configuración, incidentes y administración de Problemas		**x**					34,62

Tabla 2.22 Matriz de desempeño de los procesos de control de problemas

Para la obtención del valor total del desempeño actual del proceso de administración de problemas se aplicará la Ecuación 2-2 en la cual se obtiene el total de los porcentajes de cada proceso de control mediante su suma y se divide para el total de procesos.

$$r = \frac{c}{n_p}$$

$$\mathrm{r} = \frac{147{,}49}{4}$$

$$\mathrm{r} = 36{,}87\%$$

Por lo tanto, se tiene que el desempeño del proceso de administración de seguridad del área alcanza un 36,87%.

2.3.8 MATRIZ DE RIESGOS DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS

Para el análisis del riesgo del proceso de administración de problemas se obtienen los disparadores utilizando la guía *Assurance* de Cobit 4.1 [26], posteriormente se los analiza individualmente en base a la probabilidad de ocurrencia y el impacto que produciría en caso de que ocurra sobre los servicios ofrecidos por el área O&M MPLS, esto se realizará tomando los valores obtenidos en la matriz de riesgo de la **Figura 2.12**.

PROCESO DE ADMINISTRACIÓN DE PROBLEMAS	PROBABILIDAD				IMPACTO				Riesgo
	1	2	3	4	1	2	3	4	
Disparadores de Riesgo	Rara vez	Ocasional	Probable	Muy probable	Menor	Moderado	Mayor	Extremo	
Interrupción de servicios IT		x						x	8
Aumento de la probabilidad de recurrencia de problemas			x					x	12
Problemas e incidentes no resueltos oportunamente		x					x		6
Falta de pistas de problemas con sus soluciones para una administración controlada.			x			x			6
Pérdida de información	x							x	4
Incidentes críticos no solventados adecuadamente		x					x		6
Calidad de servicio insuficiente	x						x		3
Consultas pendientes			x			x			6
La insatisfacción con los servicios de TI			x				x		9
Incidentes críticos no resueltos adecuadamente			x					x	12
Aumento del número de problemas		x						x	8

Tabla 2.23 Matriz de Riesgo del proceso de administración de Problemas

Para la obtención del riesgo del proceso de administración de problemas al que se encuentra expuesta el área, se obtendrá el promedio de los valores de riesgo obtenidos en la **Tabla 2.23**.

Donde, $\boldsymbol{d_r}$ = número de disparadores de riesgo, $\boldsymbol{s_r}$ = suma total del riesgo y $\boldsymbol{r_e}$ = riesgo estimado.

Ecuación 2-7:

$$r_e = \frac{s_r}{d_r}$$

$$r_e = \frac{80}{11}$$

$$r_e = 7{,}27 \approx 7$$

En base al resultado obtenido, se estima que este proceso se encuentra en un riesgo medio de acuerdo a la matriz de la **Figura 2.12**.

2.3.9 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS

Como parte del análisis se verifican los roles (**Tabla 2.11**) de las actividades de este proceso y se los alinea con las funciones dentro de la estructura del área, esto se lo presenta mediante la Matriz RACI en la **Tabla 2.24**.

Actividades	GERENTE MPLS	GESTOR TÉCNICO	GESTOR DE PROYECTOS Y LOGÍSTICA	O&M BACKBONE Y CORE MPLS
Identificar y clasificar problemas				
Realizar un análisis de la causa raíz		I/R		R
Resolver problemas	I	R/I/A	I	R/A
Revisar el status de los problemas				
Emitir recomendaciones para mejorar y crear una solicitud de cambio relacionada		R	I	
Mantener registros de los problemas		R		

Tabla 2.24 Matriz RACI del Proceso de Administración de Problemas

2.3.10 MODELO DE MADUREZ DEL PROCESO DE ADMINISTRACIÓN DE PROBLEMAS

En base a los resultados obtenidos en las matrices de valor, recursos, desempeño y riesgos se pudo verificar que la organización ha reconocido que los problemas existen y requieren ser resueltos sin embargo, no existen procesos estándar y su administración es desorganizada.

Además en el área los problemas se los ha tratado como incidentes por lo que no cumple con el objetivo de control del proceso de administración de problemas planteado por COBIT 4.1.

En la **Tabla 2.25** se presenta el nivel de madurez definido para este proceso, el cual se obtiene en base a lo mencionado anteriormente y lo especificado en el modelo de la **Tabla 2.10**.

MODELO DE MADUREZ	
Proceso:	**PROCESO DE ADMINISTRACIÓN DE PROBLEMAS**
Objetivo de Control:	Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas de su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros y problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.
IMPACTO	MEDIO
DESEMPEÑO	36,87%
MADUREZ	**1**

Tabla 2.25 Nivel de Madurez del proceso de administración de problemas

2.3.11 MATRIZ DE VALOR DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK*

Tomando en cuenta la guía de *Assurance* de Cobit 4.1 [26] se han definido los disparadores de valor del dominio de administración de incidentes y *service desk*

para alinearlos a los existentes en el área de O&M IP MPLS con la información obtenida de la auditoría. Posteriormente se califican los criterios de información con P= Primario y con S = Secundario mientras que los campos vacíos se consideran criterios menos importantes según lo actualmente aplicado por el área.

Adicionalmente se marcan con un visto los recursos utilizados para los disparadores mencionados. Esta calificación se presenta en la **Tabla 2.26**.

DISPARADORES DE VALOR		CRITERIOS DE INFORMACIÓN							RECURSOS DE TI			
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS
DS8.1	Incrementar la satisfacción del cliente	S	S				P		✓		✓	✓
DS8.1	Realizar el seguimiento oportuno a los incidentes reportados y brindar una acertada resolución	S	P			S	P		✓	✓		✓
DS8.2	Resolución eficiente y oportuna de incidentes	P	P				S					✓
	Brindar valor agregado para usuarios finales						S		✓			
	Asignar responsabilidades para la resolución de incidentes	S	P				P					✓
DS8.3	Seguir el progreso de la resolución de incidentes						S					✓
DS8.4	Levantar un proceso de resolución de incidentes consistente y sistemático						S					✓
	Prevenir la repetición de incidentes		P				S					✓
DS8.5	Disminuir del tiempo de inactividad del servicio	P	P				P			✓		✓
	Confianza en los servicios ofrecidos	P	P				P				✓	✓

Tabla 2.26 Matriz de valor del proceso de incidentes y *service desk*.

2.3.12 MATRIZ DE DESEMPEÑO DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK*

Una vez desarrollada la matriz de valor indicada en la **Tabla 2.26**, se realiza la medición del desempeño de los procesos de control de administración de incidentes y *service desk* DS8 aplicados a las actividades del área de O&M.

Para medir el nivel de cumplimiento se asignarán valores a los criterios primario P= 1, secundario S=0,5 y para cada recurso se fijará √= 1. Para esto, en la **Figura 2.17** y **Figura 2.18** se presentan los criterios y recursos que deben asignarse respectivamente acorde a COBIT 4.1, en base a los cuales se ha realizado la comparación y se ha determinado el nivel de cumplimiento de los disparadores de valor correspondientes a los objetivos de control. Adicionalmente, $Total_c$ corresponde a la suma de los valores asignados a los criterios de información y $Total_R$ corresponde valor total de recursos asignados

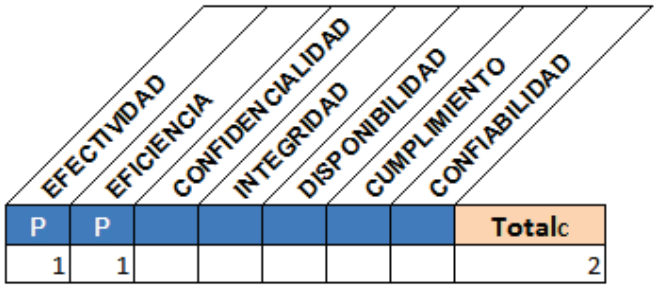


Figura 2.17 Criterios de Información del proceso de Administración de Incidentes y *Service Desk* según COBIT 4.1 [3]

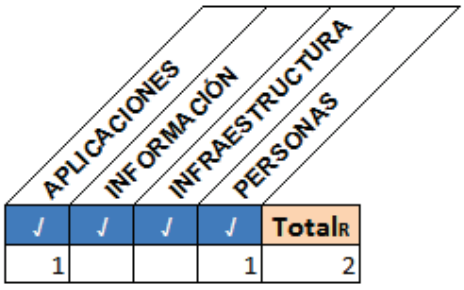


Figura 2.18 Recursos asignados por COBIT 41 del proceso de Administración de Incidentes y *Service Desk* [3]

Se sumará el valor total de los criterios de información con el de los recursos utilizados en base a la Ecuación 2-4 y este resultado corresponderá al 100%, con lo cual de acuerdo a lo especificado por COBIT indicará que el proceso de control se cumple totalmente.

Es importante aclarar que los criterios y recursos que han sido utilizados por el área y no se alinean a los sugeridos por COBIT tendrán un valor de 0.

$$V_T = Total_c + Total_R$$
$$V_T = 2 + 2$$
$$V_T = 4 = 100\%$$

Para el proceso de administración de incidentes y *service desk* de acuerdo a lo especificado por COBIT el valor total que debe cumplir cada proceso de control es 4.

Para una mejor compresión, se describen dos ejemplos indicados a continuación.

Ejemplo 1: En el proceso de Registro de Consultas de Clientes (DS8.2) se tienen tres disparadores de valor, el primero tiene como objetivo resolver eficiente y oportunamente los incidentes, para esto el área O&M IP MPLS toma como primarios los criterios de efectividad y eficiencia y como secundario el cumplimiento, además se verifica que para este disparador se utilizan las personas como recurso.

El objetivo del segundo disparador es brindar valor agregado a usuarios finales, para esto el área toma como secundario el criterio de eficiencia, además se verifica que para este disparador se utilizan las personas como recurso.

El objetivo del tercer disparador es brindar asignar responsabilidades para la resolución de incidentes, para esto el área toma como primarios los criterios de eficiencia y cumplimiento y como secundario el de efectividad, además se verifica que para este disparador se utiliza como recurso a las personas.

DISPARADOR DE VALOR	CRITERIOS DE INFORMACIÓN							RECURSOS DE TI				TOTAL V_T
	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
Resolución eficiente y oportuna de incidentes	P	P				S					✓	
	1	1	0	0	0	0	0	0	0	0	1	3
Brindar valor agregado para usuarios finales						S		✓				
	0	0	0	0	0	0	0	1	0	0	0	1
Asignar responsabilidades para la resolución de incidentes	S	P				P					✓	
	0,5	1	0	0	0	0	0	0	0	0	1	2,5

Tabla 2.27 Ejemplo 1 de calificación de nivel de cumplimiento Administración incidentes y *service desk*

Se debe promediar cada uno de los valores totales obtenidos de los disparadores para conocer el valor total del proceso de control V_P.

$$V_P = \frac{\sum V_T}{n_d}$$

Donde n_d es el número de disparadores de cada proceso de control.

$$V_P = \frac{3 + 1 + 2{,}5}{3}$$

$$V_P = \frac{6{,}5}{3} = 2{,}17$$

Cálculo del porcentaje total:

$$Cumplimiento = \frac{2{,}17 * 100\%}{4} = 54{,}17\% \approx Cumple\ Parcialmente$$

Con el análisis realizado, y en base a la **Tabla 2.6** se concluye que para este proceso el área cumple parcialmente con los criterios básicos principales sugeridos por el marco de trabajo COBIT.

Ejemplo 2: En el proceso de cierre de incidentes (DS8.4) se tienen dos disparadores de valor, el primero tiene como objetivo levantar un proceso de resolución de incidentes consistente y sistemático, para esto el área O&M IP MPLS toma como secundario el criterio de cumplimiento, además se verifica que el recurso asignado para este disparador son las personas.

El objetivo del segundo disparador es prevenir la repetición de incidentes, para esto el área de operación y mantenimiento toma como primario el criterio de eficiencia y como secundario el de cumplimiento puesto que no existe un proceso normalizado para realizarlo, además se verifica que el recurso asignado para este disparador son las personas.

En la **Tabla 2.28** se presenta la calificación de los disparadores de valor del proceso cierre de problemas aplicado al área O&M IP MPLS.

DISPARADOR DE VALOR	CRITERIOS DE INFORMACIÓN							RECURSOS DE TI				TOTAL V_T
	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	
Levantar un proceso de resolución de incidentes consistente y sistemático						S					✓	
	0	0	0	0	0	0	0	0	0	0	1	1
Prevenir la repetición de incidentes		P				S					✓	
	0	1	0	0	0	0	0	0	0	0	1	2

Tabla 2.28 Ejemplo 2 de calificación de nivel de cumplimiento Administración incidentes y *service desk*

Se debe promediar cada uno de los valores totales obtenidos de los disparadores para conocer el valor total del proceso de control V_P.

$$V_P = \frac{\sum V_T}{n_d}$$

Donde n_d es el número de disparadores de cada proceso de control.

$$V_P = \frac{1+2}{2}$$

$$V_P = \frac{3}{2} = 1{,}5$$

Cálculo del porcentaje total:

$$Cumplimiento = \frac{1{,}5 * 100\%}{4}$$

$$Cumplimiento = 37{,}5\% \approx Cumple\ Levemente$$

Con el análisis realizado, y en base a la **Tabla 2.6** se concluye que para este proceso el área cumple levemente con los criterios básicos principales sugeridos por el marco de trabajo COBIT.

En la **Tabla 2.29** se muestran los porcentajes de cumplimiento asignados a los procesos de control en base a la **Tabla 2.26** con respecto a la administración de problemas del área basados en la auditoria.

PROCESOS CONTROL DE SEGURIDAD DE TI		NO CUMPLE	CUMPLE LEVEMENTE	CUMPLE PARCIALMENTE	CUMPLE MAYORITARIAMENTE	CUMPLE CASI TOTALMENTE	CUMPLE TOTALMENTE	%
DS8.1	Mesa de Servicios					x		81,25
DS8.2	Registro de Consultas de Clientes			x				54,17
DS8.3	Escalamiento de Incidentes		x					25
DS8.4	Cierre de incidentes		x					37,5
DS8.5	Reportes y análisis de tendencias					x		87,5

Tabla 2.29 Matriz de desempeño de los procesos de control de incidentes y *service desk*

Para la obtención del valor total del desempeño actual del proceso de administración de incidentes y *service desk* se aplicará la Ecuación 2-2 en la cual se obtiene el total de los porcentajes de cada proceso de control mediante su suma y se divide para el total de procesos.

$$r = \frac{c}{n_p}$$

$$\mathrm{r} = \frac{285{,}42}{5}$$

$$\mathrm{r} = 57{,}05\%$$

Por lo tanto, se tiene que el desempeño del proceso de administración de incidentes y *service desk* es 57,05%.

2.3.13 MATRIZ DE RIESGOS DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK*

Para el análisis del riesgo del proceso de administración de incidentes y *service desk* se obtienen los disparadores utilizando la guía *Assurance* de Cobit 4.1 [26], posteriormente se los analiza individualmente en base a la probabilidad de ocurrencia y el impacto que produciría en caso de que ocurra sobre los servicios ofrecidos por el área O&M MPLS, esto se realizará tomando los valores obtenidos en la matriz de riesgo de la **Figura 2.12**.

ADMINISTRACIÓN DE INCIDENTES	PROBABILIDAD				IMPACTO				RIESGO
	1	2	3	4	1	2	3	4	
Disparadores de Riesgo	**Rara vez**	**Ocasional**	**Probable**	**Muy probable**	**Menor**	**Moderado**	**Mayor**	**Extremo**	
Incremento de tiempos de indisponibilidad del servicio		x						x	8
Decremento de la satisfacción del cliente		x					x		6
Desconocimiento de los usuarios del procedimiento para reportar un incidente.			x				x		9
Problemas recurrentes no direccionados			x				x		9

ADMINISTRACIÓN DE INCIDENTES	PROBABILIDAD				IMPACTO				RIESGO
	1	2	3	4	1	2	3	4	
Disparadores de Riesgo	Rara vez	Ocasional	Probable	Muy probable	Menor	Moderado	Mayor	Extremo	
Incidentes no detectados	x							x	4
Priorización errónea de incidentes		x					x		6
Incidentes no resueltos oportunamente		x						x	8
Uso ineficiente de recursos		x				x			4
Falta de seguimiento a la resolución de incidentes		x					x		6
Recopilación de información incorrecta	x						x		3
Incidentes resueltos inadecuadamente	x							x	4
Clientes insatisfechos	x							x	4
Tiempos de inactividad del cliente en aumento		x						x	8

Tabla 2.30 Matriz de Riesgo del proceso de administración de incidentes y *service desk*

Para obtener el riesgo al que se encuentra expuesta el área a este proceso, se obtendrá el promedio de los valores de riesgo obtenidos en la **Tabla 2.30**.

Donde, $\boldsymbol{d_r}$ = número de disparadores de riesgo, $\boldsymbol{s_r}$ = suma total del riesgo y $\boldsymbol{r_e}$ = riesgo estimado.

Ecuación 2-8:

$$r_e = \frac{s_r}{d_r}$$

$$r_e = \frac{79}{13}$$

$$r_e = 6{,}07$$

$$r_e \approx 6$$

En base al resultado obtenido, se estima que este proceso se encuentra en un riesgo medio de acuerdo a la matriz de la Figura 2.12.

2.3.14 MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK*

Como parte del análisis se verifican los roles presentados en la **Tabla 2.11** de las actividades de este proceso y se los alinea con las funciones dentro de la estructura del área, esto se lo presenta mediante la Matriz RACI en la **Tabla 2.31**.

Actividades	GERENTE MPLS	GESTOR TÉCNICO	GESTOR DE PROYECTOS Y LOGÍSTICA	O&M BACKBONE Y CORE MPLS	JEFE NOC	NOC
Crear procedimientos de clasificación (severidad e impacto) y de escalamiento (funcional y jerárquicos)	I	R	C/I	I/C	I	I
Detectar y registrar incidentes/ solicitudes de servicio/ solicitudes de Información	I/C	R/C		C	A/C/R	R/A
Clasificar, investigar y diagnosticar consultas					I/C	R/A
Resolver, recuperar y cerrar incidentes	I	I/C/R	I	R/C/I/A	A	R/A
Informar a usuarios						R/A
Hacer reportes para la gerencia	I	R			R	

Tabla 2.31 Matriz RACI del proceso de administración de incidentes y *service desk*

2.3.15 MODELO DE MADUREZ DEL PROCESO DE ADMINISTRACIÓN DE INCIDENTES Y *SERVICE DESK*

En base a los resultados obtenidos en las matrices de valor, recursos, desempeño y riesgos se pudo verificar que no existe un entrenamiento formal de los procedimientos y se deja que se ejecuten bajo la responsabilidad de los miembros del área por lo que es muy probable que se presenten errores al momento de resolver incidentes ya que en algunas ocasiones, el personal no cuenta con la experiencia suficiente.

MODELO DE MADUREZ	
Proceso:	**PROCESO DE ADMINISTRACIÓN DE CONSULTAS Y *SERVICE DESK***
Objetivo de Control:	Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.
IMPACTO	MEDIO
DESEMPEÑO	57,05%
MADUREZ	**2**

Tabla 2.32 Modelo de Madurez del proceso de administración de incidentes y *service desk*

En la **Tabla 2.32** se presenta el nivel de madurez definido para este proceso, el cual se obtiene en base a lo mencionado anteriormente y lo especificado en el modelo de la **Tabla 2.10**.

2.4 DETERMINACIÓN DE LOS PROCESOS DE OPERACIÓN EN EL ÁREA O&M DE MPLS DE LA CNT E.P.

Del análisis de los datos recopilados de la auditoría como objetivos del área, herramientas utilizadas, estructura interna, entrevistas y comprobación de documentación, se obtuvieron los procesos descritos en la sección 2.4.1 y 2.4.2.

2.4.1 PROCESOS EXISTENTES

Los procesos aplicados dentro del área son:

- Incidentes: se resuelven basándose en la experiencia de los miembros del área es decir no cuentan con un proceso normalizado.
- Gestión de seguridad de la información: dentro del área O&M IP MPLS se aplica bajo la norma ISO 27000.
- Problemas: se busca la causa raíz de los incidentes repetitivos y de aquellos que causan mayor grado de afectación sin aplicar un proceso normalizado.

2.4.2 PROCESOS NO EXISTENTES

Se determinó que para lograr mayor eficiencia en las operaciones por parte del área es necesario implementar los siguientes procesos:

- Proceso de monitoreo.
- Proceso de peticiones realizadas al área de O&M MPLS desde otras áreas.

2.4.3 PROCESOS A NORMALIZAR MEDIANTE ITIL

- Proceso de gestión de eventos
- Proceso de gestión de incidentes
- Proceso de gestión de problemas
- Proceso de gestión de consultas
- Proceso de gestión de accesos

COBIT indica **el qué** se debe realizar para alcanzar los objetivos de negocio cubriendo la capacidad de los activos de TI que muchas veces es la parte más valiosa de una organización, sin embargo ITIL indica a detalle **el cómo** cumplir con las metas trazadas orientándose en el servicio. Por lo descrito anteriormente en el capítulo 3 se normalizan los procesos existentes y se levantan los no inexistentes mediante ITIL.

CAPÍTULO 3

NORMALIZACIÓN Y DOCUMENTACIÓN DE PROCESOS BASADOS EN LA FASE DE OPERACIÓN DEL SERVICIO DEL CICLO DE VIDA DE ITIL

En este capítulo se normalizarán los procesos existentes y se levantarán los inexistentes definidos de la auditoría, adicionalmente se plantearán ejemplos con referencia al área O&M MPLS de la CNT E.P que faciliten su comprensión.

3.1 PROCESO DE GESTIÓN DE EVENTOS

3.1.1 OBJETIVO

Gestionar los eventos centrándose en divisar las notificaciones significativas del estado de la infraestructura y sus servicios para poder anticiparse a los incidentes y problemas, tomando la acción correcta para el control del evento.

3.1.2 ALCANCE

La gestión de eventos será aplicada por los operadores NOC quienes mantendrán el monitoreo de cada elemento de configuración y servicio de la red MPLS.

3.1.3 DEFINICIONES

3.1.3.1 Evento

Un evento puede ser definido como cualquier cambio de estado que tiene significancia para la gestión de un elemento de configuración (CI) o servicio de TI.

3.1.3.2 Alarma de información

Se genera cuando un evento no aporta información relevante que pueda ser usado en un análisis de datos. Por medio de estos eventos se conocerá el estado de los servicios. Sobre estos eventos no se debe tomar acciones.

3.1.3.3 Alarma de advertencia

Se genera si algo inusual ha ocurrido sobre la red o sus elementos, por lo que requiere de monitoreo y seguimiento.

3.1.3.4 Alarma de excepción

Esta alarma se presenta si el servicio está operando de manera irregular y ocasiona interrupción en el servicio.

3.1.4 RESPONSABLE

El área responsable del monitoreo de eventos será el NOC y el encargado de controlar la gestión de este proceso será el jefe del NOC, quien posteriormente presentará un informe consolidado al gerente del área de O&M de MPLS.

3.1.5 DESARROLLO DEL PROCESO DE GESTIÓN DE EVENTOS

3.1.5.1 Monitoreo de eventos

Los operadores NOC realizarán el monitoreo continuo de la red y sus servicios con las herramientas CACTI y CISCO PRIME.

Las herramientas de monitoreo censarán constantemente los elementos de configuración de la red IP MPLS mediante el protocolo SNMP. Una vez detectado el evento se almacena en el registro de logs, a partir de esto el resultado es interpretado y se activa una alarma.

Para el Cisco Prime se generarán las alarmas mostradas en la **Tabla 3.1**, además se incluye el tipo de evento relacionado a la alarma.

Ícono	Color	Significado de alarma
	Rojo	Critica
	Naranja	Mayor
	Amarillo	Menor

Ícono	Color	Significado de alarma
	Celeste	Advertencia
	Verde	Servicio estable

Tabla 3.1 Alarmas Cisco Prime

3.1.5.2 Definición de eventos

Una vez que se ha recibido la alarma, se la interpretará para definir el tipo de evento generado de acuerdo a lo indicado en la **Tabla 3.2**.

Ícono	Significado de alarma	Tipo de Evento
	Critica	Excepción
	Mayor	Excepción
	Menor	Advertencia
	Advertencia	Informativa
	Servicio estable	Informativa

Tabla 3.2 Significancia del evento correspondiente a las alarmas de Cisco Prime

Cuando se genera una excepción se seguirán los pasos del proceso de gestión de Incidentes.

En el caso del CACTI, si se visualiza disminución o caída de tráfico es necesario realizar pruebas de primer nivel para verificar si se trata de una excepción. Cuando se genera una advertencia se revisará el evento para determinar si es necesario tomar acción.

Si la alarma es repetitiva y no causa interrupción del servicio se requiere la intervención por parte del operador NOC, en caso de que la acción aplicada sea efectiva, se cerrará el evento, delo contrario se escalará al proceso de gestión de consultas para posteriormente ser analizado por el área de O&M IP/MPLS para brindar la solución correspondiente.

Si se presenta una alarma informativa, no se tomará acción debido a que este tipo de alerta solo indicará cambios esperados como restablecimiento o estabilidad del servicio.

En la **Tabla 3.3** se especifican las acciones a tomar de acuerdo al significado de cada alarma generada en la herramienta Cisco Prime.

Ícono	Significado de alarma	Acción a Tomar
	Critica	Escalar a Gestión de Incidentes
	Mayor	Escalar a Gestión de Incidentes
	Menor	Revisión y seguimiento
	Advertencia	Revisión
	Servicio estable	Sin acción

Tabla 3.3 Correlación de alarmas Cisco Prime

Cada operador presentará al jefe del NOC un informe semanal sobre los eventos atendidos acorde al **Anexo A.1**.

3.1.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE EVENTOS

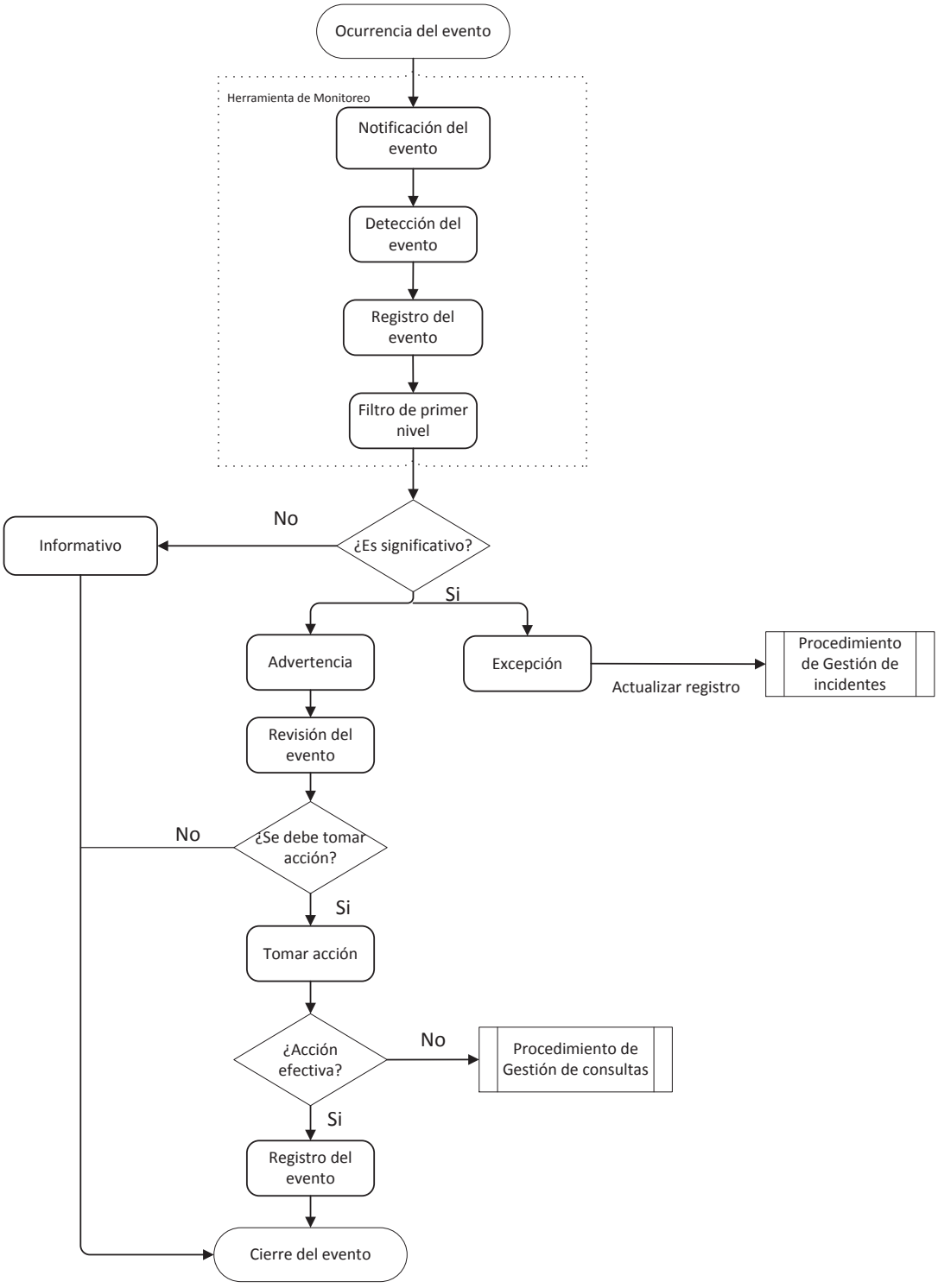


Figura 3.1 Diagrama del Proceso de Gestión de eventos

3.2 PROCESO DE GESTIÓN DE INCIDENTES

3.2.1 OBJETIVO

Gestionar eficientemente las incidencias para recuperar la operación normal del servicio lo más rápido posible, asegurando los niveles acordados de calidad del servicio con el cliente y minimizar el impacto en las operaciones de negocio.

3.2.2 ALCANCE

Este proceso será aplicado por las áreas NOC y O&M de la plataforma IP/MPLS de la Corporación Nacional de Telecomunicaciones CNT E.P.

3.2.3 DEFINICIONES

3.2.3.1 Incidente

Es un evento que no forma parte del comportamiento habitual del servicio causando una su interrupción imprevista o reducción de su calidad

3.2.3.2 Escalamiento

Es una actividad que obtiene recursos adicionales cuando son necesarios para cumplir con los acuerdos del nivel de servicio o con las expectativas del cliente.

3.2.3.3 Impacto

Determina la importancia de la incidencia dependiendo de cómo ésta afecta a los procesos del servicio y el número de usuarios afectados. A continuación se define la clasificación del impacto en la red IP/MPLS.

- **Alto.-** interrupciones que provocan que todos o gran parte de los servicios soportados por la plataforma IP/MPLS presentan indisponibilidad del servicio y gran afectación a los usuarios.

- **Medio.-** perturbaciones que afecten la funcionalidad a media escala de los servicios soportados por la plataforma IP/MPLS.

- **Bajo.-** incidentes menores que presentan una leve afectación del servicio brindado por la plataforma IP/MPLS.

3.2.3.4 Prioridad

Se usa para identificar la importancia con la que será tratado un incidente y será establecida en base a la urgencia e impacto sobre los servicios afectados.

3.2.3.5 Urgencia

Es la medida de cuánto tiempo pasará hasta solventar un incidente.

3.2.3.6 Pruebas de primer nivel

Consisten de un conjunto de comandos aplicados para determinar la falla y la posible solución del incidente.

3.2.3.7 Pruebas de segundo nivel

Consiste en comandos más específicos y avanzados para la búsqueda de la solución de incidentes.

3.2.4 RESPONSABLE

El área responsable de detección, resolución y cierre de incidentes será el centro de operación de red (NOC).

El área encargada de resolver las incidencias escaladas por el NOC será O&M de la plataforma IP/MPLS.

3.2.5 DESARROLLO DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTES NOC

3.2.5.1 Procedimiento de registro y clasificación de incidentes

3.2.5.1.1 *Identificación de incidente*

Los operadores NOC receptarán las notificaciones mediante web interface, correos electrónicos y llamadas telefónicas que informen sobre un posible

incidente. Se procederá con el análisis para identificar si se trata de un incidente, si no lo es, se escalará al personal del área de MPLS quienes seguirán el proceso de ejecución de consultas.

En el caso de que se trate de un incidente se procederá a registrarlo mediante un ticket en la herramienta gestora de tickets (Remedy).

3.2.5.1.2 *Registro del incidente*

Se debe realizar el registro en el archivo maestro de incidentes el mismo que incluirá la siguiente información:

- Número único de referencia.
- Fecha y hora en que ocurrió el incidente.
- Categorización.
- Priorización.
- Nombre del operador responsable.
- Descripción.
- Estado.
- Grupo al que ha sido asignado.

3.2.5.1.3 *Categorización del incidente*

Para categorizar se debe verificar los elementos de red y servicios afectados, estos se describen en la **Tabla 3.4**

Elementos de Red	Servicio afectado
CORE	Redundancias de todos los servicios
EDGE	Servicios masivos y corporativos, interconexión con plataformas troncales
AGREGACIÓN	Servicios masivos y corporativos
ACCESO	DSLAM y equipos terminales

Tabla 3.4 Criterios de categorización del incidente

3.2.5.1.4 *Priorización de un incidente*

Para priorizar se deben tomar en cuenta los siguientes criterios de afectación:

PRIORIDAD = IMPACTO + URGENCIA

Para determinar el impacto de un incidente se deben tomar en cuenta los siguientes criterios.

- Número de clientes afectados.
- Número de servicios afectados.
- Efectos sobre la calidad del servicio de la organización.

La urgencia será determinada acorde a la velocidad establecida para resolver un incidente con un impacto dado.

En la **Tabla 3.5** se presenta la matriz a utilizarse para establecer la prioridad del incidente basándose en la urgencia y el impacto sobre el mismo:

		IMPACTO		
URGENCIA	Prioridad	Alto	Medio	Bajo
	Alto	1	2	3
	Medio	2	3	4
	Bajo	3	4	5

Tabla 3.5 Matriz Urgencia Impacto [10]

En la **Tabla 3.6** se presentan los tiempos de resolución del incidente una vez establecida su priorización en base a una reunión con el gerente del área O&M con quien se determina estos tiempos, basados en las sugerencias de ITIL y en los recursos con que cuenta el área para brindar soluciones.

Código de prioridad	Descripción	Tiempo de Resolución (horas)
1	Crítico	3
2	Alto	5
3	Medio	9
4	Bajo	16
5	Planeado	Planeado

Tabla 3.6 Tiempo de solución en base a la prioridad

En caso de tratarse de un incidente crítico se notificará de inmediato al líder de zona, líder técnico y jefe de MPLS quienes se guiarán en los pasos definidos en el procedimiento de incidente crítico y en caso de no ser así se continuará con la búsqueda de la solución del incidente.

3.2.5.2 Procedimiento del análisis y resolución de incidentes NOC

3.2.5.2.1 *Pruebas de primer nivel*

El operador del NOC debe realizar las pruebas de primer nivel para obtener un diagnóstico inicial y dar solución al incidente. Los comandos permitidos que se aplicarán por parte de los operadores NOC para cumplir con las pruebas de primer nivel se describen en el **Anexo A.2**.

3.2.5.2.2 *Acciones correctivas*

Una vez que se ha encontrado la solución se verifica si se tienen los permisos para tomar acción, en caso de no ser así se escalará el ticket por medio del Remedy, además se notificará por medio de correo electrónico al ingeniero de turno del MPLS y se enviarán todas las pruebas realizadas.

En caso de contar con los permisos correspondientes se tomarán las acciones correctivas y se verificará si se solucionó el incidente. Si no se ha dado solución se escalará el ticket al siguiente nivel (ingeniero de turno MPLS). Si se ha solventado se realizará el procedimiento de cierre de incidentes. En todo el proceso de resolución de incidentes el operador de NOC a cargo deberá dar seguimiento hasta el cierre de la incidencia.

3.2.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE INCIDENTES NOC

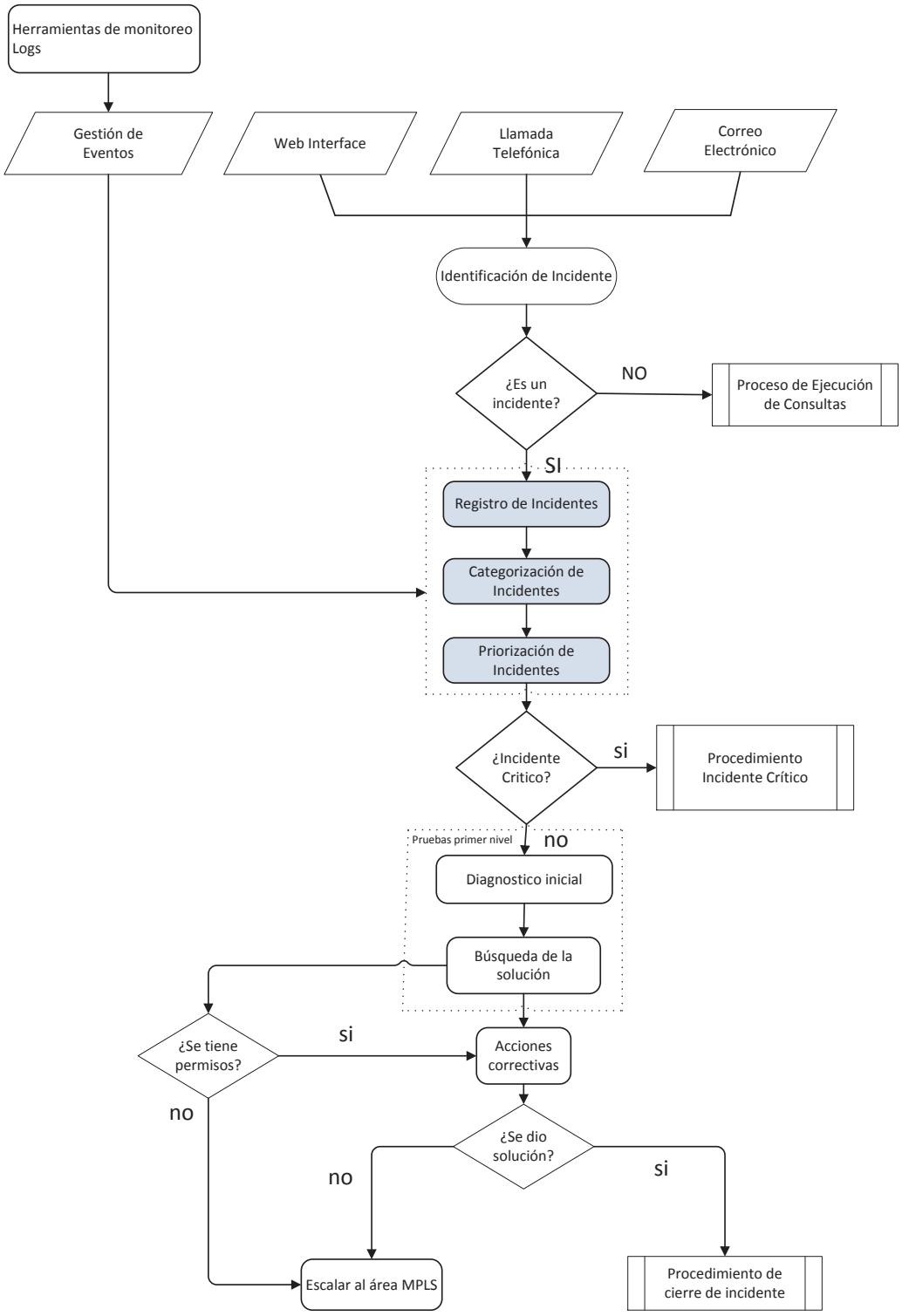


Figura 3.2 Procedimiento de Gestión de Incidentes NOC

3.2.7 DESARROLLO DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTES MPLS

3.2.7.1 Recepción del ticket

Una vez que el ingeniero de turno del MPLS ha recibido el ticket escalado desde el NOC, debe proceder con la revisión de las pruebas de primer nivel efectuadas previamente y de los resultados obtenidos.

Se realizarán pruebas de segundo y tercer nivel en búsqueda de la solución y se tomarán las acciones respectivas para restablecer el servicio.

En caso de requerir cambios para solucionar el incidente, se aplicará el procedimiento de gestión de cambios emergente.

Si se ha solucionado, se notificará al NOC quien seguirá el procedimiento de cierre de incidentes.

Se realizará un informe, mismo que contendrá la información más importante de resolución del incidente, acciones tomadas y tiempo de afectación.

En caso de no solventar el incidente con las acciones correctivas tomadas, es necesario consultar a otros grupos de apoyo del área MPLS y de no encontrar solución se solicitará apoyo del proveedor.

En caso de requerir intervención por parte del proveedor, la persona a cargo debe solicitar el informe correspondiente al incidente, este deberá contener la causa, la solución y el tiempo de afectación para con esta información notificar al NOC para la actualización del registro.

3.2.8 DIAGRAMA DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTES MPLS

En la **Figura 3.3** se presenta el diagrama sugerido para el procedimiento de resolución de incidentes para el área MPLS.

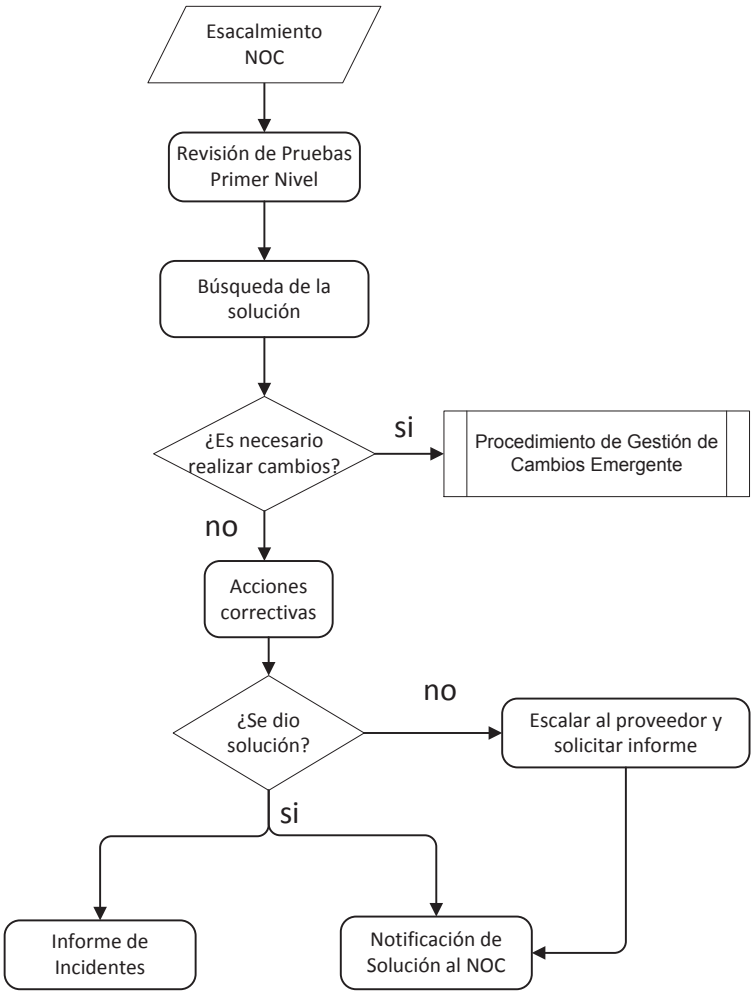


Figura 3.3 Procedimiento de resolución de incidentes MPLS

3.2.9 DESARROLLO DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTE CRÍTICO

Una vez que se ha recibido el ticket escalado desde el NOC se realiza la revisión de la descripción, y se aplican pruebas de segundo y tercer nivel para continuar en la búsqueda de la solución, si se necesitan cambios para solucionar el incidente, se seguirán los pasos del procedimiento de gestión de cambio emergente.

En caso de no ser necesarios los cambios, se tomarán las acciones respectivas para restablecer el servicio. Si se ha solucionado, se notificará al NOC quien seguirá el procedimiento de cierre de incidentes, cabe indicar que en el caso de

que se brinde una solución temporal se planificará un mantenimiento preventivo que se aplicará mediante el procedimiento de gestión de cambios normal.

También se realizará un informe, mismo que contendrá toda la información del incidente, acciones tomadas y tiempo de afectación. Una vez solventado y cerrado el incidente, se seguirán los pasos del proceso de gestión de problemas para identificar la causa raíz del mismo, esto se realizará para prevenir futuras reincidencias.

Si no se restablece el servicio, se continuará con la búsqueda de la solución con apoyo de los demás grupos del mismo nivel y de ser necesario con especialistas de niveles superiores o el proveedor.

3.2.10 DIAGRAMA DEL PROCEDIMIENTO DE RESOLUCIÓN DE INCIDENTE CRÍTICO

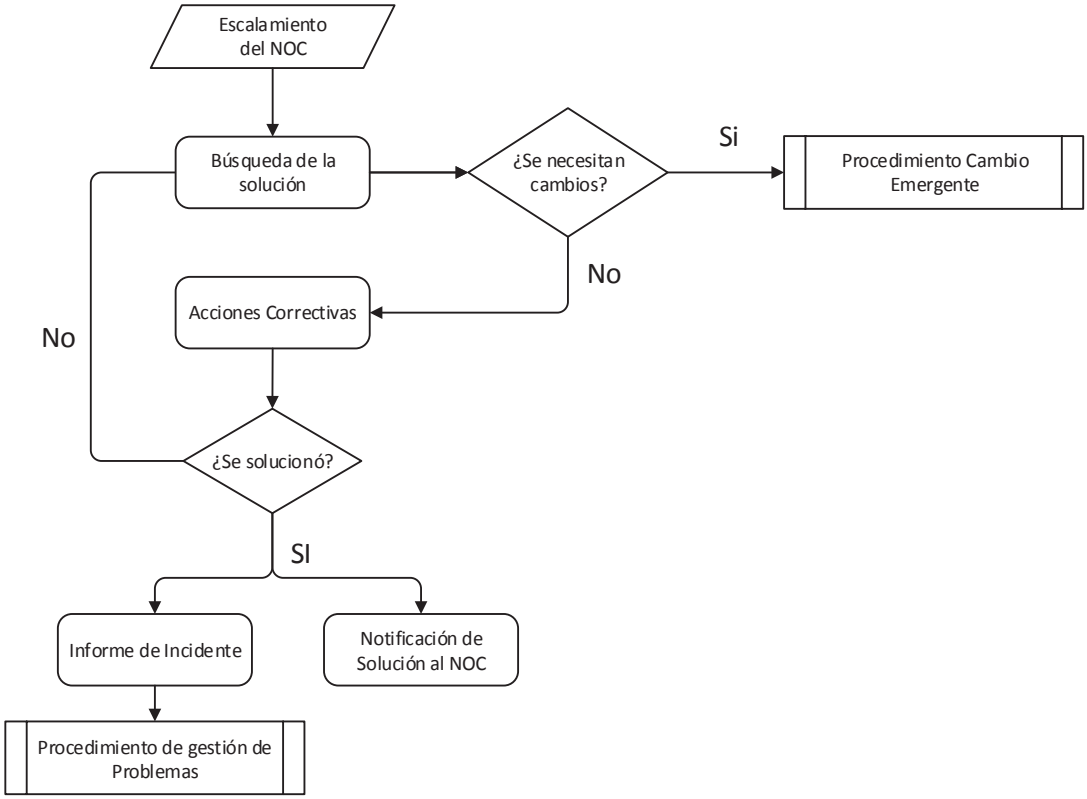


Figura 3.4 Procedimiento de Resolución de Incidente Crítico

3.2.11 DESARROLLO DEL PROCEDIMIENTO DE CIERRE DE INCIDENTES

3.2.11.1 Notificación de la solución

Una vez resuelto el incidente, se deben realizar pruebas de estabilidad del servicio, esto con el fin de verificar que el servicio se encuentra estable y operativo. En caso de no tener resultados positivos se debe escalar el ticket a O&M para que se encarguen de realizar una revisión más profunda.

Si se ha validado el servicio estable se realizará la revisión del registro de incidentes y se lo actualizará incluyendo las acciones correctivas tomadas con el tiempo de afectación, en caso de ser reincidente, será escalado para ser tratado mediante el proceso de gestión de problemas.

Finalmente, se procede con el cierre del ticket en la herramienta gestora de tickets. En caso de que el área de O&M haya resuelto el incidente debe notificar al NOC para que cumpla con el procedimiento de cierre de incidentes.

3.2.12 DIAGRAMA DEL PROCEDIMIENTO DE CIERRE DE INCIDENTES

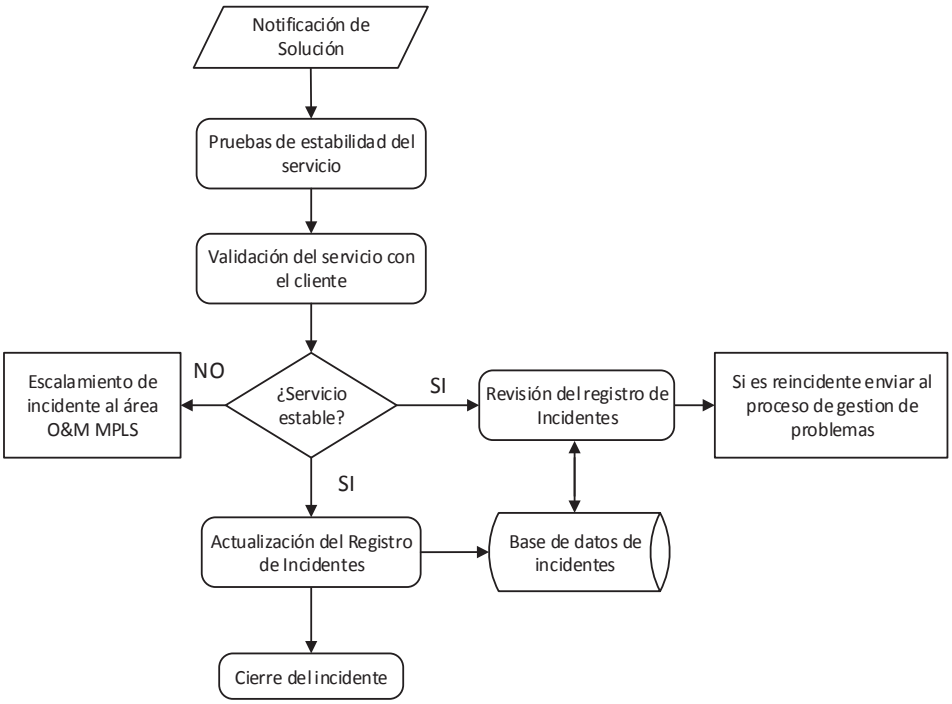


Figura 3.5 Procedimiento de Cierre de Incidentes

3.3 PROCESO DE GESTIÓN DE PROBLEMAS

3.3.1 OBJETIVO

Gestionar eficientemente los problemas para encontrar su causa raíz y evitar la recurrencia de incidentes que interrumpan la operación normal del servicio que ocasionen indisponibilidad e incumplimiento de los niveles de servicio acordados con el cliente.

3.3.2 ALCANCE

Este proceso se utilizará para brindar una solución definitiva a los incidentes repetitivos y críticos, y se aplicará dentro del área de operación y mantenimiento de la plataforma IP/MPLS de la Corporación Nacional de Telecomunicaciones CNT E.P.

3.3.3 DEFINICIONES

3.3.3.1 Problema

Causa aún no identificada, de una serie de incidentes o un incidente de importancia significativa.

3.3.3.2 Error conocido

Un problema se convierte en error conocido una vez que su causa ha sido determinada y documentada.

3.3.3.3 Base de datos de error conocido

Es una base de datos en la cual se documentan las soluciones a largo plazo aplicadas para solventar incidentes.

3.3.4 RESPONSABLE

El área responsable de la gestión de problemas será O&M plataformas MPLS, que se encargará de la verificación de las soluciones para evitar que se produzcan interrupciones del servicio nuevamente.

3.3.5 DESARROLLO DEL PROCESO DE GESTIÓN DE PROBLEMAS

3.3.5.1 Registro de problemas

Se identificarán los problemas con los resultados del análisis de los registros de incidentes recurrentes y emergentes, ya sean aquellos resueltos o reportados por el NOC y solventados por el área de O&M MPLS.

Cuando se ha detectado la existencia de un problema, se lo debe registrar dentro de la base de datos de error conocido con los siguientes datos:

- Número único de identificación.
- Fecha y hora de apertura del caso.
- Priorización (Incluye la urgencia e impacto).
- Descripción del problema.
- Número de recurrencia.
- Detalle de los diagnósticos y acciones correctivas.
- Detalle de servicios afectados.
- Detalle de equipos afectados.
- Solución definitiva.

3.3.5.2 Investigación y diagnóstico de problemas

Para diagnosticar el problema será necesario acudir a la base de datos de error conocido con el objetivo de obtener toda la información necesaria de incidentes relacionados con el problema en investigación para tener una guía de apoyo a la resolución.

En caso de no encontrar la solución se realizará una investigación más profunda y todas las pruebas necesarias que permitan plantear una medida definitiva con la colaboración de los recursos y el conocimiento del personal respectivo.

La prioridad asignada a problemas será la misma proveniente desde el proceso de incidentes, y los umbrales de tiempo de solución serán definidos por el responsable de la gestión de problemas.

3.3.5.3 Acciones correctivas

Con las revisiones realizadas, se determinarán las acciones a tomar y en el caso de requerir cambios, se seguirán los pasos detallados en el proceso de gestión de cambios normal.

El concejo de gestión de cambios analizará los RFC receptados, y resolverá la aprobación de las soluciones planteadas para solventar los problemas.

Antes de proceder con los cambios para solventar el problema, se informará como mantenimiento preventivo a todas las áreas relacionadas con el MPLS como son NOC, gestión de la red[32], gestión XDSL[33] y multiservicios[34] para que realicen las revisiones necesarias y gestiones correspondientes a sus funciones.

3.3.5.4 Solución del problema

Una vez autorizadas y aplicadas las acciones correctivas de acuerdo a lo planificado, posteriormente, se realizarán las pruebas sobre los casos más críticos asociados al incidente que generó el problema y se registrarán los resultados para próximas revisiones.

Si el problema no fue solventado, se realizará un nuevo análisis que contemple los posibles factores que se pasaron por alto para encontrar la causa del problema y plantearse nuevas soluciones.

Finalmente se actualizarán los registros del caso en la base de datos de error conocido incluyendo las pruebas realizadas y acciones correctivas que permitieron encontrar la solución para posteriormente cerrar el proceso.

3.3.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE PROBLEMAS

En la **Figura 3.6** se presenta el diagrama para la resolución de problemas.

---

[32] Gestión de Red: se encarga del monitoreo del estado de la red para obtener estadísticas de servicios y calcular su disponibilidad

[33] Gestión XDSL: realiza el direccionamiento IP de los clientes corporativos.

[34] Multiservicios: verifican la disponibilidad de la red para el aprovisionamiento de nuevos servicios.

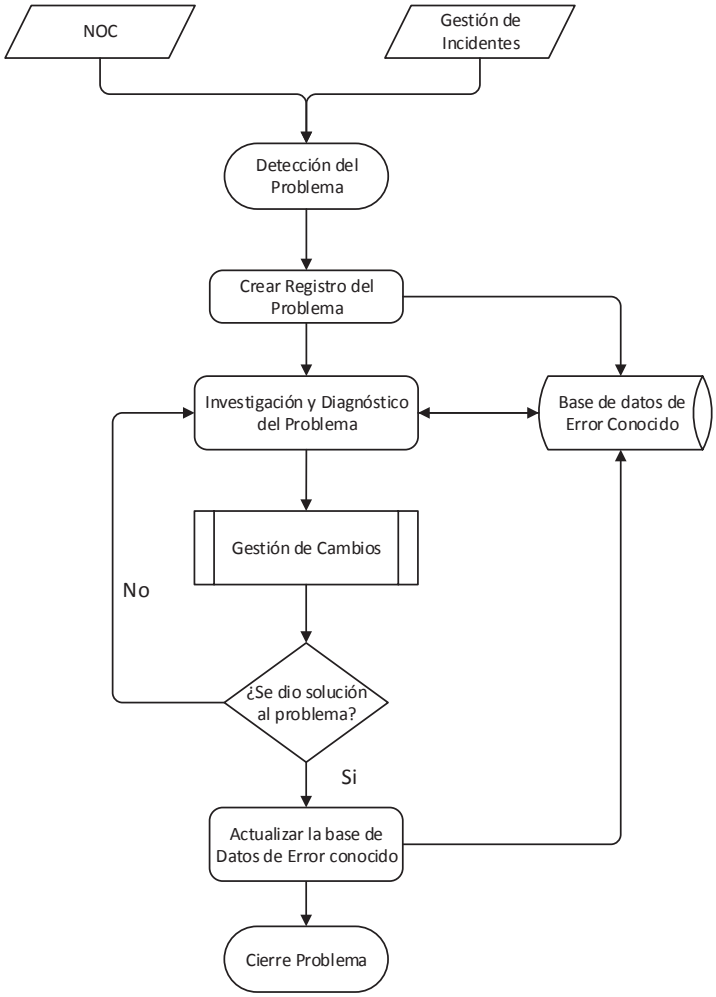


Figura 3.6 Diagrama de flujo del proceso de Gestión de Problemas

3.4 PROCESO DE GESTIÓN DE CONSULTAS

3.4.1 OBJETIVO

Mantener la satisfacción del usuario mediante una atención eficiente de sus solicitudes.

3.4.2 ALCANCE

Este proceso será aplicado para cumplir con las solicitudes provenientes de las áreas afines al O&M IP/MPLS como son: NOC, ingeniería[35], gestión de la red, gestión XDSL y multiservicios.

[35] Ingeniería: se encargan de la coordinación para la instalación de nuevos servicios.

3.4.3 RESPONSABLE

El área responsable de atender las consultas del NOC y áreas relacionadas será el área de O&M MPLS.

3.4.4 DESARROLLO DEL PROCESO DE GESTIÓN DE CONSULTAS

3.4.4.1 Recepción de la consulta

Inicialmente el área de O&M plataformas MPLS recepta la consulta desde el NOC o áreas relacionadas mediante correo electrónico, llamada telefónica y RFC, después de su recepción se procede con la verificación correspondiente.

3.4.4.2 Registro y Validación de la consulta

Una vez receptada la consulta, se validará y registrará con toda la información pertinente para que en caso de direccionarse a otro grupo, tenga la información completa para cumplir con la solicitud. La información necesaria para el registro de una solicitud de servicio incluirá:

- Número de referencia único.
- Categorización.
- Priorización.
- Fecha y hora.
- Nombre de la persona o grupo que realiza la solicitud.
- Método de notificación (teléfono o correo electrónico).
- Descripción de la solicitud.
- Nombre de la persona que atiende la consulta.
- Fecha y hora de cumplimiento de la solicitud.
- Fecha y la hora de cierre.

3.4.4.3 Categorización de la consulta

- Por servicio.
- Por actividad.
- Por elemento de configuración.

3.4.4.4 Priorización de la consulta

Se asignará la priorización adecuada, que determinará el tiempo en que la solicitud de servicio será atendida.

- **Alta:** Se resolverá en 4 horas.
- **Media:** Se resolverá de 6 a 8 horas.
- **Baja:** Se resolverá bajo planificación.

3.4.4.5 Autorización de la consulta

Previo al cumplimiento de una consulta, es necesario recibir la autorización del gerente del área. En caso de que una solicitud no sea autorizada será devuelta a quien la solicitó, se actualizará el registro de consultas, el cual contendrá el motivo del rechazo.

3.4.4.6 Revisión de consulta

En esta etapa, la solicitud será revisada para determinar las acciones a tomar para cumplir con la consulta. Los registros de la consulta deben actualizarse para reflejar el estado actual de la misma, si es verificación de servicios o agregaciones sin complejidad se lo realizarán quedando en el registro de consultas, en el caso de que requiera cambios se debe seguir la guía del procedimiento de gestión de cambios estándar.

3.4.4.7 Ejecución de la consulta

Una vez se ha realizado el análisis previo, se tomaran las acciones para cumplir con la solicitud realizada por el área del NOC hacia el área O&M plataformas MPLS.

3.4.4.8 Cierre de la consulta

Una vez completas las actividades de solicitud de servicio, se debe comprobar con el área solicitante que se haya cumplido con los requerimientos de la consulta.

3.4.5 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE CONSULTAS

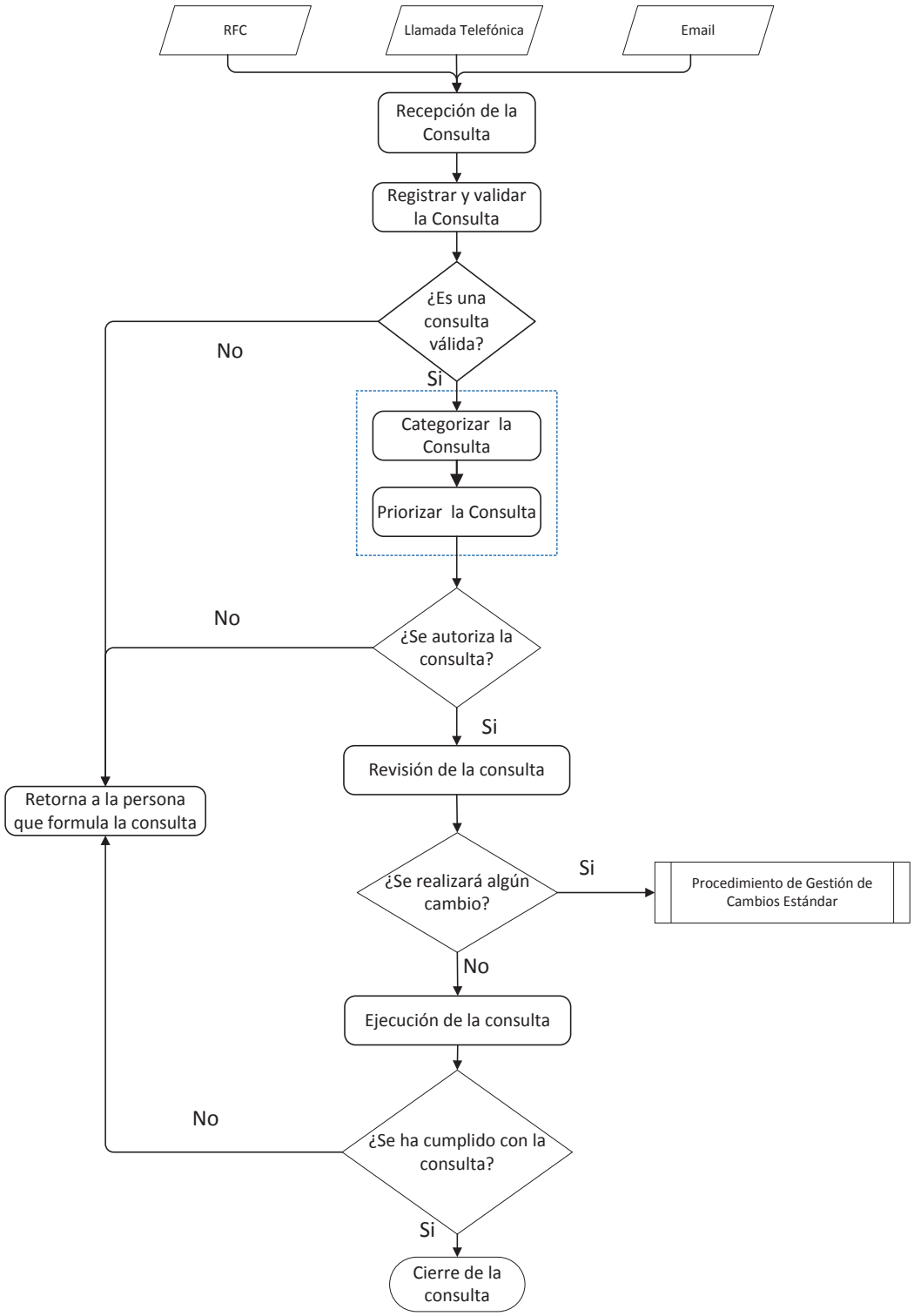


Figura 3.7 Proceso de Gestión de Consultas

3.5 PROCESO DE GESTIÓN DE ACCESOS

3.5.1 OBJETIVO

Establecer los lineamientos para un adecuado uso de la información y concesión de permisos de acceso a los equipos y servicios que sustenta el área de MPLS, con el fin de asegurar la integridad, confidencialidad disponibilidad de la operación del servicio.

3.5.2 ALCANCE

Este proceso será aplicado por todo el personal que tiene acceso a los equipos y los servicios del área de O&M de la red IP/MPLS.

3.5.3 RESPONSABLE

El área responsable de implementar, actualizar y vigilar el cumplimiento de este procedimiento será el jefe de área del O&M Plataformas MPLS.

3.5.4 DEFINICIONES

3.5.4.1 Confidencialidad

Característica de la información que establece que ésta se revela únicamente, si así está estipulada, a personas, procesos o entidades autorizadas y en el momento autorizado.

3.5.4.2 Disponibilidad

Característica de la información o servicios que establece que pueden ser accedidos por las personas o sistemas autorizados en el momento y en el medio que se requiera.

3.5.4.3 Integridad

Característica de la información que establece que ésta debe ser precisa, coherente y completa desde su creación hasta su destrucción. Para conseguir esto, es necesario evitar modificaciones no autorizadas.

3.5.5 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE ACCESOS

3.5.5.1 Recepción de la solicitud de acceso

La solicitud será realizada por el jefe inmediato de acceso y será receptada por la jefatura del área de O&M plataformas de MPLS, y se debe realizar en el caso de que una persona sea contratada, promovida o termine su contrato en la empresa. La solicitud debe incluir los siguientes datos:

- Nombre del jefe inmediato (número de teléfono y correo electrónico).
- Área /proveedor.
- Motivo de ingreso o modificación de permisos de acceso.
- Datos de la persona a la que se le creará o modificará los accesos.

En caso de modificación de permisos el solicitante debe incluir el nombre de usuario actual en la solicitud. En el **Anexo A.3** se describe el formato de la solicitud de acceso.

3.5.5.2 Verificación de la solicitud de acceso

Se verificará que la solicitud recibida sea válida tomando en cuenta los datos enviados, de ser inconsistente la información, se descarta y se regresa al solicitante indicando las causas del rechazo.

3.5.5.3 Autorización de la solicitud de acceso

Una vez que se ha validado que la solicitud y el usuario a crear son legítimos, se solicita la autorización a Gerencia, para proceder con el requerimiento, si no es autorizada será descartada y se informará las causas del rechazo de la solicitud.

3.5.5.4 Ejecución de acceso

Tan pronto sea autorizada la solicitud se proporcionará los derechos de acceso solicitado tomando en cuenta las políticas estipuladas internamente para usuarios, perfiles y contraseñas. Adicionalmente, se asignará una clave temporal misma que se deberá cambiar en el primer acceso a los equipos.

3.5.5.5 Notificación de acceso

Una vez cumplida la solicitud de acceso, se notificará al solicitante para su validación, en caso de que se haya creado un nuevo usuario, se indicará el usuario, clave temporal y políticas de contraseña para el cambio de la misma.

3.5.6 DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE ACCESO

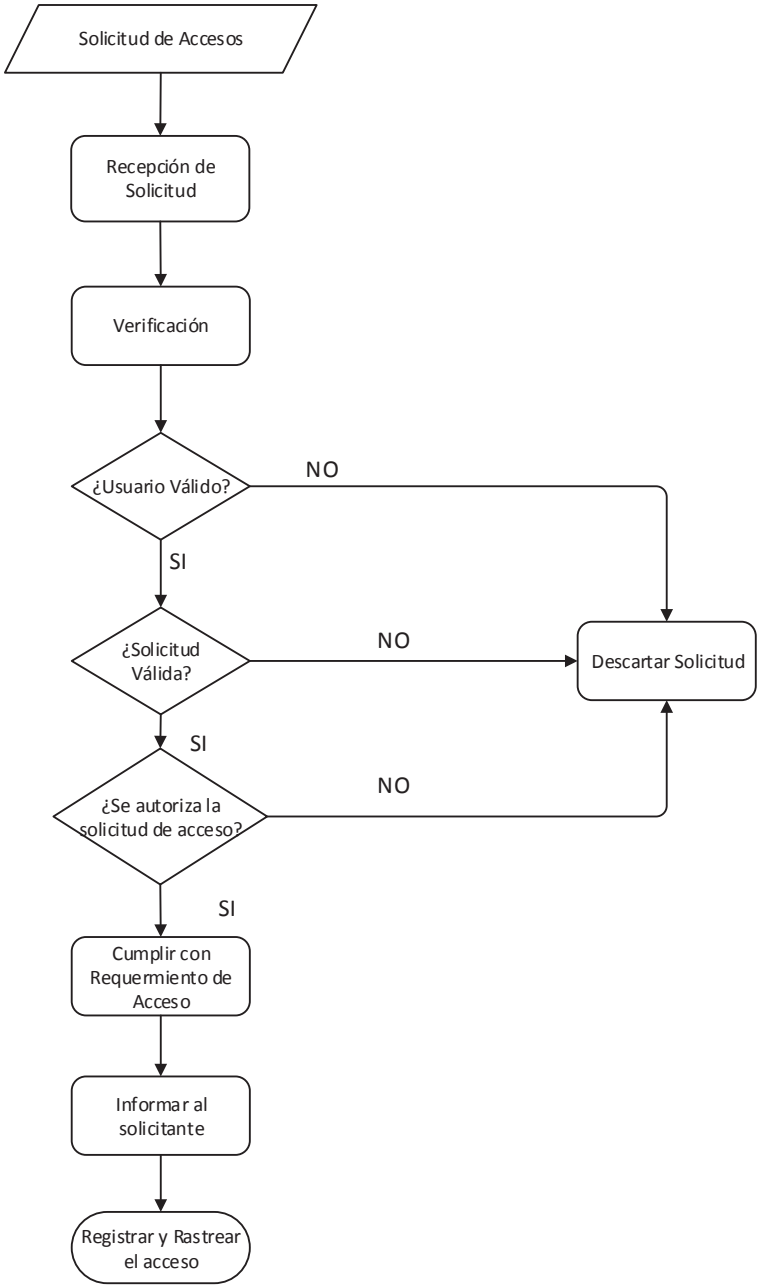


Figura 3.8 Proceso de gestión de acceso

3.6 PROCESO DE GESTIÓN DE CAMBIOS

3.6.1 OBJETIVO

Gestionar eficientemente la implementación de cambios preventivos y correctivos en la red IP/MPLS para reducir el número de incidentes y problemas asociados con éstos.

3.6.2 ALCANCE

Este proceso será aplicado a todos los elementos de configuración, servicios, tecnologías, accesos y procesos del área O&M de las plataformas IPMPLS de la Corporación Nacional de Telecomunicaciones CNT E.P para garantizar continuidad de los servicios[36] brindados.

3.6.3 DEFINICIONES

3.6.3.1 Cambio

Es la adición, modificación o remoción de algo que puede causar un efecto en los servicios TI.

3.6.3.2 Cambio normal

Se genera por una petición de un individuo o grupo que necesita el cambio para corregir o mejorar el rendimiento del servicio.

3.6.3.3 Cambio standard

Es un cambio en un servicio o infraestructura que está pre autorizado por la gestión del cambio y que tiene un procedimiento aceptado y establecido para atender a una necesidad de cambio concreta.

3.6.3.4 Cambio emergente

Tiene como fin reparar un error que afecta en forma negativa y en gran medida el servicio de TI.

[36] Continuidad de los servicios: el servicio se mantiene operativo sin suspensiones o degradaciones que afecten su funcionamiento norma.

3.6.3.5 RFC (Request For change)

Es una propuesta formal que incluye detalles de los cambios que serán realizados.

3.6.3.6 Registro de cambios

Es un documento en el cual se registrará toda la información correspondiente a los cambios realizados o que se encuentran pendientes de realización.

3.6.3.7 Propuesta de cambio

Es una comunicación formal para realizar una alteración a uno o más elementos de configuración.

3.6.3.8 Plan de recuperación (*rollback*)

Es el retorno de una operación que devuelve a los sistemas a su estado previo.

3.6.4 RESPONSABLE

El área responsable de llevar a cabo el proceso de gestión de cambios será el área de O&M IP MPLS.

3.6.5 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS NORMAL

3.6.5.1 Recepción de propuestas del cambio

El área de IP MPLS receptará las propuestas de cambios mediante solicitudes conocidas como OT[37] provenientes de los procesos de gestión de incidentes, problemas y solicitudes de servicio. Esta solicitud debe contener los siguientes datos:

- Número de OT.
- Solicitante.
- Fecha de solicitud.

[37] OT (Orden de Trabajo): propuesta de solicitud de cambio previo a la creación del RFC

- Descripción del trabajo a realizar.
- Prioridad.
- Lugar donde se realizará el trabajo.

3.6.5.2 Creación de RFC

Una vez receptada la OT se formalizará con la creación de un RFC que debe incluir los siguientes datos:

- Número de OT.
- Alcance.
- Antecedentes.
- Hora y fecha de ejecución.
- Tiempo de indisponibilidad del servicio.
- Resumen de acciones para realizar el cambio que incluirá la duración de cada actividad y responsables con las funciones a cumplir.
- Equipos involucrados.
- Impacto (servicios afectados).
- Recursos para cumplir con el cambio.
- Matriz de pruebas y validaciones.
- Riesgos y plan de contingencia.

El Anexo **A.4**, describe el formato del RFC.

3.6.5.3 Aprobación del RFC

El comité de cambios será integrado por el gerente del área de O&M, un miembro del área de ingeniería, el jefe del NOC y el responsable del proceso de gestión de cambios.

El comité de cambios del MPLS se encargará de la revisión y análisis del RFC, si cuenta con los parámetros para cumplir el proceso pasará a la siguiente etapa, caso contrario, se devuelve al solicitante indicando el motivo del rechazo del documento para que se encargue del replanteamiento del RFC.

3.6.5.4 Asignación de recursos

La gestión técnica del área de O&M MPLS se encargará de asignar los recursos necesarios para la implementación del cambio ya sean estos personas, materiales o equipos.

3.6.5.5 Implementación del cambio

Una vez autorizado el cambio, se notificará al NOC para que tomando en cuenta los parámetros establecidos dentro del RFC se responsabilice del monitoreo y seguimiento durante el cambio, adicionalmente realice las actividades asignadas.

Adicionalmente, se indicará a las áreas relacionadas a O&M MPLS para que realicen la gestión correspondiente de acuerdo a sus funciones, y de ser necesario, brinden apoyo en el momento de realizar el cambio.

El cambio será implementado en la fecha y hora especificadas en el RFC siguiendo todas las actividades de acuerdo a este documento.

Si el cambio es exitoso, se deben realizar las pruebas de validación especificadas en el RFC para verificar el correcto funcionamiento de los servicios, si no se tienen resultados favorables, se procede a realizar el rollback mediante el cual se retorna a la configuración inicial; se notificará a las áreas involucradas que el cambio no se implementó exitosamente.

Si los resultados de la evaluación son correctos, se notifica para la actualización de las herramientas de monitoreo y se cierra el cambio. Adicionalmente, es necesario incluir dentro del registro el tiempo real de afectación e indicar si se presentó algún contratiempo y la solución.

Para re plantear la implementación de un cambio fallido se requiere solicitar autorización mediante una nueva RFC en donde se corrijan los errores por los cuales no se aprobó y se incluyan las recomendaciones realizadas por el comité de cambios.

3.6.6 DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS NORMAL

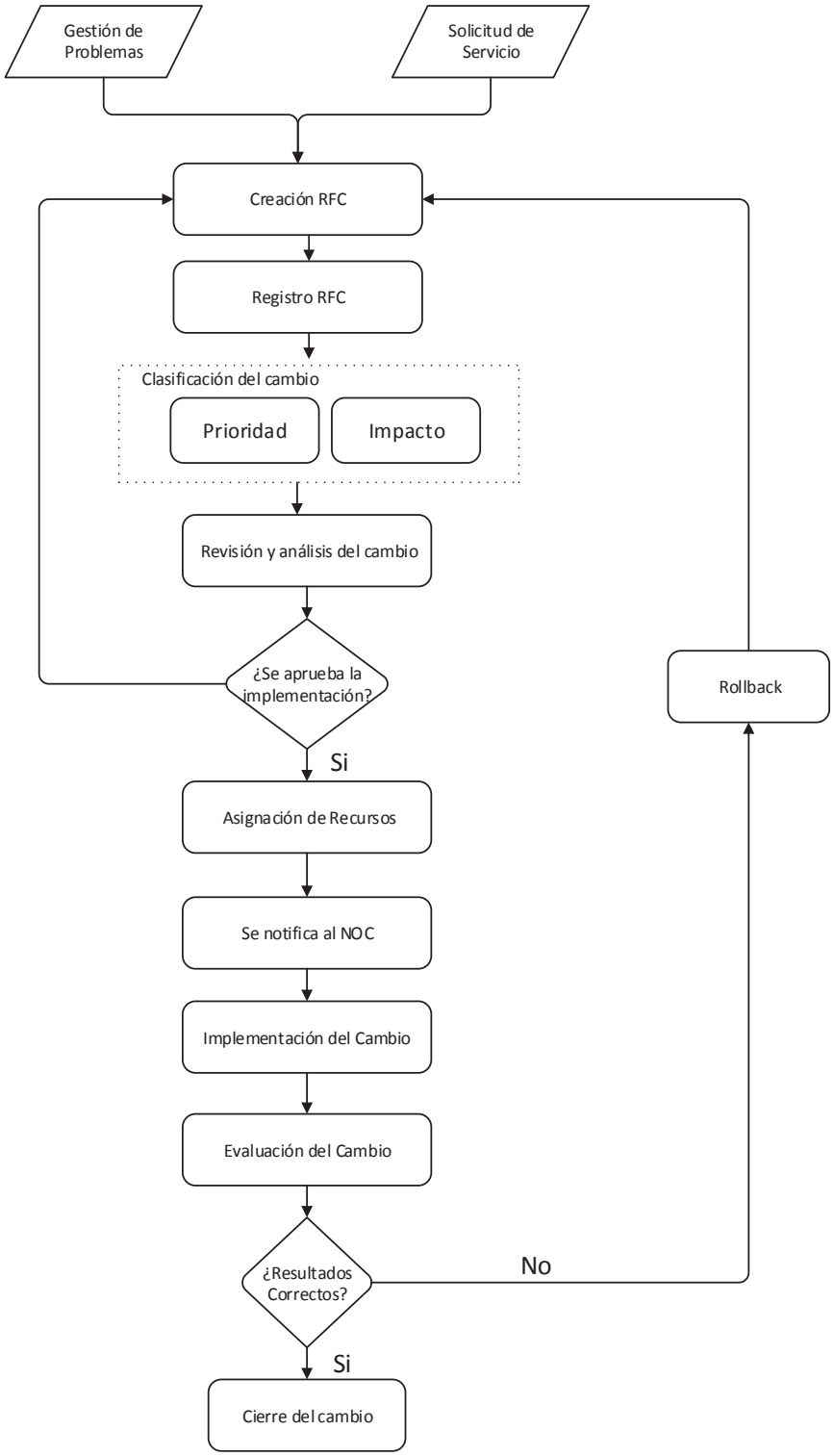


Figura 3.9 Procedimiento de gestión de cambios normal

3.6.7 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EMERGENTE

3.6.7.1 Planificación y asignación de recursos

Se planifica la ejecución del cambio incluyendo las actividades a realizar y se asignan los recursos necesarios para su implementación. Se solicitará a la gestión técnica de O&M MPLS facilite los equipos y herramientas necesarios

3.6.7.2 Autorización del cambio

Se solicitará autorización al responsable del proceso de gestión de cambios para proceder con la ejecución de las acciones planificadas en la etapa anterior.

3.6.7.3 Implementación del cambio

Se implementará el cambio de acuerdo a lo planificado, y al finalizar es necesario realizar un conjunto de pruebas para verificar que se ha restablecido el servicio afectado.

Si la implementación es exitosa y se solventa el incidente, se notifican los cambios realizados al NOC para la validación del servicio con el cliente fina y actualización de sus herramientas de monitoreo, también será necesario informar a las áreas relacionadas.

Si el cambio no es exitoso, será necesario revisar nuevamente para encontrar los errores cometidos y se procede nuevamente hasta que el servicio se restablezca completamente.

Para mantener el registro del cambio o cambios realizados, se elaborará el RFC para ser entregado al responsable de este proceso y se procederá con el cierre del cambio.

Adicionalmente, es necesario, en caso de que se presente algún inconveniente mientras se realiza el cambio, se especifique el error obtenido, la causa de que se haya presentado y las acciones correctivas.

3.6.8 DIAGRAMA DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EMERGENTE

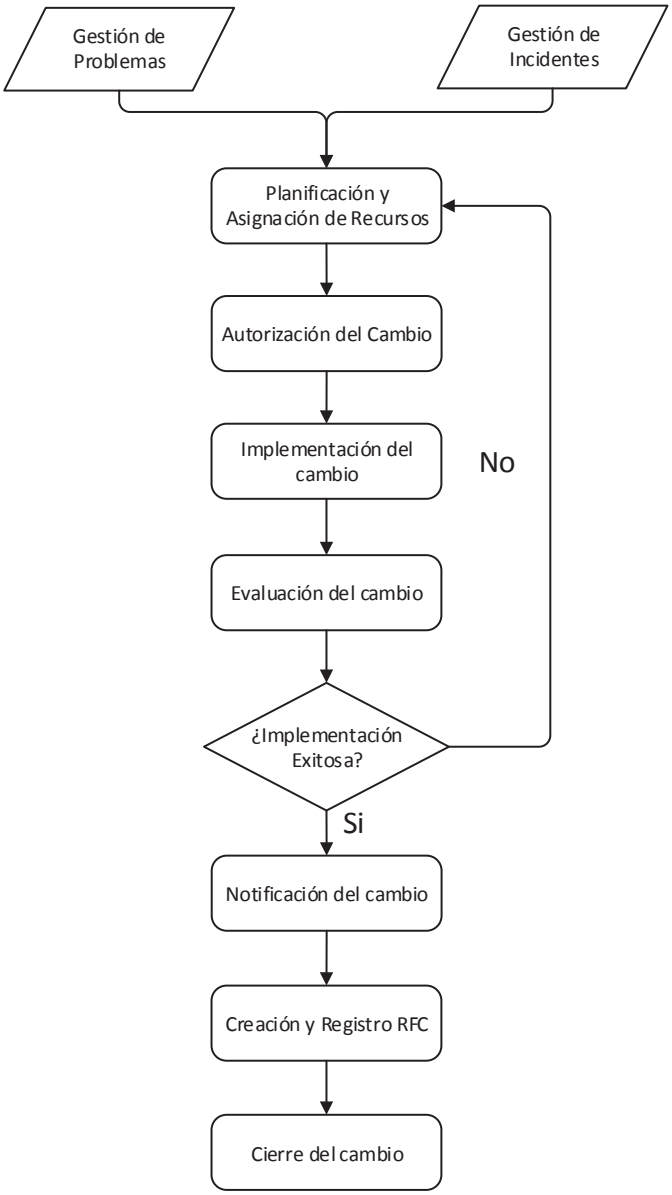


Figura 3.10 Diagrama del procedimiento de gestión de cambios emergente

3.6.9 DESARROLLO DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS ESTÁNDAR

Este procedimiento no requiere creación de RFC para su implementación y no presentará afectación en los servicios por esta razón se los conoce como cambios pre aprobados.

3.6.9.1 Revisión y análisis del cambio

Se revisará que las solicitudes recibidas cumplan con los parámetros necesarios para la realización del cambio y se solicitará autorización de la gerencia de O&M IP/MPLS previo a su ejecución.

3.6.9.2 Autorización del cambio

Si el cambio no es autorizado no se implementa y se procede con el cierre de la solicitud de cambio y devolución al solicitante indicando las causas por las que se ha rechazado su solicitud.

Si se autoriza, se planifica la implementación del cambio incluyendo fecha y hora adicionalmente las actividades a realizar, así como los recursos necesarios, mismos que se solicitarán a la gestión técnica.

3.6.9.3 Notificación e implementación del cambio

Se notificará el cambio a realizar al área de NOC y áreas relacionadas como Gestión de la red, gestión XDSL y multiservicios para que para que se encarguen de la actualización de sus herramientas de monitoreo al concluir el cambio.

Se implementará el cambio de acuerdo a la planificación previa. Si el cambio es exitoso, se cierra el procedimiento.

Si no es exitoso, se vuelve a planificar corrigiendo las fallas por las cuales fue necesario realizar el *rollback* y se solicita autorización nuevamente para realizar el cambio.

En caso de que la solicitud implique un cambio de contraseña, se lo ejecuta sin solicitar autorización previa y se notifica a la persona que realizó la petición, adicionalmente, se enviará la política para las contraseñas para el cambio al primer ingreso a los equipos. Esto se lo realiza con el propósito de evitar que los usuarios olviden realizar este cambio, lo que puede generar agujeros de seguridad que causen indisponibilidad de los servicios.

3.6.10 DIAGRAMA DEL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EMERGENTE

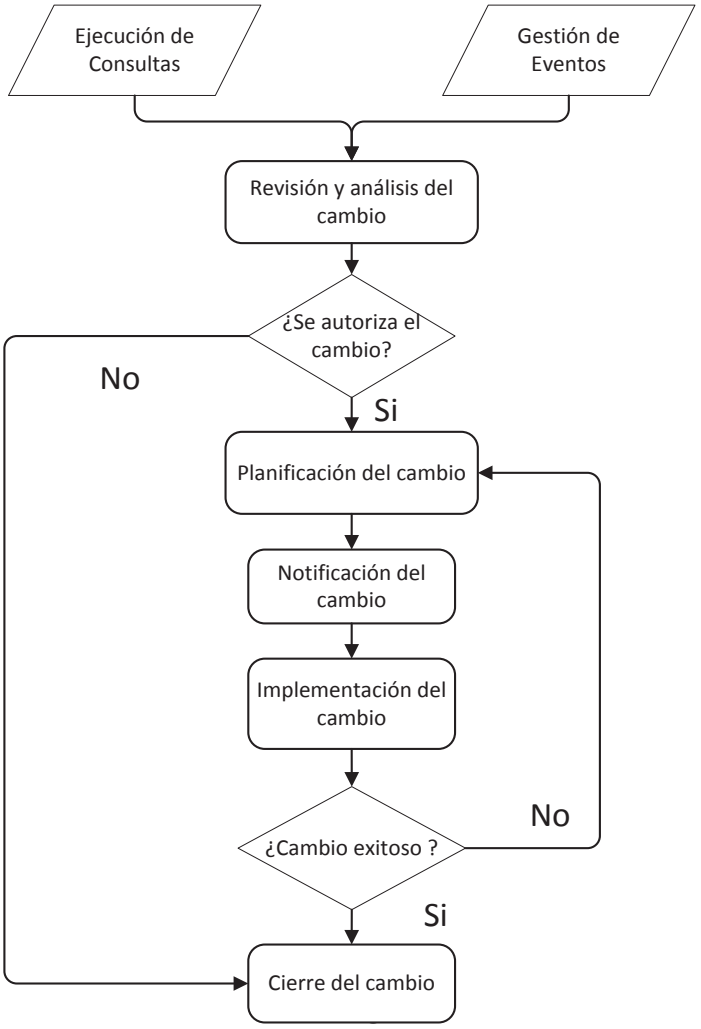


Figura 3.11 Procedimiento de Gestión de cambios estándar

3.7 EJEMPLOS DE APLICACIÓN DE LOS PROCESOS PLANTEADOS AL ÁREA DE O&M IP/MPLS

3.7.1 EJEMPLO 1

3.7.1.1 Paso 1 (Gestión de eventos)

Ocurrencia del evento: previamente se ha levantado la infraestructura (red MPLS capaz de detectar eventos) la cual se encarga del monitoreo constante de los elementos de red.

3.7.1.2 Paso 2 (Gestión de eventos)

Notificación del evento (lo realiza la herramienta de monitoreo): los equipos son interrogados por una herramienta de gestión mediante el protocolo SNMP e ICMP, los elementos de configuración empiezan a generar notificaciones.

3.7.1.3 Paso 3 (Gestión de eventos)

Detección del evento: el sistema de monitoreo detecta las notificaciones ya que no se tiene respuesta de los mismos.

3.7.1.4 Paso 4 (Gestión de eventos)

Filtrado: la herramienta de monitoreo realiza un filtrado de los eventos y genera 882 alarmas críticas de las cuales 802 clientes son home y 81 clientes son corporativos con un SLA del 99,6 %.

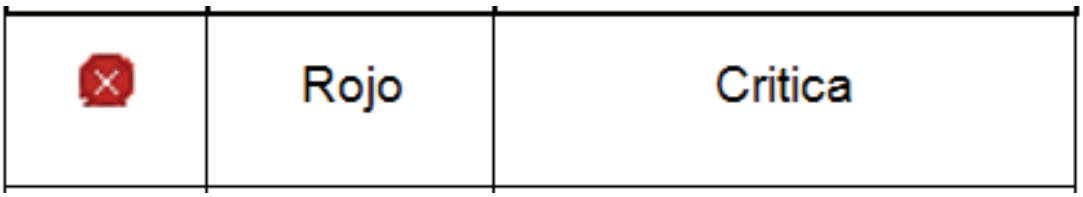


Figura 3.12 Ejemplo de alarma crítica

3.7.1.5 Paso 5 (Gestión de eventos)

El personal NOC monitorea la red y verifica las alarmas y asigna un significado de excepción debido a que las alarmas son críticas.

3.7.1.6 Paso 6 (Gestión de incidentes NOC)

Debido a que se trata de una excepción (interrupción del servicio) el evento pasa a ser un incidente y para su proceso se crea un ticket haciendo uso de la herramienta *Remedy* asignando la siguiente información:

- Número único de referencia: INC000000117211
- Fecha y hora en que ocurrió el incidente: 15/03/2016 20:32 pm

- Categorización: Elemento de Agregación
- Priorización: 1 (Crítico)
- Nombre del operador responsable
- Descripción: Se verifica alarmas en clientes masivos y corporativos
- Estado: En progreso
- Grupo al que ha sido asignado: Área O&M MPLS

3.7.1.7 Paso 7 (Gestión de incidentes NOC)

Se realiza escalamiento a Nivel 2, en este caso al área IP MPLS, una vez recibido el ticket, el ingeniero de turno se encargará de la revisión.

3.7.1.8 Paso 8 (Gestión de incidentes MPLS)

Se asigna a un técnico Nivel 2 quien realiza pruebas para diagnosticar el inconveniente surgido el cual muestra pérdida de rutas dentro del PE01 de Quito por lo que los clientes no tienen servicio de Internet.

3.7.1.9 Paso 9 (Gestión de incidentes MPLS)

Se verifica que es necesario realizar cambio emergente en la configuración de uno de los equipos principales por lo que se acude al proceso de gestión de cambios emergentes.

3.7.1.10 Paso 10 (Gestión de cambio emergente)

Se planifica los cambios que deben realizarse para reiniciar el servicio.

3.7.1.11 Paso 11 (Gestión de cambio emergente)

Se solicita autorización al ECAB, quien es el encargado de otorgar los permisos en el caso de cambios emergentes.

3.7.1.12 Paso 12 (Gestión de cambio emergente)

Una vez obtenida la autorización se realiza la configuración de enrutamiento por parte del técnico del área a quien fue asignado el caso restableciendo el servicio.

3.7.1.13 Paso 13 (Gestión de incidentes MPLS)

Se registran las acciones tomadas en la base de datos de incidentes y se registra el número de contador en 1 para el incidente.

3.7.1.14 Paso 14 (Gestión de incidentes NOC)

Se regresa el ticket al NOC para que valide el servicio con los clientes afectados.

3.7.1.15 Paso 15 (Gestión de incidentes NOC)

Una vez se haya confirmado con el cliente la estabilidad del servicio personal del NOC procede con el cierre del ticket.

3.7.1.16 Paso 16 (Gestión de incidentes NOC)

Debido a que se trata de un incidente crítico es necesario escalar al proceso de gestión de problemas para encontrar la causa raíz de la pérdida de rutas.

3.7.1.17 Paso 17 (Gestión de Problemas)

Se registra el problema dentro de la base de datos de error conocido utilizando la siguiente información obtenida del ticket generado para tratar el incidente.

- Número único de identificación: PIC117211
- Fecha y hora de apertura del caso: 16/03/2016 9:00 am
- Priorización: Alta
- Descripción del problema: se presenta una caída masiva de clientes debido a pérdida de rutas en el PE01 de Quito.
- Número de recurrencia: 1, se escala a problemas debido a que se trata de un incidente crítico
- Detalle de los diagnósticos y acciones correctivas: configuración nueva de enrutamiento.
- Detalle de servicios afectados: servicios de internet clientes corporativos y masivos
- Detalle de equipos afectados: Equipos de agregación

3.7.1.18 Paso 18 (Gestión de Problemas)

Se revisa la base de datos del error conocido para verificar si el incidente mencionado ha ocurrido con anterioridad, en este caso no se tiene registros.

3.7.1.19 Paso 19 (Gestión de Problemas)

Se realiza un análisis más profundo para determinar la causa de que se hayan borrado las rutas.

Se verifica que el equipo se reinició debido a que su procesamiento es alto y que no se cargaron todas las configuraciones cuando se encendió. Para brindar una solución definitiva y evitar un nuevo reinicio es necesario realizar el cambio del equipo.

3.7.1.20 Paso 20 (Gestión de Problemas)

Se actualiza la información dentro de la base de datos de error conocido en el campo detalle de los diagnósticos y acciones correctivas.

3.7.1.21 Paso 21 (Gestión de cambios normal)

Se plantea un RFC para realizar el cambio del equipo y se deben incluir los siguientes datos

1. **ALCANCE**

Cambio del PE01 de Quito por un equipo ASR901 con el propósito de mejorar las características del actual que está presentando fallas.

2. **ANTECEDENTES**

Se presenta un alto procesamiento en el equipo PE01 de Quito, lo que provoca que se reinicie y se pierdan configuraciones importantes.

3. **HORA Y FECHA DE EJECUCIÓN**

El cambio de equipo se realizará el 17 de marzo de 2016 a las 2:00 am ya que estas son horas de menor consumo.

4. TIEMPO TOTAL DE INDISPONIBILIDAD DEL SERVICIO:

Los clientes configurados dentro del PE01 de Quito no dispondrán de servicio durante 2 horas.

5. IMPACTO

Se presenta el listado de clientes afectados durante el mantenimiento.

Servicios Afectados			
Región	**Afectación De Trafico**	**Servicio**	**Observaciones**
R2	Indisponibilidad del servicio	Internet clientes masivos	Todos los clientes del Norte de Quito
		Internet clientes corporativos	

Tabla 3.7 Servicios afectados durante el mantenimiento

6. EQUIPOS INVOLUCRADOS (HW /SW)

PE01 Quito

7. RESUMEN DE ACTIVIDADES – DURACIÓN

#	Actividad	Duración	Responsable	Impacto (Red - Sistema)
1	Revisión de sistema de monitoreo Cisco Prime	30 min	NOC	Ninguna
2	Crear Backup del PE01 Quito	1 hora	MPLS	Ninguna
5	Cargar la configuración dentro del ASR 901	1 hora	MPLS	Ninguna
6	Verificar las conexiones del PE01 de Quito	15 minutos	MPLS	Ninguna

#	Actividad	Duración	Responsable	Impacto (Red - Sistema)
7	Desconectar el PE01 de Quito	30 minutos	MPLS	Corte de servicio a los clientes especificados
8	Conectar el ASR901	50 minutos	MPLS	Corte de servicio a los clientes especificados
9	Verificar que los clientes y servicios se encuentren operativos	30 min	NOC/ MPLS	Ninguna

Tabla 3.8 Resumen de actividades durante el mantenimiento

8. MATRIZ DE PRUEBAS / VALIDACIONES

#	Actividad	Procedimiento		Responsable
1	Revisión de servicios y crear backup	OK, Se inicia la siguiente actividad.	Caso contrario, informar que no es posible continuar con el cambio	NOC/MPLS
2	Cargar la configuración dentro del ASR 901	OK, Se inicia siguiente actividad	Caso contrario, se configura manualmente	MPLS
3	Verificación de servicios y operatividad de clientes	OK, fin de ventana	Caso contrario, realizar *rollback* hasta restablecer servicios.	MPLS

Tabla 3.9 Matriz de pruebas y validaciones

9. ROLLBACK

En caso de que no se verifiquen operativos los clientes, se procederá a desconectar el ASR 901 y se conectará nuevamente el PE01 de Quito.

10. ASIGNACIÓN DE RECURSOS

a) Responsables

Se detallan los nombres de las personas que intervendrán en el proceso.

Rol	Nombre	Número Teléfono	Responsabilidades
Operador NOC		0996183992	Monitoreo de clientes y servicios
Ingeniero MPLS	Alex Montes	0996183444	Cambio de equipo y configuración de ASR 901

T**abla 3.10** Roles y responsables en el mantenimiento

3.7.1.22 Paso 22 (Gestión de cambios normal)

Se envía el RFC a la comisión de cambios para que sea revisado.

3.7.1.23 Paso 23 (Gestión de cambios normal)

Se registra el RFC con prioridad e impacto alto, se revisa que esté correcta la información y se aprueba.

3.7.1.24 Paso 24 (Gestión de cambios normal)

Se asigna los recursos necesarios para la implementación del cambio como son el equipo ASR901 para el cambio y el operador NOC que se encargará del monitoreo constante durante la implementación.

3.7.1.25 Paso25 (Gestión de cambios normal)

Se notifica del cambio a realizar al NOC para que se encarguen de la notificación de afectación de servicios a los clientes corporativos.

3.7.1.26 Paso 26(Gestión de cambios normal)

El día y hora indicados se implementa el cambio de acuerdo al cronograma indicado en el RFC.

3.7.1.27 Paso 27 (Gestión de cambios normal)

Una vez que se haya realizado el cambio de equipo, el operador NOC de turno y el ingeniero del MPLS se encargarán de revisar que se hayan restablecido todos los servicios.

3.7.1.28 Paso 28 (Gestión de cambios normal)

Debido a que el cambio ha sido exitoso, se procede a cerrar el proceso, se envía un correo indicando las actividades realizadas y tiempo real de afectación.

3.7.2 EJEMPLO 2

3.7.2.1 Paso 1 (Gestión de incidentes NOC)

Los operadores NOC reciben un correo electrónico en el cual se reportan intermitencias en los enlaces de los clientes de Internet Masivo.

3.7.2.2 Paso 2 (Gestión de incidentes NOC)

Se verifica que es un incidente debido a que se está causando degradación de los servicios prestados.

3.7.2.3 Paso 3 (Gestión de incidentes NOC)

Se realiza el registro del incidente en la herramienta Remedy tomando en cuenta los siguientes parámetros

- Número único de referencia: INC000000112455
- Fecha y hora en que ocurrió el incidente: 10:05 am
- Categorización: Elemento de Acceso
- Priorización: 3 (Medio)
- Nombre del operador responsable
- Descripción: Se verifica intermitencias en clientes masivos
- Estado: En progreso
- Grupo al que ha sido asignado: NOC

3.7.2.4 Paso 4 (Gestión de incidentes NOC)

Con los comandos presentados en el anexo **A.2** se realizan las pruebas de primer nivel en los equipos de acceso donde se encuentran configurados los clientes afectados para obtener un diagnóstico y determinar una posible solución al incidente.

Con el comando show interface descripción se verifica el estado de la interfaz en ambos extremos. Se verifica que en la interfaz en el equipo A tiene un MTU de 1500 mientras que el equipo B Tiene un MTU de 1532

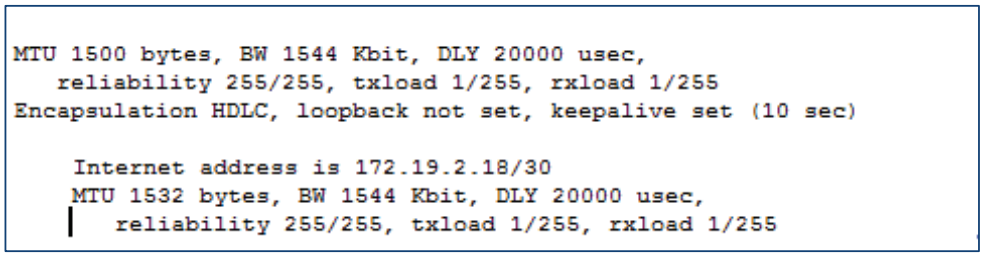


Figura 3.13 Pruebas de primer nivel en los equipos A y B

3.7.2.5 Paso 5 (Gestión de incidentes NOC)

Con el análisis realizado, se deduce que la causa de las intermitencias se debe a que el MTU es diferente. Es necesario modificar este parámetro y como se cuenta con los permisos necesarios para realizar este cambio, se procede a establecer en la interfaz del equipo A en 1532.

3.7.2.6 Paso 6 (Gestión de incidentes NOC)

Se realizan nuevas revisiones y se verifica que ya no hay pérdidas en el enlace y se procede con los pasos para cerrar el incidente.

3.7.2.7 Paso 7 (Gestión de incidentes NOC)

Se solicita la verificación de estabilidad del servicio y se realizan nuevas pruebas.

3.7.2.8 Paso 8. (Gestión de incidentes NOC)

Se recibe la notificación de que ya no existen pérdidas en los enlaces de los clientes, entonces se procede a cerrar el ticket.

3.7.3 EJEMPLO 3

Este ejemplo permitirá solicitar accesos a los equipos para un empleado nuevo del NOC.

3.7.3.1 Paso 1 (Gestión de Acceso)

El jefe del NOC debe llenar la solicitud de accesos del anexo A.3 en el cual se debe especificar los siguientes parámetros:

- Nombre del jefe inmediato (número de teléfono y correo electrónico)
- Área /proveedor
- Motivo de ingreso a los equipos de MPLS
- Datos de la persona a la que se asignará los accesos

Una vez llenados los datos descritos se procede con el envío a la persona de MPLS responsable de brindar los accesos.

3.7.3.2 Paso 2 (Gestión de Acceso)

Una vez recibida la solicitud, se verifica que la información sea válida y se solicita autorización a gerencia del área.

3.7.3.3 Paso 3 (Gestión de Acceso)

Se procede a crear el usuario utilizando los datos recibidos y se asigna una contraseña temporal, adicionalmente se realiza la configuración necesaria para que el usuario se vea obligado a cambiar la contraseña en el momento del primer acceso a los equipos..

3.7.3.4 Paso 4 (Gestión de Acceso)

Se envía un correo al solicitante con el usuario y la contraseña temporal, misma que deberá ser cambiada en el primer ingreso, por esta razón también se adjunta el documento con las políticas establecidas para la contraseña.

3.7.3.5 Paso 5 (Gestión de Acceso)

Mediante la herramienta ACS se realizará un seguimiento de los comandos ingresados por el usuario para validar el uso correcto de los accesos otorgados y se cierra el proceso.

3.7.4 EJEMPLO 4

3.7.4.1 Paso 1 (Gestión de Consultas)

Persona del área NOC solicita un cambio de contraseña para el acceso a los equipos de la red MPLS, para este objetivo envía un correo electrónico al responsable de gestión de acceso con la petición correspondiente.

3.7.4.2 Paso 2 (Gestión de Consultas)

La solicitud es receptada y se procede con su registro con la siguiente información:

- Número de referencia único: CON0000649
- Categorización: por servicio
- Priorización: Baja
- Fecha y hora: 9:43 am 23/04/2016
- Nombre de la persona o grupo que realiza la solicitud: NOC
- Método de notificación (teléfono o correo electrónico): correo electrónico
- Descripción de la solicitud: cambio de contraseña para acceso a los equipos.
- Nombre de la persona que atiende la consulta: José López ingeniero N2 O&M IP/MPLS
- Fecha y hora de cumplimiento de la solicitud: Por definir
- Fecha y la hora de cierre: Por definir

La información de hora de cumplimiento y cierre será completado una vez se resuelva la solicitud.

3.7.4.3 Paso 3 (Gestión de Cambio Estándar)

Este se trata de un cambio pre autorizado por lo cual el responsable de gestión de accesos lo realiza sin reportar al gerente de O&M IP/MPLS. Se ingresa al ACS, se busca al usuario y se cambia la contraseña y se selecciona la opción para que se cambie la contraseña en el primer acceso.

3.7.4.4 Paso 4 (Gestión de Consultas)

Se informa al solicitante que ha sido realizada su petición, para esto el solicitante valida la nueva contraseña y realiza el cambio solicitado en cuanto ingrese a los equipos, para esto debe consultar la política establecida para el cambio de contraseñas en donde deberá tomar en cuenta las recomendaciones existentes como son la longitud, caracteres especiales, mayúsculas, minúsculas.

3.7.4.5 Paso 5 (Gestión de Consultas)

Se procede con el cierre de la consulta y se actualiza el registro.

- Fecha y hora de cumplimiento de la solicitud:12:13 pm 23/04/2016
- Fecha y la hora de cierre: 14:32 pm 23/04/2016

3.7.5 EJEMPLO 5

3.7.5.1 Paso 1 (Gestión de Eventos)

Ocurrencia del evento: previamente se ha levantado la infraestructura (red MPLS capaz de detectar eventos)

3.7.5.2 Paso 2 (Gestión de Eventos)

Notificación del evento: los equipos son interrogados por una herramienta de gestión mediante el protocolo SNMP e ICMP, los elementos de configuración empiezan a generar notificaciones.

3.7.5.3 Paso 3 (Gestión de Eventos)

Detección del evento: el sistema de monitoreo detecta las notificaciones ya que no se tiene respuesta de los elementos de configuración

3.7.5.4 Paso 4 (Gestión de Eventos)

Filtrado: la herramienta de monitoreo realiza un filtrado de los eventos y genera alarmas en todos los servicios configurados en el enlace Quito – Quevedo dentro del las herramientas Cisco Prime y Cacti.

3.7.5.5 Paso 5 (Gestión de Eventos)

El personal NOC monitorea la red y verifica las alarmas en la herramienta Cisco Prime y CACTI debido a la caída de tráfico del enlace a las 12:00 por lo que se asigna un significado de excepción debido a que existe interrupción en el servicio de los clientes conectados a dicho enlace, de acuerdo a la **Figura 3.14**.

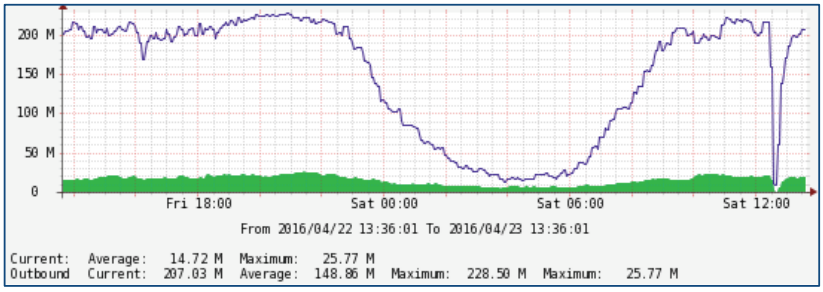


Figura 3.14 Gráfico de caída de tráfico en el CACTI

3.7.5.6 Pase 6. (Gestión de Incidentes)

Debido a que se trata de una excepción (interrupción del servicio) el evento pasa a ser un incidente y para su proceso se crea un ticket haciendo uso de la herramienta remedy asignando la siguiente información:

- Número único de referencia: INC000000117298
- Fecha y hora en que ocurrió el incidente: 16:32 pm 17/03/2016
- Categorización: Agregación
- Priorización: 2 (Alta)
- Nombre del operador responsable: Mauricio Pacheco
- Descripción: Se verifica alarmas en clientes masivos y corporativos en relacionados a un enlace troncal.
- Estado: En progreso
- Grupo al que ha sido asignado: NOC

3.7.5.7 Paso 7 (Gestión de Incidentes NOC)

Se realiza pruebas de primer nivel con lo cual no se encuentra la solución por lo que se procede con el escalamiento al área IP MPLS.

3.7.5.8 Paso 8 (Gestión de Incidentes MPLS)

Se asigna a un técnico Nivel 2 quien realiza pruebas para diagnosticar el inconveniente surgido.

3.7.5.9 Paso 9. (Gestión de Incidentes MPLS)

Se realizan pruebas de segundo nivel donde no encuentran problemas por lo que es necesario escalar al área de transmisiones, esto lo realizan por medio de llamada telefónica y correo electrónico por lo que continuarán el seguimiento y actualización del ticket cada 30 minutos.

3.7.5.10 Paso 10 (Gestión de Incidentes MPLS)

Personal de transmisiones realizan pruebas sobre instalaciones físicas relacionadas al enlace caído encontrando que la causa de caída del enlace es ruptura de la fibra principal la cual fue arrancada por la empresa eléctrica debido a cambio de postes.

Esperan a que la empresa eléctrica termine sus trabajos para proceder con la fusión de 48 hilos. Al terminar los trabajos los servicios se restablecen el informe es enviado al área MPLS.

3.7.5.11 Paso 11. (Gestión de Incidentes MPLS)

El área MPLS actualiza el registro del ticket. Y valida con el NOC que las herramientas de monitoreo no genera alarmas relacionadas a este incidente y que todos los servicio hayan sido levantados.

3.7.5.12 Paso 12 (Gestión de Incidentes MPLS)

Una vez validados los servicios se procede a actualizar el estado del ticket y su información necesaria.

Estado: Cerrado
Fecha y hora de cierre: 22:13 pm 18/03/2016

CAPÍTULO 4

PLAN DE MEJORA CONTINUA DE LOS PROCESOS DEL ÁREA DE O&M DE CNT E.P.

En este capítulo se presentará el plan de mejora continua que contendrá las metas por cada proceso de la etapa de operación del servicio, para esto se presentarán los indicadores que permitirán medir el cumplimento y rendimiento de los procesos, los cuales se analizarán periódicamente para mejorar continuamente el desempeño del área.

4.1 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE EVENTOS

4.1.1 METAS

- Detectar oportunamente los cambios de estado que producen afectación sobre los elementos de red y los servicios.

- Asegurar que los eventos se comuniquen oportunamente y de forma correcta para que se tomen las medidas de control necesarias.

- Asegurar el rendimiento operacional de la red.

4.1.2 INDICADORES DE RENDIMIENTO

- ***Número y porcentaje de eventos en comparación con el número de incidentes***, este indicador permitirá conocer los incidentes detectados con ayuda de las herramientas de monitoreo.

- ***Número y porcentaje de eventos que requieren la intervención humana y si estos han sido solventados***, este indicador brindará un

informe del número de eventos que han necesitado intervención humana para solventarse y si éstos han sido atendidos.

- ***Número de incidentes que se produjeron y el porcentaje de estos que se activa sin un evento correspondiente***, este indicador permitirá determinar el número de elementos de red que no han sido añadidos a las herramientas de monitoreo.

- ***Número de eventos que han dado lugar a incidentes***, con este valor se medirá el número de excepciones presentadas las cuales se resolvieron mediante el proceso de gestión de incidentes.

- ***Número y porcentaje de eventos causados por los problemas existentes o errores conocidos***, este indicador permite conocer los eventos que se siguen presentando porque no se ha dado una solución a la causa raíz del incidente.

- ***Número y porcentaje de eventos reincidentes que pueden causar un gran impacto en el servicio***, este porcentaje permitirá medir los eventos que se presentan reiteradamente y si se ha tomado acción sobre estos para disminuirlos y resolverlos.

4.1.3 ANÁLISIS DE DATOS

Para este análisis, se toma en consideración los tres últimos informes presentados a gerencia por parte del proveedor en el intervalo desde 00:00 am hasta las 08.00 am.

Cabe recalcar que en este caso se ha tomado el periodo de 3 semanas debido a que esta política fue implementada en el último mes.

En base a los informes presentados, se verifica que se obtienen el número de excepciones generadas sin realizar la comparación con el número de eventos totales.

También se evidencia que estos informes se están realizando en base a una única herramienta de monitoreo.

Se verificó que se registran los eventos presentados, pero no se indican qué acciones fueron tomadas para solventarlos y si estos son repetitivos, tampoco se discrimina cuáles han sido excepciones.

En base a lo indicado anteriormente, no se puede medir el desempeño del proceso de gestión de eventos.

4.1.4 RECOMENDACIONES DE MEJORA CONTINUA

En base al análisis de los datos proporcionados, a continuación se definen las acciones correctivas que permitirán mejorar continuamente el proceso de gestión de eventos.

Se deben realizar informes de monitoreo semanales por parte del personal encargado de monitoreo durante las 24 horas acorde al formato del ANEXO B.1, los cuales deben enviarse a la persona responsable de la gestión de eventos del área O&M para luego consolidarse en un informe mensual y entregarse a Gerencia, este documento debe contener los siguientes indicadores:

- Número total de eventos, discriminando excepciones y advertencia no será necesario registrar los de información ya que estos indican el correcto funcionamiento de la red.

- Número de alarmas de advertencia reincidentes indicando el número de veces que se han presentado y las acciones tomadas para solventarlas.

- Se debe registrar el número de alarmas críticas, si estas fueron escaladas, a quién fueron escaladas y su categorización.

- Se debe presentar el número de incidentes que se produjeron sin la activación de una alarma.

En base a los eventos presentados adicionalmente, en el informe de monitoreo mensual constará el número y porcentaje de eventos causados por los problemas existentes o errores conocidos, para esto se comparará con la base de datos de gestión de problemas y se realizará un análisis para brindar la solución definitiva y evitar que se repita el evento.

4.2 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE INCIDENTES

4.2.1 METAS

- Resolver incidentes tan pronto como sea posible, minimizando el impacto sobre los servicios.

- Mantener la calidad de los servicios.

- Asegurar la utilización de procedimientos estandarizados para brindar una pronta solución a los incidentes.

4.2.2 INDICADORES DE RENDIMIENTO

- ***Tiempo promedio de resolución de incidentes dependiendo del impacto***, este indicador permite conocer el tiempo de resolución de los incidentes dependiendo de su categorización.

- ***Número total de incidentes***, número de incidentes totales atendidos.

- ***Porcentaje de incidentes resueltos y cerrados sin necesidad de escalamiento***, este indicador ayudará a medir el porcentaje de tickets solucionados sin haber escalado al siguiente nivel.

- ***Número y porcentaje de incidentes resueltos remotamente***, se medirá el número de incidentes que se han resuelto mediante configuración remota.

- ***Número y porcentaje de incidentes escalados al proveedor***, este dato permitirá conocer el porcentaje de los incidentes que no se han dado solución con personal del área, si no que tuvieron que ser escalados al proveedor.

- ***Número y porcentaje de incidentes críticos***, permitirá conocer el número de incidentes críticos presentados que causaron serias afectaciones sobre los servicios.

- ***Número y porcentaje de incidentes escalados incorrectamente***, este indicador mide el porcentaje de tickets que se han escalado al área de O&M IP MPLS incorrectamente, lo mencionado se puede presentar en los siguientes casos: escalamiento de un ticket con un incidente correspondiente a otra área, o que se lo asigna sin haber realizado todas las pruebas correspondientes.

- ***Número y porcentaje de incidentes incorrectamente categorizados***, con este indicador se verifican los incidentes que se han asignado prioridad y urgencia de forma errónea por lo cual no se han tratado con la categoría correcta.

- ***Número y porcentaje de incidentes que no fueron escalados oportunamente***, este indicador permitirá conocer el número de incidentes que sobrepasaron el umbral de tiempo estipulado para la revisión de nivel 1 y que al no solventarse fueron escalados de forma tardía por lo cual ocasionaron alto impacto en el servicio.

4.2.3 ANÁLISIS DE DATOS

Para el análisis de datos se tomarán en cuenta los informes realizados de los últimos dos meses ya que a partir de esa fecha se obtienen los datos de incidentes. Cabe recalcar que los informes obtenidos únicamente muestran información de los incidentes escalados al proveedor.

Debido a que se cuenta con información parcial, no se mostrarán estadísticas sobre el análisis de datos.

4.2.4 RECOMENDACIONES DE MEJORA CONTINUA

En base a los informes recopilados, se establecen las acciones correctivas que permitirán mejorar continuamente el proceso de gestión de incidentes.

Se deben realizar informes de todos los incidentes atendidos semanalmente por parte del personal del NOC y O&M MPLS acorde a los formatos del ANEXO B.2, estos informes serán enviados al responsable de la gestión de incidentes del área O&M y deben contener los siguientes datos:

- Número de ticket asignado mediante la herramienta gestora de tickets.
- Descripción del incidente.
- Nombre del operador a cargo del ticket.
- Priorización del incidente.
- Tiempo de resolución del incidente.
- Descripción de la solución.
- En caso de escalamiento, se debe registrar el nombre del Ingeniero O&M a cargo.
- Estado del incidente

La persona responsable de la gestión de incidentes consolidará estos datos en un informe mensual que se entregará a gerencia, este documento debe contener los siguientes indicadores:

- Número total de incidentes
- Número de incidentes críticos
- Número de incidentes resueltos por el NOC que afecten a la red IP/MPLS
- Número de incidentes resueltos por el MPLS
- Número de incidentes resueltos con apoyo del proveedor
- Número de incidentes resueltos mediante configuración remota.

- Número de tickets escalados incorrectamente
- Número de incidentes incorrectamente priorizados
- Número de incidentes escalados a la gestión de problemas.

En base a los indicadores se deben presentar estadísticas, para ser analizadas posteriormente.

4.3 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE PROBLEMAS

4.3.1 METAS

- Minimizar el impacto de los incidentes que no se pueden prevenir.

- Mantener la calidad de los servicios a través de la eliminación de los incidentes recurrentes.

- Identificar los problemas tan pronto como sea posible para establecer la solución correspondiente.

4.3.2 INDICADORES DE RENDIMIENTO

- ***Número de problemas solventados añadidos a la base de datos de errores conocidos***, este indicador permitirá conocer el número de problemas a los que se ha dado solución y sus acciones correctivas.

- ***Número total de problemas (abierto, cerrado y en proceso de solución)***, este indicador permitirá conocer el estado de cada uno de problemas y si el número de problemas sin resolver es mayor al número de problemas solucionados.

- ***Número de incidentes repetitivos***, este indicador permitirá medir los incidentes que se hayan identificado como problemas debido a su reincidencia.

- ***Número de problemas que superan el tiempo máximo de resolución***, este indicador medirá el nivel de cumplimento de los umbrales de tiempo en los que se debe brindar una solución a los problemas dependiendo de su categorización.

- ***Número de mantenimientos preventivos***, con este indicador se verificarán las acciones tomadas para evitar reincidencias que causen afectación de los servicios.

- ***Número y porcentaje de problemas asignados incorrectamente***, este indicador permitirá conocer los problemas que han sido escalados sin corresponder al área.

4.3.3 ANÁLISIS DE DATOS

De la recopilación de datos se puede verificar que la información contenida en la documentación no permite obtener los indicadores sugeridos por ITIL para la medición del rendimiento del proceso de gestión de problemas, debido a que no se tienen los registros de incidentes repetitivos, ni los detalles de escalamiento al proceso de problemas para su gestión.

4.3.4 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE PROBLEMAS

Para cumplir con la mejora continua de la gestión de problemas el responsable de este proceso debe elaborar un informe mensual fundamentado en la base de datos de errores conocidos para ser entregado a gerencia y contendrá los siguientes parámetros:

- Número total de problemas.
- Número total de problemas que se encuentran en proceso de solución.
- Número total de problemas solucionados.
- Número de incidentes repetitivos identificados como problemas.
- Tiempo promedio de resolución de los problemas de acuerdo a su categorización.

- Número de problemas que superan el tiempo máximo de resolución.
- Número de mantenimientos preventivos.
- Número de problemas asignados incorrectamente.

Adicionalmente se sugiere cumplir rutinas de mantenimiento que permitan revisar el estado de los equipos periódicamente y en caso de requerir cambios se tomará la guía del procedimiento de cambios estándar.

El formato del informe mensual se presenta en el Anexo B.3

4.4 MEJORA CONTINUA DE GESTIÓN DE ACCESOS

4.4.1 METAS

- Asegurar la confidencialidad, integridad y disponibilidad de la información correspondiente a los elementos de red y herramientas de monitoreo para evitar el uso inadecuado de los permisos de acceso que puedan causar indisponibilidad de los servicios.

- Proporcionar acceso a los servicios de manera eficiente y oportuna.
- Brindar el seguimiento sobre las actividades de acceso que ocasionan incidentes y problemas.

4.4.2 INDICADORES DE RENDIMIENTO

- ***Porcentaje de incidentes causados por uso inadecuado de permisos de acceso***, este indicador permite conocer el número de veces que se afectaron los servicios a causa de permisos de acceso incorrectos.

- ***Número de configuraciones de acceso incorrectos para los usuarios que han cambiado los roles o dejado la empresa***, esta métrica permitirá determinar el número de veces que se asignaron permisos incorrectamente a los usuarios que solicitaron cambios sobre las

configuraciones de sus permisos de acceso, sea por cambio de área o por dejar la empresa.

- ***Número de solicitudes de acceso procesadas***, número total de solicitudes llevadas a cabo con éxito.

- ***Tiempo promedio de cumplimiento de la solicitud de acceso***, este indicador permitirá conocer el tiempo promedio que toma cumplir una solicitud de acceso.

- ***Número de alertas proporcionadas por las herramientas sobre el uso indebido y no autorizado de la información***, con este indicador se verificará el número de alertas que se han generado sobre uso indebido y no autorizado de la información, además se conocerán las acciones correctivas tomadas sobre estas alertas.

4.4.3 ANÁLISIS DE DATOS

Se han recopilado los datos de mayo, junio, julio, agosto y septiembre de 2015 en los que se pudieron verificar los porcentajes de intentos fallidos de acceso a la red con la alerta generada por la herramienta ACS, estos se presentan en la **Tabla 4.1**y la **Figura 4.1**

Nº	Alerta	Porcentaje de aparición de la alerta (%)
1	Request packet - possibly mismatched shared Secrets	0,03
2	Request was dropped because of system overload	97,66
3	Authentication request missing user Password	0,05
4	Authentication request missing a User name	0,07
5	Select Shell Profile is Deny Access	0,01
6	Authentication request does not contain the new password of user.	0,01
7	Authentication request contains an empty string in the Confirm New User Password field.	0,00

Nº	Alerta	Porcentaje de aparición de la alerta (%)
8	Authentication request to confirm the new password of user has failed.	0,03
9	Wrong Password or invalid shared secret	1,32
10	Subject not found in the applicable identity store (s).	0,67
11	Authentication failed. User account is disabled due to excessive failed authentication attempts.	0,01
12	Could not change password to new password	0,01
13	User disable	0,13

Tabla 4.1 Porcentaje de intentos fallidos de acceso a la red

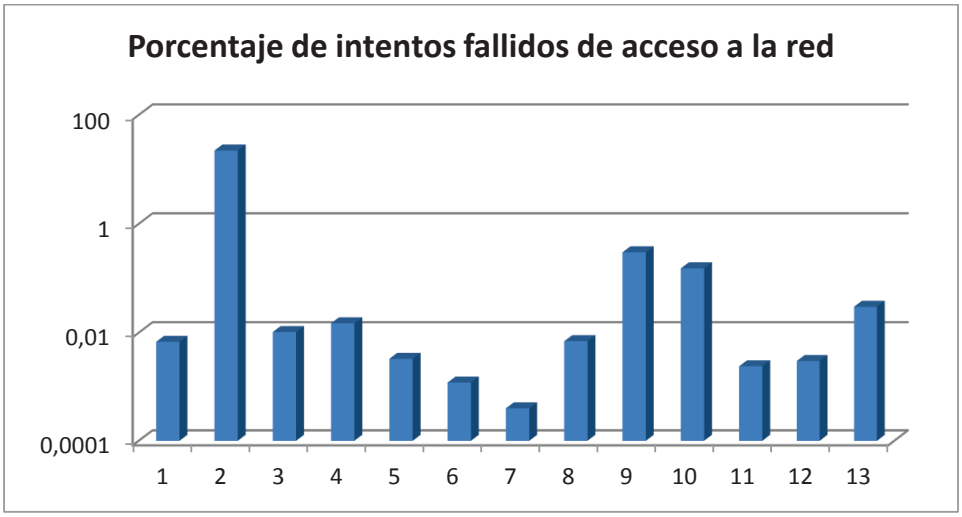


Figura 4.1 Porcentaje de aparición de alertas en la herramienta ACS

De los datos recopilados también se verifica que existe documentación de las solicitudes de acceso recibidas pero no se lleva un registro de aquellas que se han cumplido y tampoco de las que han sido rechazadas, por lo cual no se pueden obtener los indicadores sugeridos por ITIL para medir el rendimiento del proceso.

Adicionalmente se verifica que el más alto porcentaje es de rechazo de acceso a causa de la sobrecarga del sistema, pero no se han tomado acciones para dar una solución definitiva a este problema, ni a ninguno de los otros casos obtenidos de los *logs*.

4.4.4 RECOMENDACIONES DE MEJORA CONTINUA

Con el propósito de mejorar continuamente el rendimiento de este proceso el responsable de gestión de accesos debe presentar un informe mensual a gerencia que contendrá los siguientes indicadores:

- Número total de solicitudes recibidas
- Número de solicitudes de acceso procesadas con éxito
- Número de solicitudes de cambio de configuración
- Número de solicitudes rechazadas justificadas
- Número de usuarios deshabilitados
- Número de veces que se afectaron los servicios a causa de permisos de acceso incorrectos
- Número de alertas por intentos fallidos de acceso a la red y las acciones que se han tomado para disminuir dichas alertas.
- Tiempo promedio de cumplimiento de la solicitud de acceso.

Además es necesario detallar las acciones correctivas aplicadas para evitar la reincidencia de alertas de negación de acceso y uso indebido de permisos en cada incidente presentado a causa de incumplimiento de políticas de acceso.

4.5 MEJORA CONTINUA DEL PROCESO DE GESTIÓN DE CONSULTAS

4.5.1 METAS

- Cumplir las solicitudes de manera eficiente y oportuna

- Cumplir únicamente las solicitudes autorizadas

4.5.2 INDICADORES DE RENDIMIENTO

- ***Tiempo promedio de cumplimiento de consultas***, este indicador permite medir el tiempo que toma en cumplir las solicitudes receptadas y autorizadas.

- ***Número de consultas atendidas***, este indicador nos permitirá el número total de consultas atendidas.

- ***Porcentaje de solicitudes de servicio rechazadas***, con este indicador se verificarán las solicitudes que no se han llevado a cabo por falta de autorización.

4.5.3 ANÁLISIS DE DATOS

Debido a que no se lleva un registro de las actividades realizadas para el cumplimiento del proceso de consultas, a razón de que era inexistente en el área no se obtuvieron datos para el análisis.

4.5.4 RECOMENDACIONES DE MEJORA CONTINUA

Para medir el rendimiento del proceso de mejora continua se debe llevar un registro de las consultas que se desarrollen y en base al mismo elaborar un informe mensual que contenga los siguientes datos:

- Fecha de apertura de la consulta
- Tiempo de solución de la consulta
- Nombre de la persona asignada a cumplir con la solicitud
- Número total de solicitudes atendidas
- Número de solicitudes rechazadas justificadas

4.6 MEJORA CONTINUA DE CAMBIOS:

4.6.1 METAS

- Asegurar que los cambios sean gestionados, registrados e informados de forma correcta

- Cumplir con los cambios y la planificación planteada en los RFC para minimizar el Impacto en los servicios.

4.6.2 INDICADORES DE RENDIMIENTO

- ***Número de cambios que han sido registrados****,* este indicador permitirá conocer el total de cambios solicitados.

- ***Número de cambios implementados de forma exitosa***, este indicador permite medir el número de cambios que se realizaron dentro de la planificación establecida y sin realizar rollback.

- ***Porcentaje de cambios que han sido rechazados***, esta métrica determinará los cambios cuya implementación no ha sido autorizada porque no cumplen los parámetros establecidos.

- ***Porcentaje de cambios fallidos que requirieron rollback***, este valor indicará los cambios que no se realizaron exitosamente debido a que no se implementaron todos o algunos de los pasos especificados, por lo cual fue necesario revertir al estado previo.

- ***Porcentaje de los cambios que han requerido mayor tiempo del planificado****,* este indicador permite determinar aquellos cambios que se implementaron exitosamente pero demandaron más tiempo de lo planificado.

- ***Porcentaje de cambios emergentes***, esta cantidad permitirá conocer los cambios realizados de forma emergente para solventar incidentes.

4.6.3 ANÁLISIS DE DATOS

Para el análisis de datos del proceso de cambios se ha recopilado información de los meses de mayo, junio, julio, agosto y septiembre de 2015.

Se verifica que los miembros del área llevan un registro de las actividades realizadas, sin embargo no se clasifican para obtener los indicadores necesarios para mejorar continuamente el proceso, por lo cual se realizó un análisis de dicha

información donde se ha discriminado cambios normales, preventivos y emergentes obteniendo los valores que se muestran en la **Figura 4.2**.

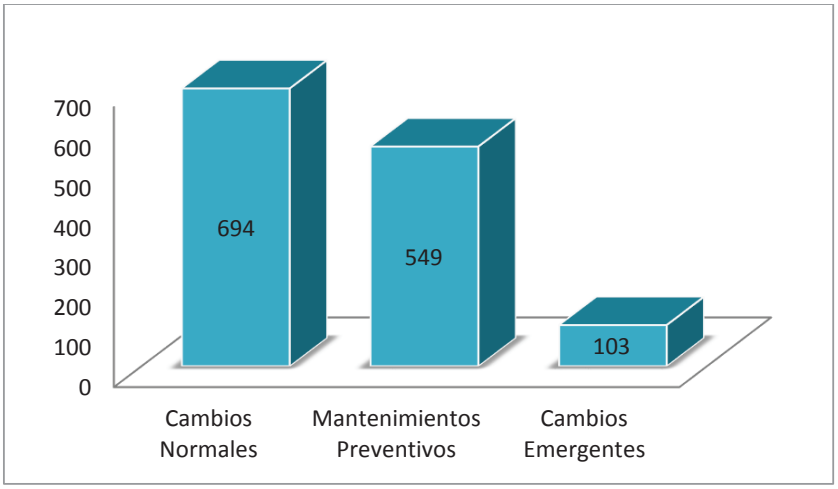


Figura 4.2 Cambios y Mantenimientos Preventivos

De los informes recopilados se tiene el número de mantenimientos preventivos, pero en su mayoría no se detallan los equipos sobre los cuales se aplicaron, el impacto que produjeron ni su descripción.

4.6.4 RECOMENDACIONES DE MEJORA CONTINUA

Con el propósito de mejorar continuamente el rendimiento de este proceso el responsable de gestión de cambios debe presentar un informe mensual a gerencia que contendrá los siguientes indicadores:

- Número de cambios estándar realizados
- Número de cambios emergentes realizados
- Número de cambios normales realizados
- Número total de cambios realizados
- Número de RFC implementadas con éxito
- Número de RFC rechazados y no autorizados.

El formato del informe se encuentra en el anexo.

CAPÍTULO 5

CONCLUSIONES Y RECOMEDACIONES

5.1 CONCLUSIONES

- La investigación acerca del levantamiento y componentes de los procesos en una organización permitió conocer su importancia a la hora de cumplir con las actividades para brindar un servicio específico de forma eficiente y con un índice de disponibilidad alto.

- Se verificó que el área de O&M de las plataformas IP MPLS requiere de una estructura de procesos bien definidos de operación y mantenimiento como son: eventos, incidentes, consultas, problemas y accesos para cumplir con las metas del servicio y del negocio ya que es un área esencial para el aprovisionamiento de los servicios prestados por CNT.

- Como resultado del estudio realizado mediante el marco de referencia COBIT 4.1 se determinó que para cumplir con los objetivos del negocio es importante realizar la medición del nivel de madurez mediante la auditoría de los procesos en los que se está guiando una empresa para corregir falencias y plantearse nuevas metas para superar dichos niveles.

- Se verificó que ITIL es un conjunto neutral y no prescriptivo de buenas prácticas que se adaptan a las necesidades de la empresa sin imponer reglas y permiten gestionar los procesos de una organización de manera eficaz y eficiente para garantizar calidad en los servicios ofrecidos.

- Se pudo verificar que un error muy común dentro del área de O&M plataformas IP MPLS de la Corporación Nacional de Telecomunicaciones es no distinguir los eventos de los incidentes y problemas, como ejemplo el personal del área tomaba como un evento un corte de fibra lo cual

ocasionó que no se lleve un registro adecuado de estos, por lo que fue necesaria la definición de estos procesos.

- Se observó que a causa de no llevar los procesos ordenadamente, se produjeron consecuencias graves sobre la prestación del servicio, pues se generaron retrasos en la resolución de incidentes, problemas y consultas, lo que causó inconformidad en los clientes.

- El presente trabajo permitió identificar mediante la auditoría los procesos inexistentes como gestión de eventos, consultas y problemas, además se midieron los procesos que se aplicaban de forma mecánica sin un control ni un flujo establecido; por lo cual el nivel de madurez fue bajo en la mayoría de los procesos y en el caso de la gestión de accesos se lo calificó en un nivel de madurez 3, la cual fue la más alta, debido a que la empresa cumple con la norma ISO 27000.

- Debido a que en el área de operaciones de la CNT E.P. las actividades definidas para todos los procesos planteados ocasionalmente requieren realizar cambios, se planteó la guía para la normalización de éste proceso mediante la gestión de cambios de la etapa de Transición del ciclo de vida de ITIL.

- Se alineó el planteamiento del RFC sugerido por ITIL con el MOP (*Method of Procedure*) que actualmente se maneja en el área, donde se plantean las actividades a cumplir durante la implementación de cambios.

- Se planteó el proceso de gestión de consultas, debido a que en la auditoría se verificó de que se da solución a peticiones de otras áreas como ingeniería, gestión de la red y el NOC sin llevar un registro de éstas.

- Se implementó el proceso de gestión de problemas para reducir el tiempo que emplean los miembros del área en resolver incidentes repetitivitos, lo cual mejorará el rendimiento en otras tareas asignadas.

- Se definieron indicadores para cada uno de los procesos planteados mismos que permitirán medir el rendimiento de estos y de ser necesario plantear cambios que permitan mejorar su desempeño.

- Se evidenció que es necesario definir un responsable por cada proceso con el objetivo de mantener un control adecuado del cumplimiento de éstos y supervisar el manejo correcto de la información para garantizar que sea útil para el planteamiento de mejora continua.

- Se determinó que es indispensable realizar rutinas de mantenimiento que permitan realizar revisiones constantes de la red IP MPLS así como de sus elementos de configuración para detectar posibles fallas que afecten el funcionamiento normal de los servicios.

- Se definió que los mantenimientos preventivos estarán ligados a la guía de gestión de cambios normal y se realizarán con el propósito de resolver fallas en la red o elementos de configuración que puedan provocar incidentes que causen interrupción de los servicios.

5.2 RECOMENDACIONES

- La demanda de regulación a las empresas obliga a tomar una guía estándar para funcionar en base a ella de forma ordenada y precisa, por lo que se recomienda no pasar por alto realizar un estudio antes de acatarse a una en específico.

- Para garantizar la mejora de la calidad de los servicios, será necesario aplicar las prácticas ITIL a los procesos de las otras áreas O&M.

- Una vez que estos procesos sean implementados, se recomienda realizar auditorías al menos una vez al año para saber en qué estado de madurez se encuentran y por medio de esto tener en cuenta las mejorías que se deben agregar para plantear nuevos procedimientos.

- Se recomienda socializar los procesos establecidos una vez aprobados, además resulta esencial una capacitación para aclarar diferencias entre Incidentes, eventos y problemas en vista de que la mayoría del personal de O&M ignora estos conceptos básicos e importantes.

- Es importante llevar un registro adecuado de incidentes y problemas para reducir tiempos de resolución de los mismos.

- Se recomienda priorizar los incidentes correctamente para brindarles una correcta atención que permita cumplir los tiempos establecidos y reducir la indisponibilidad de los servicios.

- Se recomienda que en la gestión del proceso de cambios siempre se notifique a todas las áreas involucradas antes y después de su implementación.

- Es imperativo registrar, informar y actualizar en las herramientas de monitoreo los cambios realizados para evitar confusiones al momento de realizar la gestión de eventos o incidentes que puedan alargar los tiempos de resolución.

- Es importante crear un comité de cambios en el cual se incluyan los miembros del NOC, MPLS e ingeniería para verificar que todos los parámetros indicados en los RFC sean apropiados para garantizar la menor afectación posible al momento de implementarlos.

- Las herramientas de monitoreo utilizadas por el área son adecuadas, sin embargo, se recomienda implementar nuevas herramientas, mismas que permitan una notificación más eficiente de las alarmas generadas.

- Se recomienda designar un responsable para la gestión de cada proceso de la etapa de operación del servicio.

- Es importante que la gerencia del área tenga una participación activa para garantizar el cumplimiento de los procesos levantados mediante ITIL, lo que permitirá que la calidad de los servicios brindados por el área mejore continuamente.

- Se requiere realizar reuniones entre el gerente de O&M MPLS y los responsables de cada proceso periódicamente para verificar si los procesos se están desarrollando correctamente, y en caso de ser requerido, se deben plantear nuevos indicadores que permitan cumplir con las metas planteadas.

- Es importante mantener una comunicación activa entre áreas para brindar un servicio más eficiente y que se cumplan todos los requerimientos de manera oportuna.

- Se sugiere que durante la reunión mantenida para el análisis de la mejora continua de los procesos se verifique el número de cambios que no fueron informados, por lo cual fueron tratados por la gestión de incidentes.

- Para mejorar de forma continua los procesos que se siguen en el área se deben elaborar informes con los indicadores sugeridos para analizarlos periódicamente y tomar las medidas correspondientes para mejorar los umbrales de tiempos de respuesta y disminuir los problemas e incidentes.

REFERENCIAS BIBLIOGRÁFICAS

[1] Shirley López, *Guía para el levantamiento documentación y rediseño de procesos*, Segunda ed., 2007.

[2] Ministerio de planificación nacional y política, Área de Modernización del Estado, *Guía para el Levantamiento de Procesos*., 2009.

[3] IT Governance Institute, *COBIT 4.1*, 3rd ed. United States of America, 2007.

[4] José Manuel Ballester Fernández, Gobierno Corporativo TIC, 2008.

[5] Karel Kohout, IT Risk Register, 2012 - 2013.

[6] IT Governance Institute, *Cobit Objetivos de Control*, 3rd ed. Estados Unidos de América, 2000.

[7] Hernán Lara Muñoz, José Humberto Reyes Reina, and Washington Navarrete Mera, *Diseño de Sistema de Gestión de Seguridad de Información*.: Escuela Politécnica del Litoral, 2006.

[8] ITSM, *ITIL Fundation Complete Certification Kit*., Edición 2011.

[9] ITSM, *Service Transition*. United Kingdom: TSO (The Stationery Office), Edición 2011.

[10] ITSM, *ITIL Service Operation*. United Kingdom: TSO (The Stationery Office), Edición 2011.

[11] ITSM, *Continual Service Improvement*. United Kingdom: TSO (The Stationery Office), Edición 2011.

[12] IT Governance Institute, Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa, 2008.

[13] Área O&M IP MLS CNT E.P. , Organización Interna del área IP MPLS, 2012, Documento interno IP MPLS.

[14] Area IP MPLS CNT E.P., Organigrama del área O&M IP MPLS, 2015.

[15] Inc. Cisco Systems, Cisco Prime Infrastructure 2.0 User Guide, 2013.

[16] Cisco. Working with the Cisco Prime Network Vision. [Online]. http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network/3-9/user/guide/CiscoPrimeNetwork-UserGuide/nv-getstart.pdf

[17] CNT E.P., Cisco Prime Network.

[18] CNT EP, Cisco prime Network Events.

[19] CNT E.P, Prime Network Administration.

[20] CNT E.P, Vista CACTI.

[21] Inc. Cisco Systems. User Guide for Cisco Secure Access Control System 5.2. [Online]. http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-2/user/guide/acsuserguide.pdf

[22] CNT E.P, Herramienta ACS.

[23] BMC Software. Suite BMC Remedy IT Service Management. [Online]. http://documents.bmc.com/products/documents/39/94/63994/63994.pdf

[24] Komputerkraft. Komputerkraft. [Online]. http://www.komputerkraft.co.nz/kkc-products/remedy/

[25] Fondo de prevención y atención de emergencias - FOPAE. (2014, Enero) METODOLOGÍAS DE ANÁLISIS DE RIESGO. [Online]. http://www.sire.gov.co/documents/12134/43764/A.3.4+Metodologias+AR.pdf/288b65be-c4d8-4d3f-a5f6-51942324e699

[26] IT Governance Institute, *IT Assurance Guide: Using COBIT*. United States of America, 2007.

[27] ITpreneurs Netherland B.V., Curso ITIL Foundation, 2013.

[28] OSIATIS S.A. ITIL ® - Gestión de Servicios. [Online]. http://itil.osiatis.es/Curso_ITIL/

[29] ISACA, *COBIT5 Process Reference Guide*., 2011.

[30] Ana María Benjumea Gil and Laura Sofía Rodríguez Pulecio, Metodología para el diseño y la gestión de Acuerdos de Niveles de Servicios (ANS) entre clientes de servicios de conectividad y sus proveedores, alineados con los objetivos estratégicos de la organización., 2012.

[31] Llumihuasi Quispe Juan Miguel, Auditoría de la gestión de tecnologías de la información en el gobierno municipal de San Miguel de Urcuquí utilizando como modelo de referncia Cobit 4.0, 2010.

[32] Enrique Andrés Larco Ampudia Christian Fabian Alcocer Castillo,

Acoplamiento de Cobit e Itil de empresas de vigilancia que tienen implementada la norma ISO 9001:2008, 2013.

[33] María Eugenia Regalado López, Propuesta de mejora del proceso de manejo de incidentes en una red de telecomunicaciones, basado en las mejores prácticas de ITIL. Caso aplicado a Telefónica Ecuador, 2009.

[34] Jim Clinch, ITIL V3 and Information Security, 2009.

[35] Chao Zhou Dong Zhang, Adoption of COBIT 5 and ITIL in Small and Medium Size Enterprises in China, 2014.

[36] (2010, Mayo) Innovación en el management desde la necesidad del cliente. [Online]. http://www.arpcalidad.com/definicin-de-proceso/

[37] Norberto Figuerola. (2012, Junio) Matriz de Asignación de Responsabilidades (RAM). [Online]. https://articulospm.files.wordpress.com/2012/07/matriz-de-asignacic3b3n-de-responsabilidades1.pdf

[38] Antonio Velasco Figallo. (2015) CLAVES PARA LA GESTIÓN DE RIESGOS. [Online]. http://docplayer.es/3542316-Claves-para-la-gestion-de-riesgos-antonio-velasco-figallo.html

[39] Área IP MPLS, CNT E.P., Procedimiento O&M, 2014.

[40] Centro de investigación de las Telecomunicaciones, ITIL MEJORES PRACTICAS, 2008.

[41] Maritza Yohana Ramírez Robayo, Edwin Alberto Londoño Rúa, and Jairo Andrés Gómez Gómez, Propuesta de mejoramiento y contingencia de sistemas informáticos en la empresa “T”, 2012.

[42] Verónica Quintuña Rodríguez, Auditoría informática a la Superintendencia de Telecomunicaciones, 2012.

[43] Felipe Donoso Jaurés Pía Ramírez Bravo, METODOLOGÍA ITIL, 2006.

ANEXOS

A. OPERACIÓN DEL SERVICIO

A.1 Formato de informe semanal de monitoreo

	INFORME SEMANAL DE EVENTOS DEL MONITOREO IP MPLS		
	Responsable:	Fecha:	Página Número:

Fecha	Hora	Significado Alarma	Tipo de Evento	Descripción	Repetición	Equipo Afectado	Acción Tomada

COMENTARIOS Y SUGERENCIAS:

	Nombre:	Fecha:	Firma:
Revisado y Aprobado por:			

A.2 Comandos pruebas primer nivel

Tipo	Comando	Argumento
Comados Generales	ping	
	telnet	
	ssh	
	exit	
	traceroute	
Comandos Cisco	switchport	trunk allowed vlan remove
		trunk allowed vlan add
		access vlan
	no	switchport trunk allowed vlan
		service-policy
		shutdown
		ip address
	port	nni
	terminal	
	attach	
	ip	helper-address
		access-group
		access-list
		domain
		domain-lookup
		host
		route vrf netdef
		address
		route vrf
		sla
		routing
	copy	
	dir	
	service-policy	
	shutdown	
	cdp	
	conform-action	*
	configure	terminal
	end	
	interface	
	class	
	police	cir
	write	
	route-target	

	address-family	ipv4 vrf
	autonomous-system	
	network	
	bridge-domain	
	default-information	originate
	do	
	flow control	
	icmp-echo	
	mtu	
	name	
	neighbor	
	police	
	redistribute	
	rewrite	
	snmp-server	
	speed	
	vlan	
	xconnect	
	load	interval
	channel	
	violate-action	
	exceed-action	
	banner	exec
		login
	clock	timezone
	ntp	server
	archive	log
	track	
	logging	enable
		size
	hidekeys	notify
	delay down	
Comandos Huawei	write	memory
	display	
	tracert	
	reset	
	undo	shutdown
		negotiation
		port
	lldp	
	system-view	
	negotiation	
	port	link-type trunk
		trunk allow-pass

		trunk permit vlan
		link-type access
		access vlan
	icmp	
	duplex	
	timeout	
	frequency	
	maximum	
Comandos Alcatel	show	startup-config
		running-config vrf
		running-config interface
		running-config community-set
		running-config class-map
		running-config bridge-domain
		running-config policy-map
		running-config vlan
		running-config partition
		running-config l2vpn
		running-config router bgp
		running-config router static vrf
		running-config router static
		ip multicast vrf *
	read-aaa	
	readwrite-telnet	
	readwrite-iproute	
	read-vlan	
	read-interfaces	
	read-*	
	readwrite-ssh	
	readwrite-	
	readwrite-802.1q	
	readwrite-conffile-mgmt	
	readwrite-chassis	
	readwrite-vlan	
	track	*
	delay down	*
	switchport	access vlan
	clear	Counters
	service	Instance
	no	service instase
Configuración EIGRP	router	Eigrp
		Static

A.3 Solicitud de accesos

FORMULARIO PARA EL INGRESO A EQUIPOS MPLS

1. Detalle de Ingreso:

Detalle	Nombre	
Nombre del Responsable/Jefe Inmediato:		
Nombre del área a la que pertenece/Proveedor:		
Motivo del ingreso (trabajos a realizarse):		
Fecha de acceso:	Activación :	Caducidad:
Número de contacto de Responsable :		
Dirección de correo electrónico:		

2. Identificación: (*Nombre(s) de la (s) persona (s) a ingresar:***)**

Nombre Completo	Usuario	Contraseña Temporal	Correo electrónico	Telefono

Las personas que ingresen a los equipos de la red IP/MPLS de la CNT EP, se comprometen a cumplir con los siguientes procedimientos:

En cuanto a los usuarios:

- *El usuario asignado es de uso personal e intransferible, queda bajo responsabilidad de la persona solicitante el mal uso del mismo.*
- *El solicitante estará en facultad de ejecutar las funcionalidades permitidas de acuerdo al perfil otorgado por el administrador de la herramienta y/o Jefe del Área IP/MPLS, la utilización de las funcionalidades queda bajo la responsabilidad del solicitante.*
- *Se tendrá como máximo 5 conexiones simultaneas*

En cuanto a las políticas de contraseña:

- *La contraseña asignada deberá ser obligatoriamente cambiada por el usuario luego del primer acceso.*
- *El contraseña no podrá contener el mismo nombre de usuario.*
- *Las cuentas serán deshabilitadas si se registran 3 intentos fallidos de conexión.*
- *Al cambiar el contraseña, éste no deberá ser el mismo anterior.*
- *El contraseña deberá ser cambiado máximo a los 60 días.*
- *El número máximo de conexiones por usuario es 5*

Solicitado por: ***Autorizado por:***

_____ _____

Nombre: *Nombre:*

A.4 RFC

RFC

Escribir el título del cambio a realizar
Escribir el número de OT en base a la cual se realiza la ventana de mantenimiento

Realizado por:
Revisado por:

CONTENIDO

1. ALCANCE .....
2. ANTECEDENTES .....
3. HORA Y FECHA DE EJECUCIÓN .....
4. TIEMPO TOTAL DE INDISPONIBILIDAD DEL SERVICIO:
5. IMPACTO .....
6. EQUIPOS INVOLUCRADOS (HW /SW) .....
7. RESUMEN DE ACTIVIDADES – DURACIÓN .....
8. MATRIZ DE PRUEBAS / VALIDACIONES .....
9. ROLLBACK .....
10. ASIGNACIÓN DE RECURSOS .....

1. ALCANCE

2. ANTECEDENTES

3. HORA Y FECHA DE EJECUCIÓN

4. TIEMPO TOTAL DE INDISPONIBILIDAD DEL SERVICIO:

5. IMPACTO

Se detallan los servicios afectados durante el mantenimiento en la Tabla:

Servicios Afectados			
Región	**Afectación De Trafico**	**Servicio**	**Observaciones**

6. EQUIPOS INVOLUCRADOS (HW /SW)

7. RESUMEN DE ACTIVIDADES – DURACIÓN

Nº	Actividad	Duración	Responsable	Impacto (Red - Sistema)
1				
2				
3				
4				

8. MATRIZ DE PRUEBAS / VALIDACIONES

Nº	Prueba de validación	Procedimiento		Responsable
		OK, continuar con la siguiente actividad	Caso contrario,	
		OK, continuar con la siguiente actividad	Caso contrario,	
		OK, continuar con la siguiente actividad	Caso contrario,	

9. ROLLBACK

10. ASIGNACIÓN DE RECURSOS

b) Responsables

Se detallan los nombres de las personas que intervendrán en el proceso, tanto de CNT como externos y la responsabilidad de cada uno.

Responsable CNT

Rol	Nombre	Número Teléfono	Responsabilidades

Responsable Proveedor

Proveedor						
Cargo	**Nombre**	**Nº teléfono**	**Responsabilidades**	**C.I.**	**Sitio de ingreso**	**Horario**

c) Requerimientos Generales

Nota:

De acuerdo al Procedimiento "**Comunicación al Cliente de Interrupción de Servicio**" se aprueba la ventana solicitada en base al RFC enviado por el área requirente

Aprobado por:

B. Mejora continua del servicio

B.1 Formato de Informe Mensual de Eventos

INFORME SEMANAL DE MONITOREO

Escribir la fecha de inicio y fin del monitoreo sobre el cual se realiza el informe

Realizado por:
Revisado por:

O&M IP MPLS

CONTENIDO

1. OBJETIVO GENERAL 3
2. DERECHOS DEL DOCUMENTO 3
3. ESTADÍSTICAS 3
   3.1 Número total de eventos 3
   3.2 Número de excepciones 3
   3.3 Número de advertencias 3
   3.4 Alarmas reincidentes 3
   3.5 Número de incidentes presentados sin la activación previa de una alarma 4
   3.6 Número de eventos provenientes de problemas con solución pendiente 4
4. COMENTARIOS Y SUGERENCIAS 4

1. OBJETIVO GENERAL

2. DERECHOS DEL DOCUMENTO

3. ESTADÍSTICAS

3.1. Número total de eventos

3.2. Número de excepciones

Alarma	Equipo Afectado/ Descripción	¿Se escaló? Si/No	Atendido por:	Acción Tomada
Total:				

3.3. Número de advertencias

Alarma	Acción Tomada
Total:	

3.4. Alarmas reincidentes

Alarma	Equipo Afectado/ Descripción	Repetición	Acción Tomada

Total:			

3.5. Número de incidentes presentados sin la activación previa de una alarma

Nº ticket	Equipo Afectado/ Descripción	Acción Tomada
Total:		

3.6. Número de eventos provenientes de problemas con solución pendiente

Alarma	Equipo Afectado/ Descripción	Identificador del problema
Total:		

4. COMENTARIOS Y SUGERENCIAS

B.2 Formato de informe mensual de incidentes

INFORME MENSUAL DE INCIDENTES

Realizado por:
Revisado por:

CONTENIDO

1. OBJETIVO GENERAL 3
2. DERECHOS DEL DOCUMENTO 3
3. ESTADÍSTICAS 3
3.1 Número total de incidentes 3
3.2 Tiempo promedio de resolución de incidentes dependiendo del impacto 3
3.3 Porcentaje de incidentes resueltos sin necesidad de escalamiento 3
3.4 Número y porcentaje de incidentes resueltos remotamente. 4
3.5 Número y porcentaje de incidentes escalados al proveedor. 4
3.6 Número y porcentaje de incidentes críticos. 4
3.7 Número y porcentaje de incidentes escalados incorrectamente. 4
3.8 Número y porcentaje de incidentes incorrectamente priorizados. 5
3.9 Número y porcentaje de incidentes que no fueron escalados ..... oportunamente. 5
3.10 Número y porcentaje de incidentes que fueron escalados a la gestión... de problemas. 5
4. COMENTARIOS Y SUGERENCIAS 5

1. OBJETIVO GENERAL

2. DERECHOS DEL DOCUMENTO

3. ESTADÍSTICAS

3.1. Número total de incidentes

Impacto	Número	Porcentaje
Alto		
Medio		
Bajo		
Total		

Número de Tickets Resueltos por el NOC:	
Número de Tickets Resueltos por el MPLS:	

3.2. Tiempo promedio de resolución de incidentes dependiendo del impacto

Impacto	Duración promedio
Alto	
Medio	
Bajo	

3.3. Porcentaje de incidentes resueltos sin necesidad de escalamiento

Número de incidentes resueltos sin escalamiento:	
Número de incidentes que requirieron escalamiento:	

3.4. Número y porcentaje de incidentes resueltos remotamente.

3.5. Número y porcentaje de incidentes escalados al proveedor.

Nº Ticket Escalado:	Descripción:	Solución:
Total:		

3.6. Número y porcentaje de incidentes críticos.

Nº Ticket Escalado:	Descripción:	Solución:
Total:		

3.7. Número y porcentaje de incidentes escalados incorrectamente.

Nº Ticket:	Descripción:	Acciones tomadas:	Motivo Error:
Total:			

3.8. Número y porcentaje de incidentes incorrectamente priorizados.

Nº Ticket :	Descripción:	Prioridad Corregida:
Total:		

3.9. Número y porcentaje de incidentes que no fueron escalados oportunamente.

Nº Ticket :	Descripción:	Prioridad	Causa de retraso:
Total:			

3.10. Número y porcentaje de incidentes que fueron escalados a gestión de problemas.

Nº Ticket :	Descripción:	Repetición:
Total:		

4. COMENTARIOS Y SUGERENCIAS

B.3 Formato de Informe Mensual de Problemas

INFORME MENSUAL DE GESTIÓN DE PROBLEMAS

Realizado por:
Revisado por:

O&M IP MPLS

CONTENIDO

1. OBJETIVO GENERAL 3
2. DERECHOS DEL DOCUMENTO 3
3. ESTADÍSTICAS 3
3.1 Número total de problemas 3
3.2 Número de incidentes escalados a la gestión de problemas 3
3.3 Tiempo promedio de resolución de problemas en base a la prioridad 3
3.4 Número de problemas que superan el tiempo máximo de resolución. 3
3.5 Número de mantenimientos preventivos 4
4. COMENTARIOS Y SUGERENCIAS 4

1. OBJETIVO GENERAL

2. DERECHOS DEL DOCUMENTO

3. ESTADÍSTICAS

3.1. Número total de problemas

Nº de problemas resueltos	Nº de problemas pendientes	Total

3.2. Número de incidentes escalados a la gestión de problemas

Nº ticket	Descripción	Solución

3.3. Tiempo promedio de resolución de problemas en base a la prioridad

Prioridad	Duración Promedio
Crítico	
Alto	
Medio	
Bajo	
Planeado	

3.4. Número de problemas que superan el tiempo máximo de resolución.

Identificador del Problema	Descripción	Tiempo de Solución
Total:		

3.5. Número de mantenimientos preventivos

Nº RFC	Descripción	Estado	Observaciones
Total:			

4. COMENTARIOS Y SUGERENCIAS

B.4 Formato de Informe Mensual de Consultas

INFORME MENSUAL DE GESTIÓN DE CONSULTAS

Realizado por:
Revisado por:

CONTENIDO

1. OBJETIVO GENERAL 3

2. DERECHOS DEL DOCUMENTO 3

3. ESTADÍSTICAS 3

3.1 Número total de consultas 3

3.2 Número de consultas rechazadas 3

3.3 Tiempo promedio de resolución de consultas 3

4. COMENTARIOS Y SUGERENCIAS 4

1. OBJETIVO GENERAL

2. DERECHOS DEL DOCUMENTO

3. ESTADÍSTICAS

3.1. Número total de consultas

Nº de consultas atendidas	Nº de consultas pendientes	Total

3.2. Número de consultas rechazadas

Consulta Rechazada	Justificación
Total:	

3.3. Tiempo promedio de resolución de consultas

Prioridad	Tiempo Promedio
Alta	
Media	
Baja	

4. COMENTARIOS Y SUGERENCIAS

B.5 Formato de Informe Mensual de Accesos

INFORME MENSUAL DE GESTIÓN DE ACCESOS

Realizado por:

Revisado por:

CONTENIDO

1. OBJETIVO GENERAL 3
2. DERECHOS DEL DOCUMENTO 3
3. ESTADÍSTICAS 3
3.1 Número de solicitudes recibidas 3
3.2 Número de solicitudes procesadas 3
3.3 Número de veces que se afectaron los servicios a causa de permisos de acceso incorrectos 3
3.4 Número de alertas por intentos fallidos de acceso a la red y las acciones que se han tomado para disminuir dichas alertas. 4
3.5 Tiempo promedio de cumplimiento de la solicitud de acceso 4
4. COMENTARIOS Y SUGERENCIAS 4

1. OBJETIVO GENERAL

2. DERECHOS DEL DOCUMENTO

3. ESTADÍSTICAS

3.1. Número de solicitudes recibidas

Nº de solicitud	Solicitante	Fecha	Descripción
Total:			

3.2. Número de solicitudes procesadas

Tipo de solicitud	**Número**
Número de solicitudes de acceso procesadas con éxito	
Número de solicitudes de cambio de configuración	
Número de solicitudes rechazadas	
Número de usuarios deshabilitados	

3.3. Número de veces que se afectaron los servicios a causa de permisos de acceso incorrectos

Nº de ticket	**Descripción**	**Acción Tomada**
Total:		

3.4. Número de alertas por intentos fallidos de acceso a la red y las acciones que se han tomado para disminuir dichas alertas.

Evento	Descripción	Acción Tomada
Total:		

3.5. Tiempo promedio de cumplimiento de la solicitud de acceso

Tipo de solicitud	Duración
Número de solicitudes de acceso procesadas con éxito	
Número de solicitudes de cambio de configuración	
Número de usuarios deshabilitados	
Tiempo Promedio:	

4. COMENTARIOS Y SUGERENCIAS

B.6 Formato de Informe Mensual de Cambios

INFORME MENSUAL DE GESTIÓN DE CAMBIOS

Realizado por:

Revisado por:

CONTENIDO

1. OBJETIVO GENERAL 3
2. DERECHOS DEL DOCUMENTO 3
3. ESTADÍSTICAS 3
3.1 Número total de cambios 3
3.2 Número de cambios rechazados 3
3.3 Número de cambios que requirieron rollback 3
3.4 Número de cambios que superaron el tiempo estipulado en el RFC 4
3.5 Número de cambios emergentes 4
4. COMENTARIOS Y SUGERENCIAS 4

1. OBJETIVO GENERAL

2. DERECHOS DEL DOCUMENTO

3. ESTADÍSTICAS

3.1. Número total de cambios

Nº de cambios implementados	Nº de cambios pendientes	Total

3.2. Número de cambios rechazados

Cambio Rechazado	Justificación
Total:	

3.3. Número de cambios que requirieron rollback

Rollback	Justificación	Observaciones
Total:		

3.4. Número de cambios que superaron el tiempo estipulado en el RFC

Nº RFC	Descripción	Justificación
Total:		

3.5. Número de cambios emergentes

Nº de ticket	Descripción	Cambio Realizado	Observaciones
Total:			

4. COMENTARIOS Y SUGERENCIAS