

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES



TEMA:

MODELO DE GESTIÓN FCAPS DE LA ISO PARA MEJORAR EL RENDIMIENTO,
DISPONIBILIDAD Y ADMINISTRACIÓN DE LA RED DE LA EMPRESA
OMEGATELCOM S.A

Trabajo de Grado previo a la obtención del título de Ingeniero en Telecomunicaciones.

AUTOR (A):

JHONATAN DANIEL JACOME CHIPANTASHI

DIRECTOR (A):

MSc. JARAMILLO VINUEZA EDGAR DANIEL

Ibarra, 2024



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1726569955		
APELLIDOS Y NOMBRES:	Jacome Chipantashi Jhonatan Daniel		
DIRECCIÓN:	Tabacundo – Bolívar y Rocafuerte		
EMAIL:	jdjacomec@utn.edu.ec		
TELÉFONO FIJO:	02 2365018	TELÉFONO MÓVIL:	0981196873

DATOS DE LA OBRA	
TÍTULO:	MODELO DE GESTIÓN FCAPS DE LA ISO PARA MEJORAR EL RENDIMIENTO, DISPONIBILIDAD Y ADMINISTRACIÓN DE LA RED DE LA EMPRESA OMEGATELCOM S. A
AUTOR (ES):	Jacome Chipantashi Jhonatan Daniel
FECHA DE APROBACIÓN: DD/MM/AAAA	16/06/2023
PROGRAMA:	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO
TITULO POR EL QUE OPTA:	Ingeniero en Telecomunicaciones
ASESOR /DIRECTOR:	MSc. Jaramillo Vinuesa Edgar Daniel

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 28 días del mes de febrero de 2024

EL AUTOR:



Jhonatan Daniel Jacome Chipantashi



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES
CERTIFICACIÓN

MAGISTER EDGAR DANIEL JARAMILLO VINUEZA, DIRECTOR DEL PRESENTA TRABAJO DE TITULACION CERTIFICA:

Que el presente trabajo de titulación **“MODELO DE GESTIÓN FCAPS DE LA ISO PARA MEJORAR EL RENDIMIENTO, DISPONIBILIDAD Y ADMINISTRACIÓN DE LA RED DE LA EMPRESA OMEGATELCOM S.A”** Fue desarrollado en su totalidad por el Sr. Jhonatan Daniel Jacome Chipantashi bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad

A handwritten signature in blue ink, which appears to read "E. Jaramillo", is written over a horizontal dashed line. The signature is enclosed within a large, hand-drawn blue oval.

ING. Jaramillo Vinueza Edgar Daniel

DIRECTOR DE TESIS



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Este trabajo de investigación es fruto del esfuerzo y la dedicación de mis Padres, el fundamento de mi fortaleza y el faro que ilumina mi camino. A ustedes, que me han inculcado valores, paciencia y amor incondicional. Este logro es el resultado de su sacrificio y dedicación. Gracias por ser mi constante inspiración y por enseñarme a perseverar incluso en los momentos más desafiantes.

A mi hermana, compañera de risas y amiga leal. Tu apoyo inquebrantable ha sido mi ancla en las tormentas académicas. Este logro igual lleva tu huella, y agradezco por cada palabra de aliento y cada sonrisa compartida en este viaje.

A Dios, fuente de fuerza y guía, le agradezco por iluminar mi camino académico. Este logro es un testimonio de su gracia constante.

A todos ustedes, mi familia, con gratitud infinita dedico este logro. Su amor y apoyo han sido mi motor, y esta tesis es un tributo a la unidad y fuerza que encontré en cada uno de ustedes.



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Ante todo, mi gratitud se dirige hacia mi familia, cuyo apoyo incondicional ha sido la fuerza motriz detrás de mi empeño académico. Sus palabras de inspiración, comprensión y amor fueron el sostén que me ha permitido superar desafíos y perseverar en este viaje educativo.

Quisiera expresar mi más sincera gratitud a mis docentes de la carrera de Telecomunicaciones y al ING. Edgar Jaramillo tutor de tesis, por su dedicación, tolerancia y guía especializada durante todo este procedimiento. Su conocimiento profundo y su compromiso jugaron un papel crucial en el desarrollo de esta tesis.

Por último, quiero reconocer y agradecer a la empresa OMEGATELCOM por permitirme acceder a sus servicios y recursos. La colaboración con su equipo no solo facilitó la investigación, sino que también enriqueció la perspectiva práctica de mi trabajo. La experiencia de trabajar con profesionales de renombre comprometidos en el campo ha sido invaluable para mi desarrollo profesional.

ÍNDICE DE CONTENIDOS

1.	CAPITULO I - INTRODUCCIÓN.....	18
1.1.	Problema.....	18
1.2.	Justificación.....	20
1.3.	Objetivos	22
1.3.1.	Objetivo General.....	22
1.3.2.	Objetivos Específicos.....	22
2.	CAPITULO II - MARCO TEÓRICO.....	23
2.1	Gestión de red.....	23
2.1.1	Historia de la Gestión de Red	23
2.1.2	Componentes de la gestión de red	24
2.1.2.1	Agentes	25
2.1.2.2	Gestores.....	26
2.1.2.3	Dispositivo Administrativo.....	26
2.1.3	Protocolos para la Gestión de red	27
2.1.3.1	SNMP.....	27
2.1.3.2	CMIP.....	30
2.1.3.3	NETCONF	30
2.1.3.4	Comparación entre los protocolos SNMP, CMIP y NETCONF	30
2.2	Rendimiento de la red	31

2.2.1 Ancho de banda.....	32
2.2.2 Latencia.....	32
2.2.3 Congestión	32
2.3 Disponibilidad de la red	33
2.3.1 Redundancia.....	33
2.3.2 Tolerancia	34
2.4 Modelo de gestión FCAPS de la ISO.....	34
2.4.1 Gestión	35
2.4.1.1 Gestión de Fallos (F).....	35
2.4.1.2 Gestión de Configuración (C).....	36
2.4.1.3 Gestión de Contabilidad (A).....	37
2.4.1.4 Gestión de Rendimiento (P).....	37
2.4.1.5 Gestión de Seguridad (S)	38
2.5 Programas de gestión de software libre.....	38
2.5.1 Zabbix	38
2.5.2 Nagios	39
2.5.3 LibreNMS	39
2.5.4 Diferencias entre las Herramientas de Gestión	40
2.6 Políticas de Gestión.....	41
3. CAPITULO III – SITUACIÓN ACTUAL DE LA EMPRESA.....	42

3.1 OMEGATELCOM S.A.....	42
3.2 Organigrama Estructural	43
3.2.1 El Departamento de Operaciones.....	44
3.2.2 El Departamento Comercial.....	44
3.2.3 El Departamento de Finanzas	44
3.2.4 El Departamento Administrativo	45
3.3 Infraestructura Tecnológica.....	45
3.4 Características Técnicas de los Dispositivos.....	47
3.5 Evaluación de la Gestión de las TI de OMEGATELCOM S.A.	50
3.5.1 Encuestas.....	50
3.5.2 Muestras	51
3.5.3 Análisis de Resultados Obtenidos.....	52
3.6 Definir y priorizar los problemas	57
3.7 Selección de la Herramienta de Gestión	59
4. CAPITULO IV – MODELO DE GESTIÓN FCAPS DE LA ISO.....	63
4.1 Fases de definición del modelo de gestión de OMEGATELCOM.....	63
4.2 Establecimiento de las políticas de gestión para OMEGATELCOM.....	65
4.2.1 Políticas para el manejo de Gestión de Fallos	68
4.2.1.1 Manejo para Fallos.....	69
4.2.1.2 Manejo para Incidentes	69

4.2.1.3 Documentación para Incidentes y Fallos	70
4.2.1.4 Mesa de Servicios	70
4.2.2 Políticas de la Gestión de Configuraciones	71
4.2.2.1 Ingreso de Dispositivos a la Red.....	71
4.2.2.2 Configuración de Dispositivos.....	71
4.2.3 Políticas de Gestión en Contabilidad	72
4.2.3.1 Inventario de Dispositivos de la red.....	72
4.2.4.2 Uso de los Servicios de Red.....	72
4.2.4 Políticas de Gestión de Rendimiento	73
4.2.4.1 Informe de rendimiento de Dispositivos.....	73
4.2.5 Políticas de Gestión de Seguridad.....	74
4.2.5.1 Acceso al Sistema de la Red	74
4.3 Levantamiento de Procesos de Gestión para OMEGATELCOM.....	74
4.3.1 Proceso para la Gestión en Fallos	76
4.3.1.1 Manejo para Fallos.....	76
4.3.1.2 Manejo para Incidentes	76
4.3.1.3 Documentación para Incidentes y Fallos	77
4.3.1.4 Mesa de Servicio.....	77
4.3.2 Proceso para la Gestión de Configuración.....	77
4.3.2.1 Ingreso de Dispositivos a la Red.....	77

4.3.2.2 Configuración de Dispositivos.....	77
4.3.3 Proceso para la Gestión de Contabilidad	78
4.3.3.1 Inventario de Dispositivos de la red.....	78
4.3.3.2 Uso de los Servicios de la Red.....	78
4.3.4 Proceso para la Gestión de Rendimiento	78
4.3.4.1 Informe de Rendimiento de Dispositivos	78
4.3.5 Proceso para la Gestión de Seguridad.....	79
4.3.5.1 Acceso al Sistema de Red.....	79
4.4 Análisis de Resultados	79
4.4.1 Optimización del Rendimiento, Disponibilidad y Administración en OMEGATELCOM	81
CONCLUSIONES	83
RECOMENDACIONES	84
GLOSARIO.....	86
Bibliografía	90
ANEXOS.....	93
Anexo 1: Formato de Encuestas.....	94
A. Encuesta dirigida al personal de la empresa OMEGATELCOM S.A.....	94
B. Encuesta dirigida a los usuarios de la empresa OMEGATELCOM S.A	96
Anexo 2: Manuales de las políticas de gestión para la empresa OMEGATELCOM ..	97

A.	Principios de las Políticas de Gestión de Red.....	97
B.	Compromiso por parte de las Autoridades	98
C.	Políticas para el Manejo para Fallos.....	99
D.	Políticas para el Manejo para Incidentes	100
E.	Políticas para la Documentación de Incidentes y Fallos	102
F.	Políticas para la Mesa de Servicio.....	104
G.	Políticas para Ingresar Dispositivos a la Red	105
H.	Políticas para la Configuración de Dispositivos.....	106
I.	Políticas para el Inventario de Dispositivos	107
J.	Políticas para el Uso de los Servicios de Red.....	108
K.	Políticas para el Informe de Rendimiento de Dispositivos.....	108
L.	Políticas para el Acceso al Sistema de Red	110

Anexo 3: Manuales de Procesos de Gestión para la empresa OMEGATELCOM S.A

112

A.	Proceso de Manejo para Fallos	112
B.	Proceso de Manejo para Incidentes	114
C.	Proceso de Documentación para de Incidentes y Fallos.....	117
D.	Proceso de Mesa de Servicio	119
E.	Ingreso de Dispositivos a la Red	121
F.	Configuración de los Dispositivos.....	123

G. Inventario de Dispositivos de la red 125

H. Uso de los Servicios de la Red 127

I. Informe de Rendimiento de Dispositivos 129

J. Acceso al Sistema de la Red..... 131

ANEXO 4. Rubrica de Evaluación para ingresar Equipos en la red de
OMEGATELCOM S.A..... 133

ANEXO 5. Parámetros para la Configuración de Equipos de OMEGATELCOM S.A.

ÍNDICE DE FIGURAS

<i>Figura 1 Elementos de la gestión de la red.....</i>	25
<i>Figura 2 Comunicación de los elementos de gestión</i>	27
<i>Figura 3 Árbol jerárquico MIBs.....</i>	29
<i>Figura 4 Áreas Funcionales.....</i>	35
<i>Figura 5 Ubicación del Nodo de la empresa OMEGATELCOM S.A.....</i>	42
<i>Figura 6 Estructura Empresarial de OMEGATELCOM</i>	43
<i>Figura 7 Topología Física de la empresa OMEGATELCOM S.A</i>	45
<i>Figura 8 Resultado de la encuesta en la Gestión de Fallas.....</i>	53
<i>Figura 9 Resultado de la encuesta en la Gestión de Configuración</i>	54
<i>Figura 10 Resultado de la encuesta en la Gestión de Contabilidad</i>	54
<i>Figura 11 Resultado de la encuesta en la Gestión de Rendimiento</i>	55
<i>Figura 12 Resultado de la encuesta en la Gestión de Seguridad.....</i>	56
<i>Figura 13 Resultado de la encuesta en la Calidad de servicio de los clientes</i>	56
<i>Figura 14 Resultado de la encuesta en la Resolución de problemas en los clientes</i>	57
<i>Figura 15 Fases de definición del modelo de gestión de la empresa OMEGATELCOM</i>	63
<i>Figura 16 Recomendación de estructura empresarial para OMEGATELCOM S.A.....</i>	75

ÍNDICE DE TABLAS

<i>Tabla 1</i> Comparación entre SNMP, CMIP y NETCONF.....	31
<i>Tabla 2</i> Diferencias entre Zabbix, Nagios y LibreNMS.....	40
<i>Tabla 3</i> Especificaciones de los equipos	47
<i>Tabla 4</i> Encuesta dirigida al personal de OMEGATELCOM.....	51
<i>Tabla 5</i> Encuesta dirigida a los clientes de OMEGATELCOM.....	51
<i>Tabla 6</i> Personal encuestado.....	52
<i>Tabla 7</i> Problema, Solución y Beneficio por obtener.....	80

RESUMEN

El presente trabajo se focaliza en el levantamiento e implementación de un Modelo de Gestión fundamentado en los principios del FCAPS de la ISO, con el propósito de optimizar el rendimiento, asegurar la disponibilidad y fortalecer la administración en la red de OMEGATELCOM S.A. La metodología aplicada es la de FCAPS en la cual abarcó el análisis de la situación actual hasta la definición y priorización de problemas, creación de políticas, desarrollo de procesos y adicional la recomendación de la herramienta de gestión Zabbix. Los resultados obtenidos revelan mejoras significativas en la eficiencia operativa, resolución más rápida de fallas y una mejor transparencia en la gestión de los recursos. Como conclusiones destacadas, se resalta la importancia del desarrollo de este modelo en entornos empresariales para optimizar sus operaciones de red. Las recomendaciones incluyen la continua actualización y adaptación de las políticas y procesos, así como la promoción de la formación constante del personal. Este estudio proporciona una fundamentación robusta para investigaciones futuras en el ámbito de la gestión de redes y telecomunicaciones

Palabras clave: Gestión de red, FCAPS, Rendimiento, Disponibilidad, Administración y OMEGATELCOM S.A.

ABSTRACT

The present research focuses on the development and implementation of a Management Model based on the FCAPS principles of ISO, aiming to optimize performance, ensure availability, and strengthen network management at OMEGATELCOM S.A. The applied methodology follows the FCAPS framework, encompassing analysis of the current situation, definition and prioritization of issues, policy creation, process development, and the additional recommendation of the Zabbix management tool. The results reveal significant improvements in operational efficiency, faster fault resolution, and increased transparency in resource management. Key conclusions emphasize the importance of implementing this model in business environments to optimize their network operations. Recommendations include continuous updating and adaptation of policies and processes, along with the promotion of ongoing staff training. This study establishes a firm groundwork for forthcoming research in the realm of network and telecommunications management.

Keywords: Network Management, FCAPS, Performance, Availability, Administration and OMEGATELCOM S.A.

1. CAPITULO I - INTRODUCCIÓN

En este capítulo se describen los fundamentos esenciales para la elaboración de la presente tesis, abordando aspectos como el problema, los objetivos y la justificación. Estos elementos influyen en la evolución del proyecto, buscando la creación de un modelo de gestión que satisfaga las exigencias de la empresa OMEGATELCOM S.A.

1.1. Problema

La optimización del rendimiento permite que una empresa de internet ofrezca una experiencia de usuario rápida y eficiente. Esto es fundamental ya que los usuarios de internet tienen expectativas cada vez mayores en términos de velocidad de respuesta de páginas web y en los tiempos de carga de aplicaciones. Según estudios realizados por Google (2018), reveló que el 53% de los visitantes optan por abandonar un sitio web si su carga supera los tres segundos.

La disponibilidad de la red es esencial para garantizar que los servicios y aplicaciones en línea estén siempre accesibles para los usuarios. Un tiempo de inactividad prolongado o frecuente puede acarrear resultados adversos para una empresa, como la pérdida de ingresos, daño a la reputación de la marca y pérdida de clientes. Según Gartner (2020), el costo promedio de un tiempo de inactividad no planificado es de aproximadamente \$5,600 por minuto.

Actualmente la empresa de telecomunicaciones OMEGATELCOM S.A ofrece el servicio de internet a sus clientes. La infraestructura de red de la empresa desempeña un papel crucial en la entrega de este servicio, pero según el área de soporte técnico informático en los últimos meses ha experimentado problemas frecuentes de rendimiento y disponibilidad, vinculado a la pérdida de conexión, infecciones por virus, complicaciones asociadas al cableado estructurado, deficiencias en la supervisión de la red de datos y la ausencia de políticas para la gestión de fallos.

Esto ha llevado a una disminución en la satisfacción del cliente y ha afectado la reputación de la empresa lo cual afecta directamente a su economía.

El principal problema que tiene OMEGATELCOM S.A, es la ausencia de un modelo de gestión de red eficiente y estandarizado. Actualmente, la empresa no cuenta con un plan estructurado para monitorear, administrar y solucionar problemas en su red. Esto ha dado lugar a una falta de visibilidad y control sobre la eficacia de la red, lo que dificulta el reconocimiento y pronta solución de problemas. Además, la empresa no cuenta con una estrategia clara de mantenimiento preventivo y capacidad para anticipar posibles cortes del servicio. Esto genera tiempos de inactividad no planificados y una respuesta lenta en la resolución de problemas, lo cual afecta la disponibilidad de la red.

Es por ello la importancia de desarrollar un modelo de gestión FCAPS de la ISO para la empresa el cual permitirá optimizar la calidad del servicio de internet al identificar y resolver problemas de disponibilidad y rendimiento de la red, así como la satisfacción del cliente al proporcionar una conexión estable y confiable; y sobre todo una ventaja competitiva al optimizar la disponibilidad y rendimiento de la red.

1.2. Justificación

En el entorno empresarial actual, la red de comunicaciones se convirtió en una infraestructura crítica para las organizaciones. La empresa OMEGATELCOM S.A, como proveedor de servicios de telecomunicaciones, se enfrenta a desafíos constantes para asegurar un rendimiento ideal y una disponibilidad ininterrumpida de su red. En la Ley Orgánica de las Telecomunicaciones Art. 22 según Del Pozo (2015), “Los suscriptores, clientes y usuarios de servicios de telecomunicaciones tendrán el derecho de recibir de manera constante, regular, eficiente, con calidad y eficacia los servicios de telecomunicaciones que han contratado”. En este contexto, el modelo de gestión FCAPS (Fault, Configuration, Accounting, Performance, and Security) de la ISO ofrece un enfoque integral y estructurado que puede ayudar a OMEGATELCOM S.A a mejorar su rendimiento y disponibilidad de red, esto permite optimizar la satisfacción del cliente y la reputación de la organización.

En primer lugar, el modelo FCAPS se enfoca en identificar y solucionar fallas. Según Peterson (2017), "Las empresas que implementan un enfoque proactivo para la gestión de fallas, como el modelo FCAPS, experimentan una reducción significativa en el tiempo de inactividad de la red y un incremento en la capacidad de respuesta ante problemas". Esto permitirá a la empresa pueda identificar y resolver problemas rápidamente, minimizando así el tiempo de inactividad y mejorando la calidad del servicio que brinda a sus clientes.

Además, la gestión de la configuración es otro aspecto clave abordado por el modelo FCAPS. Varios estudios demostraron que el manejo de la configuración de la red mediante un enfoque basado en FCAPS de la ISO permite a las organizaciones como OMEGATELCOM S.A mantener una infraestructura coherente y bien documentada, lo que a su vez facilita la respuesta de problemas y la ejecución de cambios de manera más eficiente (Morris, 2018).

En cuanto al rendimiento de la red, el modelo FCAPS proporciona un marco para supervisar y optimizar el desempeño. La aplicación de políticas de rendimiento y el monitoreo constante son aspectos cruciales para optimizar la calidad del servicio en las redes empresariales. El modelo FCAPS de la ISO ofrece directrices claras para el seguimiento y la optimización del rendimiento de la red (Johnson, 2019). Al poseer una visibilidad clara del desempeño de la red, la empresa puede analizar cuellos de botella, optimizar la configuración y garantizar un rendimiento óptimo para los usuarios finales.

Por último, la seguridad de la red aplicando modelos de gestión FCAPS es muy importante para una empresa de internet. En un entorno digital en constante evolución y con el aumento en la complejidad de las amenazas cibernéticas, contar con una red segura se vuelve muy importante para resguardar la información confidencial de la empresa, salvaguardar la información de los clientes y garantizar la continuidad de los servicios.

Es así como, la empresa OMEGATELCOM con la implementación del modelo de gestión FCAPS permitirá a los administradores de la red solucionar los problemas de una manera más eficiente, y los usuarios obtendrán una satisfacción al mejorar la calidad del servicio y la eficiencia operativa.

1.3. Objetivos

1.3.1. Objetivo General

Realizar un modelo de gestión de red y servicios de telecomunicaciones para la empresa OMEGATELCOM, basado en el Modelo de Gestión FCAPS de la ISO para mejorar el rendimiento, disponibilidad y administración.

1.3.2. Objetivos Específicos

- Analizar el Framework del Modelo de Gestión FCAPS de la ISO para poder aplicar y adecuar a las necesidades de la red de la empresa OMEGATELCOM.
- Determinar el estado de la red mediante la recopilación de información sobre la situación actual y las necesidades de la red de la empresa, a través de herramientas de recolección de datos.
- Desarrollar un modelo de gestión basado en el Modelo de Gestión FCAPS de la ISO el cual permita planificar, mantener y gestionar la red de la empresa y sus servicios.

2. CAPITULO II - MARCO TEÓRICO

En esta sección se exponen los principios fundamentales del modelo de gestión de red FCAPS de la ISO y protocolos de red asociados en el programa de recomendación para aplicar dicho modelo de gestión. Estos elementos constituirán la base para elaborar manuales de procesos y establecer políticas de gestión, fundamentales para respaldar el desarrollo del presente trabajo.

2.1 Gestión de red

La administración de la red comprende una variedad de actividades y procesos asociados con la administración, control y supervisión de una red de computadoras. Estas tareas incluyen la configuración, supervisión, diagnóstico y resolución de inconvenientes en la red, con el objetivo de garantizar su rendimiento, seguridad y disponibilidad (Tanenbaum, 2011).

El propósito de la gestión de redes es garantizar el buen funcionamiento, seguro y fiable de las redes informáticas. Además, garantiza la disponibilidad continua de la red, optimiza el rendimiento para una comunicación rápida, implementa precauciones de seguridad para resguardarla la red de amenazas, administra de manera efectiva los recursos de la red y corrige rápidamente posibles problemas o errores. Así garantiza que la red cumple atendiendo a las necesidades de comunicación de los usuarios, al mismo tiempo que se mejora el rendimiento y se reduce al mínimo el mal funcionamiento.

2.1.1 Historia de la Gestión de Red

En las décadas de 1960 y 1970 se presentaron las bases para la gestión de redes (Stallings, 2013). En los primeros años, el enfoque principal estaba en la administración de sistemas individuales y el monitoreo manual de recursos de red. Pero gradualmente las redes se expandieron y se interconectaron más, se tuvo la necesidad de una gestión ordenada y automatizada.

La década de 1980 se introduce los primeros protocolos de gestión de redes, como el Protocolo Simple de Administración de Redes (SNMP, por sus siglas en inglés). (Stallings, 2013). SNMP se convirtió en un estándar ampliamente utilizado para monitorear y gestionar redes. Además, en esta época se desarrollaron las primeras herramientas de la gestión de la red, como los sistemas de monitoreo en rendimiento y las herramientas de detección de fallas.

En la década de 1990 y principios de 2000, la gestión de redes se volvió más compleja con la aparición de redes empresariales y la introducción de tecnologías como Internet (Kurose, 2017). Se introducen nuevos estándares y protocolos, utilizando elementos como la Base de Información de Administración (MIB) y la Monitorización Remota (RMON), con el objetivo de optimizar la administración de las redes.

En la actualidad, la administración de redes ha adquirido mayor complejidad debido al incremento en el tamaño de las redes, la diversificación de dispositivos conectados y la creciente exigencia de servicios de red (Tanenbaum, 2011). La administración de redes se ha convertido en un ámbito multidisciplinario que incluye aspectos como la seguridad de la red, la gestión del rendimiento, la detección de fallos, la contabilidad y las prestaciones.

2.1.2 Componentes de la gestión de red

En la gestión de las redes existen varios elementos fundamentales que aseguran un funcionamiento eficiente y confiable. Entre los elementos más importantes son los agentes, gestores y un dispositivo administrativo.

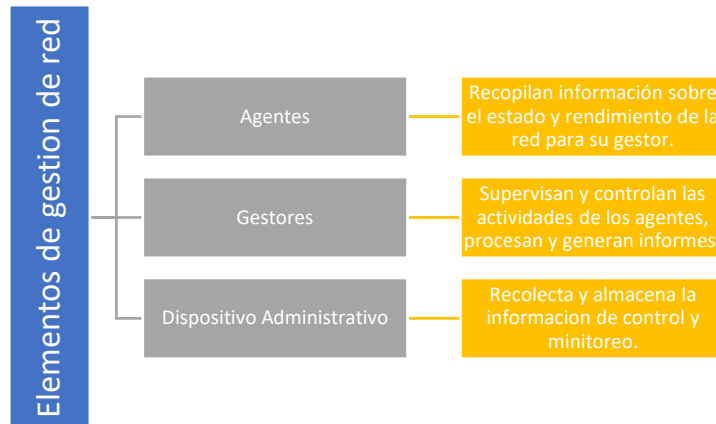
Un agente es un componente de software o hardware ubicado en un dispositivo de red que recopila y transmite información sobre el estado de la red.

Los gestores son aplicaciones que monitorean y controlan a los agentes, toman decisiones y hacen los ajustes necesarios.

Y el dispositivo administrativo el cual actúa como un centro de comando, proporcionando una interfaz centralizada para configurar, monitorear y administrar toda la red. Estos elementos trabajan juntos para garantizar una gestión de red eficiente y eficaz.

Figura 1

Elementos de la gestión de la red.



Fuente: Autoría

Iniciando de la Figura 1 a continuación, se describe algunos elementos de la gestión de red.

2.1.2.1 Agentes

En la gestión de redes, un agente hace referencia a un componente de software que está ubicado en un dispositivo de red y es responsable de recopilar y transmitir datos acerca del estado, y el rendimiento de la red. Estos agentes actúan como intermediarios entre los dispositivos de red y los administradores, brindando datos relevantes para la supervisión de la red (Stallings, 2013).

Los agentes poseen datos de información de administración llamados MIB, los cuales son convertidos a un formato congruente según el protocolo de administración del sistema (Windows, Linux o macOS) y es organizada en jerarquías. En entornos Windows, las estaciones de trabajo

cuentan con versiones cliente del servicio SNMP, también conocido como Protocolo de Administración Sencilla de Red Cliente.

2.1.2.2 Gestores

Un gestor es una aplicación o software que controla y supervisa las acciones de los agentes en una red. Estas aplicaciones reciben los datos recopilados por los agentes, la procesan, realizan análisis y generan informes. Además, los administradores pueden tomar decisiones y realizar acciones para optimizar el rendimiento, solucionar problemas y configurar dispositivos de red (Stallings, 2013).

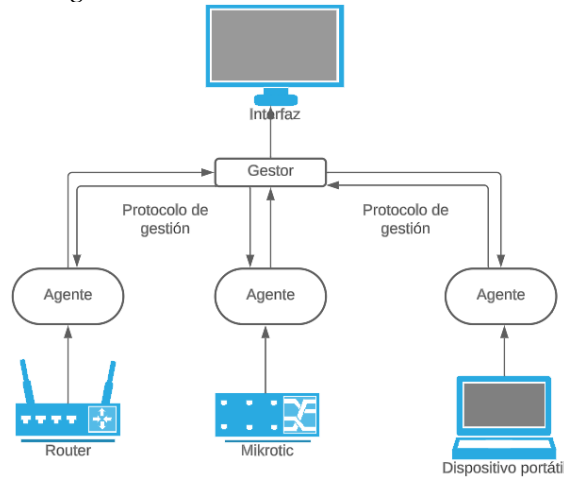
Los gestores proporcionan un grupo de recursos y memoria necesarios para la administración de la red. En cualquier red que este gestionada, puede haber uno o varios gestores.

2.1.2.3 Dispositivo Administrativo

Un dispositivo administrativo se refiere a cualquier dispositivo conectado a una red que contenga un agente SNMP. Puede ser una computadora, un servidor, switches, bridges, hubs u otros dispositivos de red.

Estos son capaces de enviar, recibir, procesar o transmitir datos en la red. Puede tener una dirección única en la red, como una IP, que puede ser identificada de manera única en el entorno de una red.

Figura 2
Comunicación de los elementos de gestión



Fuente: Autoría

En la figura 2 se observa los dispositivos administrados (Router, Mikrotic y portátil) los cuales están monitoreados por un agente el cual se está retroalimentado de las peticiones del gestor el cual posee una interfaz.

2.1.3 Protocolos para la Gestión de red

Son un conjunto de procedimientos y reglas que actúan como mediador para supervisar y controlar dispositivos y redes de manera efectiva. Estos protocolos permiten la comunicación entre los administradores de red y los agentes, lo que facilita la recopilación de datos, la supervisión del rendimiento, la configuración de dispositivos y la resolución de problemas. A continuación, se analiza los protocolos CMIP, Netconf y SNMP.

2.1.3.1 SNMP

SNMP es ampliamente empleado para gestionar y monitorear dispositivos en la red. Proporciona un mecanismo simple y eficiente para recopilar información de administración, configurar y administrar de forma remota los dispositivos. SNMP se fundamenta en una arquitectura cliente-servidor, en la cual los dispositivos gestionados funcionan como servidores

que pueden recibir instrucciones y ser controlados por un dispositivo central de gestión que opera como cliente (Fedor, Schoffstall, Davin, & Case, 1990).

Funcionamiento

SNMP utiliza un protocolo de transporte, como UDP (User Datagram Protocol), para enviar y recibir mensajes entre los agentes y los gestores. Las comunicaciones entre los agentes y los gestores se basan en intercambios de mensajes, donde los gestores envían solicitudes y los agentes responden con respuestas (Fedor, Schoffstall, Davin, & Case, 1990).

SNMP define mensajes o un conjunto de operaciones que los gestores pueden utilizar para interactuar con los agentes. Estas operaciones incluyen:

- **GetRequest:** Una solicitud para obtener el valor de una o varias variables administradas del agente.
- **GetNextRequest:** Una solicitud para obtener el siguiente valor en la secuencia de variables administradas del agente.
- **SetRequest:** Una solicitud para establecer el valor de una o varias variables administradas en el agente.
- **GetResponse:** Una respuesta del agente que contiene el valor solicitado por el gestor.
- **Trap:** Una notificación enviada por el agente al gestor para informar sobre un evento importante que ha ocurrido.

Bases de información de gestión (MIBs)

Las MIBs son una base de información de gestión que utiliza SNMP para describir y organizar los objetos gestionados en un sistema, y define una jerarquía de objetos que representan variables administradas dentro de un dispositivo o sistema. Los objetos administrados por MIB están representados por identificadores únicos conocidos como identificadores de objeto (OID) en

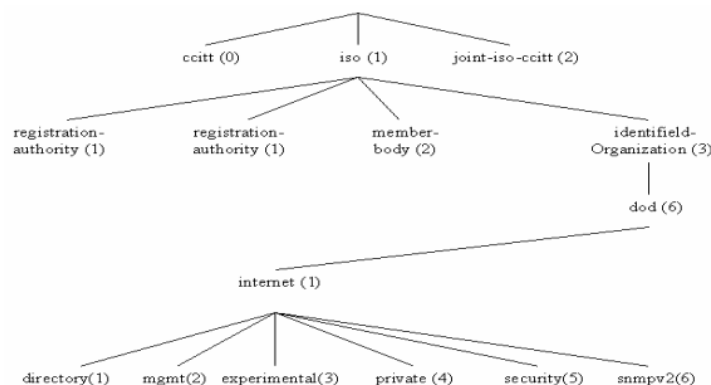
donde cada entidad gestionada tiene un OID único que la identifica en la MIB (Cloghrie & Rose, 1991).

Las MIB están organizadas como una estructura de árbol donde los nodos del árbol representan objetos administrados y sus nodos secundarios representan variables o instancias más específicas de esos objetos. Los nodos superiores del árbol, llamados nodos raíz, definen las categorías comunes de objetos administrados, mientras que los nodos inferiores representan variables y sus instancias individuales (Cloghrie & Rose, 1991).

Cada objeto administrado en la MIB tiene un nombre único y está asociado con un tipo de datos específico que define la información que contiene. Los tipos de datos pueden incluir números enteros, cadenas, direcciones IP, etc.

Figura 3

Árbol jerárquico MIBs.



Nota. La identificación del MIB correspondiente a la gestión de Internet puede expresarse como .iso.org.dod.internet.mgmt, o de manera numérica como .1.3.6.1.2. Adaptado de Rose, M. T., & McCloghrie, K. (14 de Julio de 2023). MIBs. Obtenido de Cinvestav.mx.: <https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf>

Identificación de objeto (OID)

Los OIDs se utilizan para identificar y referenciar de manera única los objetos administrados en una MIB. Cada objeto tiene un OID asociado que lo distingue de otros objetos

en la misma MIB y en la gestión de redes en general. Los gestores SNMP utilizan los OIDs para solicitar información específica de los agentes SNMP y controlar los dispositivos de red.

2.1.3.2 CMIP

Es un protocolo de gestión de redes definido por ISO (International Organization for Standardization) y CCITT proporciona un marco completo para la gestión de redes, permitiendo a los sistemas de gestión supervisar y controlar dispositivos de red mediante la recopilación de información. CMIP puede trabajar con TCP/IP es sofisticado e involucra comandos complejos, es más versátil, pero no tan común en el mundo de la administración de red (Manolo, 2005).

2.1.3.3 NETCONF

Es un protocolo también de gestión de red simple para administrar un dispositivo en la red, a través del cual se puede extraer información de datos de ajustes y se pueden manipular nuevos datos, además este protocolo ofrece a los dispositivos una interfaz de programación (API) completa, la cual utiliza para recibir y enviar datos de configuración completos (Enns, Björklund, Bierman, & Schönwälder, 2011).

NETCONF utiliza RPC y XML para intercambiar información. En donde RPC crea una conexión entre cliente y servidor, XML establece el formato de los datos compartidos y la envía a un servidor utilizando una sesión segura como lo es SSH (Enns, Björklund, Bierman, & Schönwälder, 2011).

2.1.3.4 Comparación entre los protocolos SNMP, CMIP y NETCONF

En este cuadro comparativo destaca algunas de las características clave de los protocolos SNMP, CMIP y NETCONF empleados en la gestión de las redes.

Tabla 1*Comparación entre SNMP, CMIP y NETCONF*

Características	SNMP (Simple Network Management Protocol)	CMIP (Common Management Information Protocol)	NETCONF (Network Configuration Protocol)
Tipo de Protocolo	Ligero, basado en UDP	Pesado, basado en OSI	Ligero, basado en XML y SSH/HTTPS
Arquitectura de Red	Cliente-Servidor	Cliente-Servidor	Cliente-Servidor
Modelo de Datos	Jerárquico, basado en MIB	Jerárquico, basado en ASN.1	Jerárquico, basado en YANG
Seguridad	SNMPv3 incluye características de seguridad como cifrado y autenticación	Puede ser complejo de implementar, dependerá de las extensiones específicas	Incluye funciones de autenticación y autorización, puede usar SSH/HTTPS para seguridad de transporte
Transporte de Datos	UDP	TP4 (Transport Protocol Class 4) de OSI	SSH/HTTPS
Sintaxis de Datos	Protocol Data Units (PDUs) con estructuras de datos simples	ASN.1 definido en BER (Basic Encoding Rules)	XML para datos de configuración y operaciones
Eficiencia de Red	Menos eficiente en términos de ancho de banda	Puede ser más eficiente que SNMP, pero más complejo	Eficiente debido al uso de XML y la capacidad de enviar solo cambios de configuración
Flexibilidad y Extensibilidad	Menos flexible en comparación con CMIP y NETCONF	Puede ser extenso y flexible, pero a costa de complejidad	Altamente flexible y extensible debido a YANG y XML
Uso Principal	Ampliamente utilizado para supervisión y gestión de red	Menos común en comparación con SNMP	Enfoque en la configuración y gestión de dispositivos de red
Estandarización	Estándares SNMP definidos por la IETF	Estándares CMIP definidos por la ITU-T	NETCONF estandarizado por la IETF

Fuente: Autoría

2.2 Rendimiento de la red

El rendimiento de una red se fundamenta en el análisis de las estadísticas de toda una red de una empresa, el cual determina la excelencia del servicio proporcionado por la red.

Es un proceso cualitativo y cuantitativo utilizado para medir y determinar el nivel de rendimiento de una red específica y ayuda a los administradores a la revisión y mejora de los servicios que ofrecen. El rendimiento de una red principalmente se determina mediante las estadísticas y métricas obtenidas en el equipo terminal de los usuarios finales, dichas métricas son por ejemplo latencia, congestión y ancho de banda.

2.2.1 Ancho de banda

Es un tipo de medida que se utiliza para representar la cantidad de recursos para un canal de transmisión. En el contexto del servicio de Internet, el ancho de banda se refiere a la cantidad de datos que puede ser transmitida a través de una conexión de red en un período específico, esta medida se muestra por lo general en bites por segundo, kilobites por segundo, o megabites por segundo, los cuales pueden ser transmitidos a través de cables de par trenzado, fibra óptica o mediante el aire (Suarez-Tapia, Carvajal-Gómez, & Carreto-Arellano, 2015).

2.2.2 Latencia

Se define como el retraso experimentado durante la comunicación en una red. Este término representa el tiempo requerido para que la información se transfiera por medio de dicha red. Una red con mayor demora se caracteriza por tener una latencia alta, en cambio aquellas que proporcionan respuestas rápidas exhiben una latencia baja. En el ámbito empresarial, la búsqueda de una latencia reducida y una comunicación de red más veloz se traduce en un aumento de la eficiencia y en actividades mucho más productivas. (AWS, 2023).

2.2.3 Congestión

La congestión en una red ocurre cuando hay una acumulación excesiva de datos en los buffers, en espera de ser entregados. Esta situación incrementa los tiempos de viaje de los paquetes y retrasa la comunicación entre las personas (Barreto & Patrón, 2008).

Actualmente, el crece la transmisión de archivos grandes, imágenes y videos, así como el incremento de personas en la red, genera una mayor solicitud de ancho de banda. La congestión de red ocurre cuando hay un número creciente de personas compartiendo archivos, accediendo a servidores y utilizando Internet (Barreto & Patrón, 2008).

Esto conduce a tiempos de respuesta más lentos, así como a transferencias de archivos más prolongadas y menor productividad debido a los retrasos en la red.

2.3 Disponibilidad de la red

Según la UIT-T X.137, se refiere a la medida de la capacidad de una red para estar operativa y funcionando correctamente durante un determinado período de tiempo. Este es un indicador de la confiabilidad y la capacidad de una red para proporcionar servicios de manera continua, sin interrupciones significativas.

La disponibilidad de red se expresa generalmente como un porcentaje, que representa el tiempo en el que la red está en funcionamiento en relación con el tiempo total considerado. Por ejemplo, una disponibilidad del 99% significa que la red está operativa el 99% del tiempo y solo experimenta un tiempo de inactividad del 1%.

En el caso de las redes públicas de datos que brindan servicios internacionales de conmutación de paquetes, la UIT-T X.137 establece principios de disponibilidad específicos que deben cumplir. Estos valores pueden variar dependiendo del nivel de servicio y la importancia estratégica de la red en cuestión. En este sentido la disponibilidad de una red está relacionada con la redundancia y la tolerancia a fallos.

2.3.1 Redundancia

La redundancia se refiere a la duplicación o multiplicación de componentes críticos de una red para mejorar la fiabilidad del sistema. Según Tanenbaum y Wetherall (2011), la redundancia

es "el uso de componentes adicionales que son fundamentales para el correcto funcionamiento del sistema, pero que están disponibles para su uso en caso de fallar uno de los componentes principales" (p. 480). Es decir que la implementación de redundancia implica contar con duplicados de componentes, como enlaces de red, switches, routers o servidores. Esta duplicación permite que, en caso de fallo de un componente, el sistema pueda cambiar automáticamente al componente redundante sin experimentar una interrupción significativa en el servicio

2.3.2 Tolerancia

Según Stallings (2013), la tolerancia es "la habilidad de un sistema para proporcionar su servicio esencial a pesar de que algunos de sus componentes hayan fallado" (p. 524). Es decir, la tolerancia es la capacidad de un sistema o red para soportar y restablecerse de falla o interrupciones sin experimentar una degradación significativa en su correcto funcionamiento.

La tolerancia es la implementación de mecanismos que permiten al sistema detectar, aislar y recuperarse de los fallos de forma automática o con mínima intervención del usuario. Estas técnicas incluyen la redundancia, la detección de fallos, la conmutación por error, la recuperación automática y otras herramientas diseñadas para minimizar el impacto de las fallas en el correcto funcionamiento de un sistema.

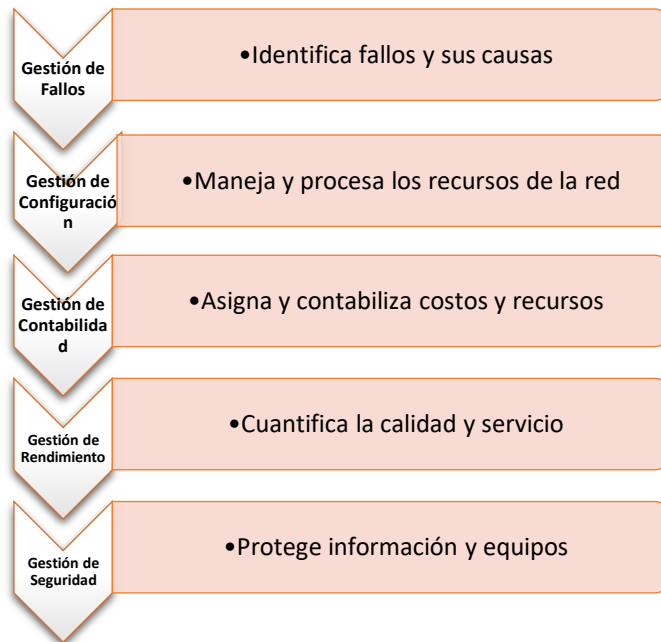
2.4 Modelo de gestión FCAPS de la ISO

El modelo FCAPS fue introducida por la ITU-T en 1988 con el propósito de estandarizar y proporcionar una guía para la administración de redes de telecomunicaciones en todo el planeta. El propósito principal de la ITU era establecer un conjunto de funciones que aborden aspectos críticos en la administración de redes, lo que permitiría una gestión más eficiente en las redes de telecomunicaciones (ITU-T, 1993) . Desde entonces, el modelo de gestión FCAPS se ha empleado extensamente en las industrias de telecomunicaciones y ha sido una referencia fundamental para

la administración de redes. Este modelo se divide en 5 áreas funcionales como se observa en la figura 4.

Figura 4

Áreas Funcionales



Fuente: Autoría

Las cinco áreas funcionales nos ayudan a tener una mejor organización ante cualquier problema que presenta cualquier empresa de telecomunicaciones.

A continuación, se describe las áreas funcionales mencionadas en el gráfico anterior.

2.4.1 Gestión

2.4.1.1 Gestión de Fallos (F)

La gestión de fallas se refiere al proceso de supervisar, detectar, informar, aislar, resolver y registrar los problemas o fallas en una red de telecomunicaciones. Esto tiene como objetivo

mantener la disponibilidad del servicio al garantizar que los problemas sean identificados y resueltos de manera eficiente (Hermosa Torres, 2015).

El procedimiento de manejo de fallas en el modelo FCAPS se puede establecer lo siguiente:

- Detección de fallas: Supervisar y detectar problemas en la red.
- Notificación y registro: Generar alertas y documentar detalles de la falla.
- Aislamiento y diagnóstico: Identificar la causa y ubicación de la falla.
- Resolución y restauración: Tomar medidas para corregir la falla y restaurar el servicio.
- Documentación y análisis: Registrar acciones y analizar la causa raíz.
- Comunicación: Informar a los equipos de soporte y si es necesario a niveles superiores.

2.4.1.2 Gestión de Configuración (C)

Es un procedimiento fundamental que implica la recaudación de la información de la red, para gestionar de manera efectiva la incorporación, mantenimiento y configuración de los componentes de la red, basados en políticas y procesos de configuración. Todos los cambios que se realicen en software y hardware son establecidos por medio de esta área (Hermosa Torres, 2015).

Los objetivos de la gestión de configuración son:

- Recaudar información
- Ajustar la configuración
- Generar de reportes
- Almacenar los cambios

Así este proceso garantiza coherencia, seguridad y eficiencia en la configuración de la red, contribuyendo así a una gestión exitosa de los componentes de la red y a un buen funcionamiento.

2.4.1.3 Gestión de Contabilidad (A)

En la Gestión de Contabilidad se centra en el registro de la utilización de los recursos proporcionados por la red a sus abonados. En las funciones de esta área tenemos la recopilación de información acerca del uso de los recursos, mantenimiento de cuentas de usuario, lo cual nos permita la creación de estadísticas de uso para la formulación de informes de tarificación (Pérez, 2019).

El proceso es el siguiente:

- Recopilación de datos
- Configuración de cuentas: Definir cuentas y categorías de contabilidad según los recursos utilizados por los clientes.
- Registro de eventos y datos: Implementar un sistema de registro de eventos (tráfico de red, planes de servicio y facturación).
- Procesamiento de datos: Calcular los costos y generar registros financieros.
- Facturación a clientes: Generar facturas precisas para los clientes.
- Generación de informes financieros: Crear informes regulares sobre ingresos y gastos.

2.4.1.4 Gestión de Rendimiento (P)

Garantiza que la red funcione de manera adecuada mediante la aplicación de estándares que evalúan el nivel y la calidad del servicio. Además, realiza una supervisión continua de la red con el propósito de prevenir congestiones, establece los parámetros que definen la calidad del servicio y recopila y analiza los datos obtenidos, como el tráfico, el cual genera los informes necesarios (Molero, 2010).

Algunas de las funciones de la gestión de rendimiento son:

- Registra los datos que nos indiquen el desempeño de la red.

- Examinar los datos de desempeño para identificar niveles normales de desempeño.
- Instaurar alarmas de problemas en el desempeño de la red.
- Generar reportes de desempeño.

2.4.1.5 Gestión de Seguridad (S)

El propósito es dar herramientas que simplifiquen la aplicación de políticas y servicios de seguridad tanto a los elementos individuales de la red o a toda la red en general. Esto implica la formulación de estrategias destinadas a prevenir y detectar ataques, además de responder a incidentes de seguridad de manera rápida y efectiva (Torres Chicaiza, 2015).

Algunas de las tareas de la gestión de seguridad son:

- Analizar la red frente ataques.
- Prevención de medidas de seguridad.
- Control de acceso a los recursos.
- Respuestas a incidentes.

2.5 Programas de gestión de software libre

En este proyecto se ha optado por emplear una herramienta de gestión de redes de código abierto, como Nagios, Zabbix o Libre NMS, en lugar de recurrir a soluciones de gestión pagadas. Estas herramientas cumplen con la eficiencia y la economía, permitiendo aprovechar al máximo las ventajas de estas plataformas de software libre para supervisar y administrar la infraestructura sin incurrir en gastos adicionales.

2.5.1 Zabbix

Zabbix es un sistema de monitorización de código abierto y libre, creado con el propósito de supervisar y registrar el estado de diversos servicios de red, servidores y hardware de red. Utiliza MySQL, SQLite, Oracle o IBM como sistema de gestión de bases de datos. Zabbix utiliza una

arquitectura cliente-servidor y es altamente personalizable, lo que permite a los administradores de sistemas adaptar la monitorización a las necesidades específicas de su infraestructura. (Zabbix, 2023).

2.5.2 Nagios

Nagios es una plataforma de monitorización de sistemas y redes que fue lanzada por primera vez en 1999. Su propósito principal es monitorear toda la infraestructura de tecnología de la información (TI) de una organización para garantizar que los sistemas, aplicaciones, servicios y procesos comerciales funcionen de manera correcta (Nagios, 2020).

Cuando se produce una falla o un problema en cualquiera de estos componentes, Nagios tiene la capacidad de alertar al personal técnico, permitiéndoles iniciar procesos de reparación antes de que dichas interrupciones afecten negativamente los procesos comerciales, los usuarios finales o los clientes.

2.5.3 LibreNMS

LibreNMS es una plataforma de monitorización de redes y sistemas de código abierto que se basa en una arquitectura cliente-servidor. Utiliza protocolos estándar de la industria, como SNMP (Simple Network Management Protocol), para recopilar información sobre dispositivos de red, servidores y servicios. LibreNMS se caracteriza por su capacidad de gestionar una amplia gama de dispositivos y sistemas operativos, ofreciendo una visión detallada del rendimiento y la disponibilidad de la infraestructura de TI de una organización (libreNMS, 2023).

La plataforma proporciona una interfaz web para configurar, personalizar y visualizar la información recopilada, permitiendo a los administradores de sistemas y redes supervisar de manera proactiva la salud y el funcionamiento de sus activos de TI.

2.5.4 Diferencias entre las Herramientas de Gestión

Se presenta un cuadro comparativo entre las herramientas de gestión libre donde se presentan las características más relevantes.

Tabla 2

Diferencias entre Zabbix, Nagios y LibreNMS

Características	Zabbix	Nagios	LibreNMS
Tipo de Herramienta	Monitorización de Red	Monitorización de Red	Monitorización de Red
Interfaz de Usuario	Moderna y personalizable	Interfaz web clásica	Interfaz web intuitiva
Licencia	GPL v2	GPL v2	GPL v3
Soporte para Múltiples Plataformas	Sí	Sí	Sí
Protocolos Soportados	SNMP, IPMI, JMX, etc.	SNMP, NRPE	SNMP, BGP, OSPF, etc.
Auto Descubrimiento de Dispositivos	Sí	Con plugins adicionales	Sí
Capacidad de Escalamiento	Excelente	Buena	Buena
Monitoreo de Rendimiento	Sí	Sí	Sí
Alertas y Notificaciones	Personalizables y flexibles	Personalizables	Personalizables
Gestión de Configuración	Sí	Con complementos	Sí
Gráficos e Informes	Detallados y personalizables	Básicos	Detallados
Soporte para Plugins y Extensiones	Amplio soporte	Sí	Sí
Comunidad y Documentación	Activa y extensa	Amplia comunidad	Activa y creciente
Integración con Sistemas de Ticketing	Sí	A través de plugins	Sí
Monitorización de Aplicaciones	Sí, con agentes dedicados	A través de plugins	En desarrollo
Historial de Desarrollo	Desde 2001	Desde 1999	Desde 2012
Desarrollo Activo	Sí	Sí	Sí

Fuente: Autoría

2.6 Políticas de Gestión

Para determinar las políticas de gestión, no hay un estándar particular que lo defina. En lugar de ello, las políticas de gestión son un conjunto de directrices que se establecen en este caso en referencia al modelo de gestión FCAPS, adaptándose a las necesidades específicas de dicha red. Estas directrices son esenciales para garantizar un óptimo desempeño de la red. Es crucial considerar que el modelo de gestión aplicado en la red y los objetivos que la institución establezca como condiciones para el acceso, control y administración de los servicios sean los adecuados para la buena operación de la red.

3. CAPITULO III – SITUACIÓN ACTUAL DE LA EMPRESA

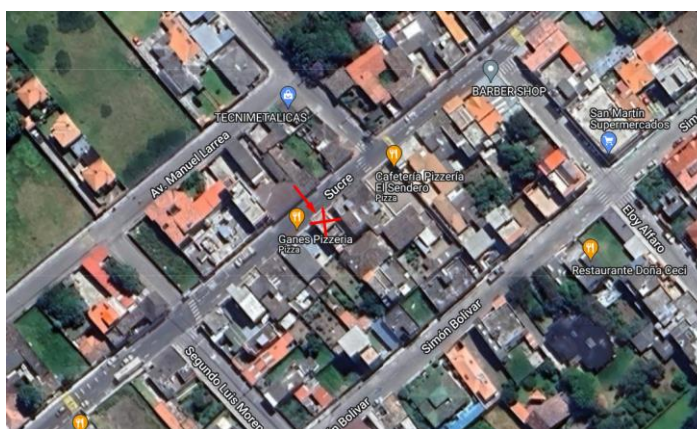
En el mundo competitivo de las telecomunicaciones, es esencial que las empresas mantengan un conocimiento profundo de su infraestructura, organización y tecnología para lograr un rendimiento óptimo y una gestión eficiente de sus redes y servicios. Este capítulo se centra en proporcionar una visión detallada de la situación actual de la empresa OMEGATELCOM S.A. como el organigrama estructural, infraestructura tecnológica y las especificaciones técnicas de los equipos, las cuales serán las bases para la posterior implementación de un modelo de gestión basado en el Modelo FCAPS de la ISO.

3.1 OMEGATELCOM S.A

Omegatelcom S.A es una empresa de telecomunicaciones con sede en la ciudad de Cotacachi. Fundada en 2020, se ha consolidado como un proveedor líder en el mercado de las telecomunicaciones en su ciudad. La empresa se dedica a ofrecer el servicio de acceso a Internet, dirigidos tanto a consumidores residenciales como a empresas.

Figura 5

Ubicación del Nodo de la empresa OMEGATELCOM S.A



Fuente: Autoría

OMEGATELCOM S.A se especializa en proporcionar servicios de acceso a Internet de alta velocidad, ofreciendo una variedad de planes adaptados a las necesidades de las personas. La empresa se enorgullece de su enfoque en la innovación tecnológica. Por lo cual ha implementado tecnologías de vanguardia, como fibra óptica y 5G. A demás, brindan soluciones de conectividad personalizadas para garantizar que sus clientes tengan una conexión estable y confiable.

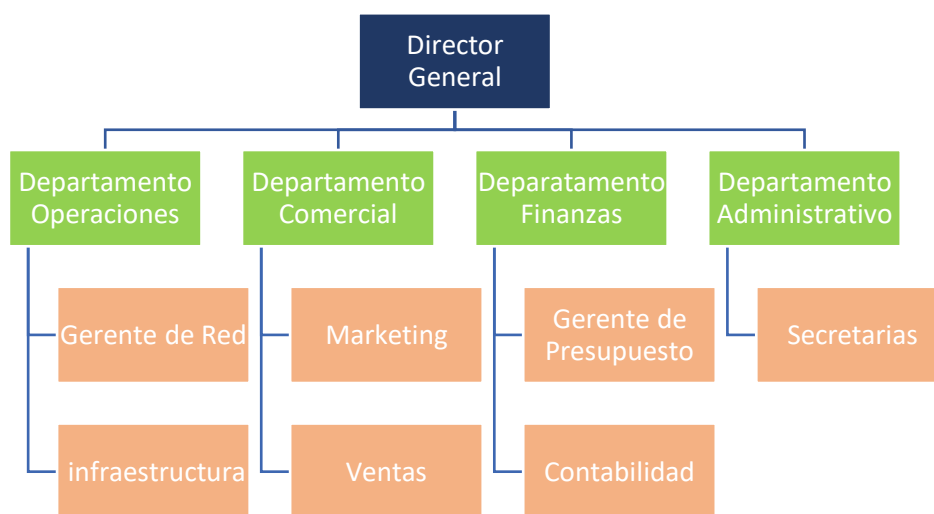
Esta empresa ha establecido programas de responsabilidad social corporativa que incluyen iniciativas para conectar a comunidades rurales y proyectos de educación digital.

3.2 Organigrama Estructural

El organigrama de OMEGATELCOM S.A representa la estructura organizativa de la empresa y la distribución de roles y responsabilidades dentro de la organización. Esta estructura se ha diseñado para garantizar una gestión eficiente de los recursos y una prestación de servicios de alta calidad a los clientes. A continuación, se observa de forma detallada las áreas que desempeñan en esta empresa.

Figura 6

Estructura Empresarial de OMEGATELCOM



Fuente: Autoría

La estructura empresarial de OMEGATELCOM cuenta con 4 departamentos fundamentales las cuales delegan a distintas personas según sus habilidades.

En la empresa OMEGATELCOM S.A, la interacción efectiva entre los departamentos de Operaciones, Comercial, Finanzas y Administrativo es esencial para garantizar el funcionamiento sin problemas de la organización y para ofrecer servicios de alta calidad a los clientes. Cada uno de estos departamentos desempeña un papel crucial en el éxito de la empresa y su capacidad para mantenerse como un líder en el mercado de servicios de Internet.

3.2.1 El Departamento de Operaciones

Es el núcleo de la infraestructura de OMEGATELCOM S.A. ya que supervisa la gestión de los servicios de la red, la infraestructura tecnológica y la prestación de servicios. Garantiza que la infraestructura de red esté en óptimas condiciones y cumpla con los estándares de calidad. Este departamento es vital para asegurar una conectividad confiable y de alta velocidad para los clientes.

3.2.2 El Departamento Comercial

Este departamento se encarga de atraer y retener a los clientes. Colabora estrechamente con el Departamento de Operaciones para comprender las capacidades de la red y los servicios que pueden ofrecerse. La información proporcionada por Operaciones es fundamental para que Comercial diseñe ofertas atractivas y ajustadas a las necesidades del mercado.

3.2.3 El Departamento de Finanzas

Gestiona los recursos económicos y garantiza la viabilidad financiera de la empresa. Trabaja en estrecha colaboración con los departamentos de Operaciones y Comercial para asegurar de que los proyectos de expansión y mejora de la red sean económicamente viables.

3.2.4 El Departamento Administrativo

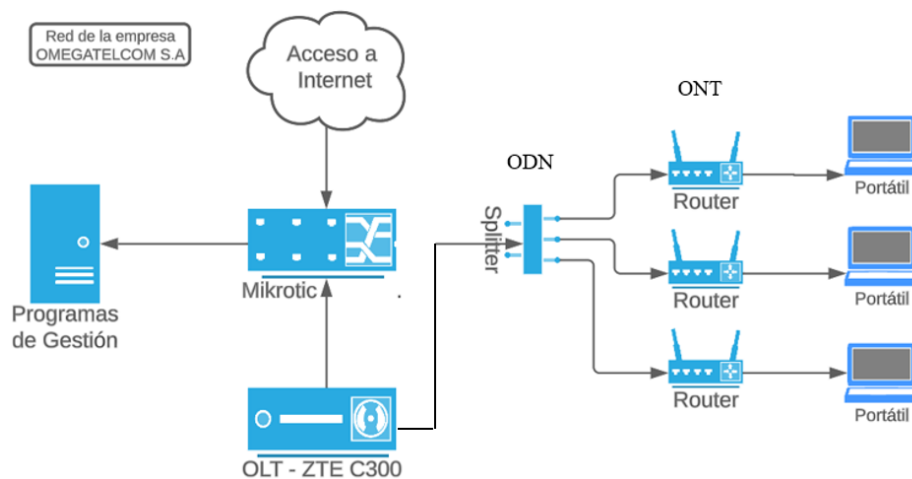
Proporciona el apoyo administrativo y logístico necesario para el funcionamiento diario de la empresa. Colabora con todos los departamentos para garantizar la eficiencia operativa.

3.3 Infraestructura Tecnológica

La infraestructura tecnológica desempeña un papel muy importante en la capacidad de OMEGATELCOM S.A para proporcionar servicios de Internet confiables y de alta calidad a sus clientes. En la siguiente Figura, se puede observar el esquema de la red GPON utilizada por la empresa, que está compuesta por 3 partes importantes: la OLT, ODN y ONT en donde la OLT se encuentra en el nodo en donde están todos los equipos. La ODN es la red pasiva de distribución que incluye a la red troncal (la cual se Splittea), la red distribución (la cual va conectada a las NAPs) y a la red de dispersión (por lo general fibra DROP). La NAP o caja óptica de distribución es el dispositivo terminal que enlaza la red de distribución con la red de dispersión. Finalmente, en la residencia del cliente se ubica la ONT (ONU), que sirve como el dispositivo terminal de la red GPON, transformando las señales ópticas en señales eléctricas.

Figura 7

Topología Física de la empresa OMEGATELCOM S.A



Fuente: Autoría

A continuación, se describe cada uno de los elementos que intervienen en la red:

Optical Line Termination (OLT): La OLT es el componente central de la red GPON ubicado en la Central de Operaciones de OMEGATELCOM. Actúa como un conmutador de alto rendimiento que gestiona múltiples conexiones de fibra óptica hacia las ONTs en la red GPON.

Red Feeder: La red troncal se compone de fibra óptica y transporta la señal óptica desde la OLT hasta un punto de distribución como el armario de GPON (FDH).

Armario de GPON (FDH - Fiber Distribution Hub): El FDH es un punto de distribución en la red de GPON donde se realizan conexiones importantes. Aquí, se conecta la red de alimentación (Red Feeder) con la red de distribución (Red de Distribución) mediante un Splitter.

Splitter: El splitter óptico es un dispositivo pasivo que divide la señal óptica en varias partes, permitiendo que una sola fibra óptica sirva a múltiples clientes en un área geográfica.

Optical Distribution Network (Red de Distribución): La red de distribución es una red de fibra óptica que parte del FDH y se extiende hacia diferentes zonas geográficas. Transporta las señales divididas desde el splitter hacia las NAP.

Caja de Distribución Óptica (NAP - Network Access Point): Las NAP son ubicaciones donde la red de distribución se distribuye hacia las ubicaciones de los clientes. Aquí, se conecta la red de distribución a las rosetas ópticas.

Red de Dispersión: La red de dispersión conecta las NAP con las ubicaciones de los clientes, como hogares y empresas. Es una parte importante de la red de acceso y permite llevar la señal óptica hasta el punto de terminación en el cliente.

Roseta Óptica: Las rosetas ópticas son puntos de terminación en las ubicaciones de los clientes. Aquí es donde se conecta la ONT para proporcionar servicios de Internet.



Optical Network Terminal (ONT): La ONT es el dispositivo que se instala en la ubicación del cliente, en la roseta óptica. Convierte la señal óptica en señales eléctricas utilizables para dispositivos del cliente, como computadoras.

3.4 Características Técnicas de los Dispositivos

En la siguiente tabla se describe los equipos que cuentan en la empresa:

Tabla 3

Especificaciones de los equipos

Dispositivos	Especificaciones	Logo
OLT – ZTE C300	<ul style="list-style-type: none"> - Capacidad del plano posterior de 5,76 Terabits por segundo (Tbit/s). - Capacidad de conmutación de 800 Gigabits por segundo (Gbit/s). - Cantidad de tarjetas de servicio: 14 (GPON/P2P/XG). - Cantidad de tarjetas de control: 2. - Cantidad de tarjetas de enlace ascendente: 2 - Número máximo de suscriptores GPON: 16384. 	
Mikrotic RB1100AH	<ul style="list-style-type: none"> - La frecuencia nominal de la CPU es de 1GHz - Dimensiones Caja 1U: 44 x 176 x 442 mm, 1200 g. - Licencia de enrutador OS 6 - El Sistema operativo es enrutadorOS - Tamaño de almacenamiento de 128 megas - Almacenamiento NAND - MTBF de 200.000 horas a 25C 	

- Temperatura probada de -25 °C a +65 °C
- Tipo de arquitectura: SMIPS
- Número de núcleos de CPU: 1
- Frecuencia nominal de la CPU: 650MHz
- Licencia para el sistema operativo del enrutador OS 4
- El sistema operativo utilizado es enrutadorOS
- Capacidad de RAM: 32 megabytes
- Capacidad de almacenamiento: 16 megabytes



- Cubierta exterior fabricado con MDPE.
- Resistencia máxima a la tensión: 1250 N.
- Rango de temperatura operativa: -20°C a +65°C.
- Distancia entre postes (Span): 80 metros.
- Incorpora protección contra rayos UV y humedad.
- Diámetro nominal: 6.6 ± 0.3 mm.
- Peso estándar por kilómetro (kg/km): 50 ± 10 kg/km.
- Consta de 12 hilos.
- Presenta un forro de color negro.



- Carcasa diseñada para uso en exteriores, presenta un excelente rendimiento de sellado y cuenta con protección IP68.
- Incluye un puerto para sangrado, dos puertos adicionales para derivación y dieciséis puertos para cables tipo DROP.
- Capacidad de fusión de hasta 96 hilos y un panel con 24 adaptadores SC.



- Cuatro caseteras para alojar 12 o 24 fusiones cada una.
- Capacidad para albergar splitters de 1x8 o 1x16.
- Sellado mecánico reutilizable sin necesidad de tornillos.
- Construida con material plástico de alto impacto.
- Resistente a los rayos UV, condiciones de lluvia, ambientes salinos y ácidos.
- Diseñada para uso en exteriores, con protección IP65.
- Apropiada tanto para empalmes por fusión como mecánicos.
- Panel de parcheo con capacidad para hasta 16 adaptadores SC.
- Puede albergar splitters PLC de 1x8 y 1x16.
- Dispone de 2 puertos de entrada y 16 puertos de salida para cables tipo DROP.



NAP IP 65

ONT Huawei
HG8310M

- 1 puerto GPON SC/UPC
- 1 puerto Ethernet Gigabit
- Servidor DHCP integrado para la asignación automática de direcciones IP
- Compatibilidad con DNS dinámico (DDNS) incorporado y compatibilidad con el servicio No-IP
- Soporte para reenvío de puertos, DMZ, funciones de firewall



- Router Cudi
AX1800
- Wi-Fi AX1800 6 súper rápido
 - Potente CPU de doble núcleo
 - 5 puertos Gigabit
 - 4 antenas omnidireccionales fijas
 - Servidor y cliente VPN
 - DDNS



Fuente: Autoría

3.5 Evaluación de la Gestión de las TI de OMEGATELCOM S.A.

Para la evaluación de la gestión de las TI se llevó a cabo entrevistas con el personal de la empresa y dos encuestas, basadas en los objetivos de la empresa OMEGATELCOM en el área de TI tanto para los trabajadores de la empresa y sus clientes.

3.5.1 Encuestas

Las encuestas planteadas tanto para el personal como para los clientes tienen como objetivo principal, obtener de forma detallada y precisa las necesidades y experiencias en relación con la gestión de la infraestructura de tecnologías de la información en OMEGATELCOM. Estas encuestas buscan recopilar información valiosa para identificar áreas de mejora, fortalezas y oportunidades en la gestión de la infraestructura de las TI, tanto desde la perspectiva interna del personal como desde la perspectiva externa de los clientes.

Las interrogantes del cuestionario se encuentran determinadas en función de las áreas funcionales del modelo de gestión FCAPS. En la siguiente tabla, se puede observar la estructura de la encuesta tanto para el personal de la empresa y sus los clientes:

Tabla 4*Encuesta dirigida al personal de OMEGATELCOM*

Áreas Funcionales	N.º
Área de Fault Management (Gestión de Fallas)	5
Área de Configuration Management (Gestión de Configuración)	5
Área de Accounting Management (Gestión de Contabilidad)	5
Área de Performance Management (Gestión de Rendimiento)	5
Área de Security Management (Gestión de Seguridad)	5
Total	25

*Fuente: Autoría***Tabla 5***Encuesta dirigida a los clientes de OMEGATELCOM*

Preguntas	N.º
Calidad de servicio	6
Resolución de Problemas	7
Total	13

Fuente: Autoría

3.5.2 Muestras

Para la realización de las encuestas en los trabajadores, se optó por la recopilación de información mediante un muestreo no probabilístico. Este enfoque implica la selección de participantes basada en criterios específicos y no en un proceso aleatorio, lo que permite dirigir la investigación hacia grupos específicos que son relevantes para los objetivos de esta encuesta. De esta manera, se busca obtener datos representativos que reflejen las percepciones y experiencias

clave relacionadas con la administración de la infraestructura de tecnologías de la información en OMEGATELCOM.

En las encuestas dirigidas a los clientes, se llevó a cabo la selección de 10 participantes anónimos de distintas zonas de las ciudades de Cotacachi. Este enfoque permite capturar una diversidad de perspectivas y experiencias, considerando las posibles variaciones en la percepción de la gestión de la infraestructura de tecnologías de la información en diferentes áreas geográficas.

A continuación, en la siguiente Tabla se muestra el personal que contribuyó en las encuestas, estas personas son líderes en las áreas funcionales de la empresa OMEGATELCOM.

Tabla 6

Personal encuestado

Nombre	Oficio
Roberto Gómez	Presidente
Javier Lema	Gerente de red
Marcelo Malte	Secretario
Marco Quetama	Infraestructura
Andrés Díaz	Infraestructura

Fuente: Autoría

3.5.3 Análisis de Resultados Obtenidos

A continuación, se presenta los resultados de cada una de las áreas funcionales del modelo de gestión FCAPS, los detalles en general de la encuesta se encuentran en el anexo.

1. Área de Fault Management (Gestión de Fallas)

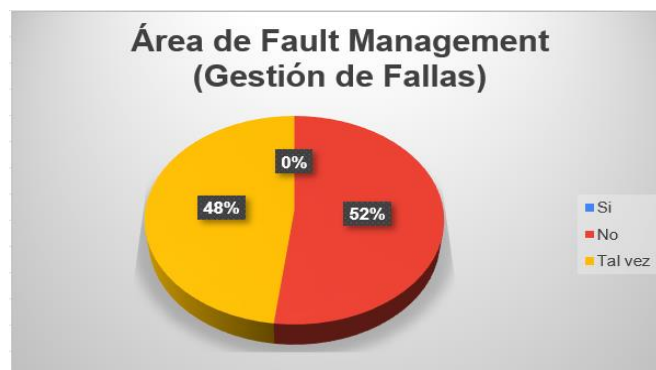
El 52% de los encuestados indicaron “No”. Esto indica que el manejo, resolución, comunicación y transparencia de las fallas en la red no son las adecuadas.

El 48% de los encuestados respondió con “Tal vez”. Este grupo puede representar a aquellos que no están completamente seguros de la eficacia de la gestión de fallas en la empresa.

La ausencia de respuestas “Sí” (0%) indica que ninguno de los encuestados expresó plena satisfacción con el área de Fault Management. Este hallazgo podría ser una señal importante de áreas críticas que requieren atención y mejoras.

Figura 8

Resultado de la encuesta en la Gestión de Fallas



Fuente: Autoría

2. Área de Configuration Management (Gestión de Configuración)

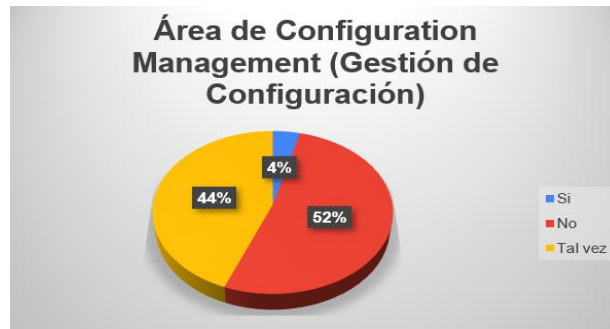
El 52% de los encuestados indique que los procedimientos de configuración de la red no son claros o fáciles de seguir sugiere una posible falta de claridad en los procesos, lo que podría impactar en la eficiencia de la configuración.

El 44% ha experimentado problemas debido a errores de configuración y no están seguros de que exista una buena colaboración entre los equipos de configuración en la red.

El hecho de que solo el 4% indique que los problemas de configuración se resuelven de manera inmediata podría ser un área clave de mejora.

Figura 9

Resultado de la encuesta en la Gestión de Configuración



Fuente: Autoría

3. Área de Accounting Management (Gestión de Contabilidad)

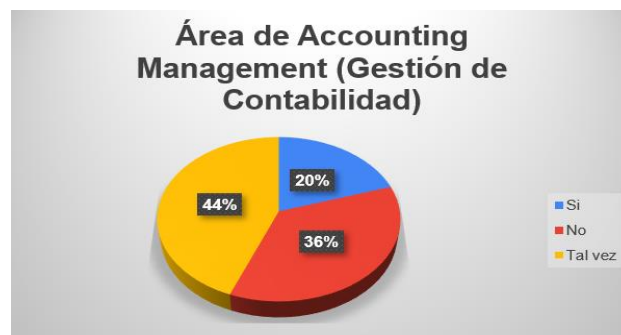
El 36% de los encuestados indicaron que no se sienten informados sobre los costos y tarifas, han notado problemas en el registro de recursos utilizados y no consideran precisa la facturación.

El 44% de respuestas “Tal Vez” indica cierta ambigüedad o incertidumbre en las percepciones de los encuestados.

El 20% de respuestas “Sí” en aspectos, como la precisión en la facturación, sugiere que hay una proporción de encuestados que perciben un buen desempeño en ciertos aspectos de la gestión financiera.

Figura 10

Resultado de la encuesta en la Gestión de Contabilidad



Fuente: Autoría

4. Área de Performance Management (Gestión de Rendimiento)

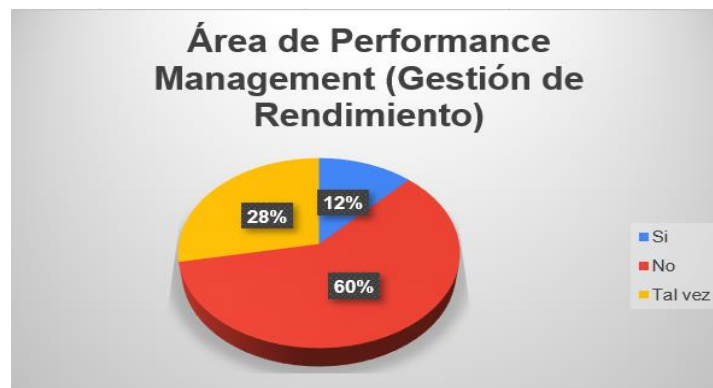
El 60% de los encuestados respondieron “No” por lo que, en diversas áreas, incluyendo el cumplimiento de expectativas de calidad y velocidad, la experiencia de congestión en la red, y la visualización gráfica del rendimiento, son áreas críticas que requieren una reformación inmediata.

El 28% de respuestas “Tal Vez” indica que la visualización del rendimiento del sistema y monitorización de la red pueden ser mejoradas.

El 12% de respuestas “Sí” indica que hay un segmento de usuarios que percibe que se cumplen sus expectativas de calidad de servicio.

Figura 11

Resultado de la encuesta en la Gestión de Rendimiento



Fuente: Autoría

5. Área de Security Management (Gestión de Seguridad)

El 60% de los encuestados respondieron “No” esto nos indica que la protección contra amenazas de seguridad cibernética, la experiencia de intentos de acceso no autorizado, la efectividad de las políticas de seguridad, y la rapidez en la resolución de problemas de seguridad, sugiere una preocupación generalizada sobre la seguridad de la red.

El 36% de respuestas “Tal Vez” indica que no están muy seguros de tener una protección adecuada ante amenazas de seguridad para proteger la red.

El 4% de respuestas "Sí" tiene capacitaciones de seguridad, pero de manera voluntaria en diferentes cursos que no son de la empresa OMEGATELCOM.

Figura 12

Resultado de la encuesta en la Gestión de Seguridad



Fuente: Autoría

1. Calidad de Servicio en Clientes

El 48% de respuestas "Tal Vez" indica una posición neutral en cuanto a la calidad del servicio. El 42% de respuestas "No" sugiere que un segmento significativo de los clientes no percibe que el servicio cumple con sus expectativas de calidad. Y el 10% de respuestas "Sí" indica que hay un grupo más reducido de clientes que están satisfechos con la calidad del servicio

Figura 13

Resultado de la encuesta en la Calidad de servicio de los clientes



Fuente: Autoría

2. Resolución de Problemas en Clientes

El 44% de respuestas “No” sugiere que un porcentaje significativo de los clientes no percibe que los problemas técnicos se resuelven de manera efectiva. El 43% de respuestas “Tal Vez” indica que los clientes no se sienten totalmente satisfechos en la resolución, notificación y prontitud de fallas en la red. El 13% de respuestas “Sí” indica que hay un grupo más reducido de clientes que percibe que los problemas se resuelven de manera satisfactoria.

Figura 14

Resultado de la encuesta en la Resolución de problemas en los clientes



Fuente: Autoría

3.6 Definir y priorizar los problemas

Gracias a los resultados de las preguntas y los porcentajes de las respuestas, podemos definir y priorizar los problemas en cada área:

Área de Fault Management (Gestión de Fallas):

1. Problema Prioritario:

- El 52% indicó "No" en la eficacia de los procedimientos de detección y resolución de fallas. Esto señala una posible falta de eficiencia en la gestión de fallas, que debería investigarse y abordarse.

2. Problema Secundario:

- El 48% indicó "Tal vez" en la comunicación eficiente de la información sobre fallas en la red. Mejorar la comunicación en tiempo real sobre las fallas puede ser un área de enfoque.

Área de Configuration Management (Gestión de Configuración):

1. Problema Prioritario:

- El 52% indicó "No" en la claridad y facilidad de seguimiento de los procedimientos de configuración. Esto sugiere que los procedimientos pueden necesitar mejoras para evitar problemas futuros.

2. Problema Secundario:

- El 44% indicó "Tal vez" en la resolución inmediata de problemas de configuración. La eficiencia en la resolución inmediata es esencial y puede ser objeto de mejoras.

Área de Accounting Management (Gestión de Contabilidad):

1. Problema Prioritario:

- El 36% indicó "No" en sentirse informado sobre costos y tarifas. Mejorar la comunicación de costos puede aumentar la transparencia y la satisfacción del cliente.

Área de Performance Management (Gestión de Rendimiento):

1. Problema Prioritario:

- El 60% indicó "No" en que la calidad y velocidad cumplan con expectativas. Este es un problema central que afecta directamente a la satisfacción del cliente y debe abordarse con urgencia.

2. Problema Secundario:

- El 28% indicó "Tal vez" en la efectividad de la monitorización de red y rendimiento. Mejorar la monitorización puede contribuir a una gestión más eficaz.

Área de Security Management (Gestión de Seguridad):

1. Problema Prioritario:

- El 60% indicó "No" en sentir que la red está adecuadamente protegida contra amenazas cibernéticas. Reforzar la seguridad cibernética es esencial para proteger la red y la confianza del cliente.

2. Problema Secundario:

- El 36% indicó "Tal vez" en la eficacia de las políticas de seguridad. Revisar y fortalecer las políticas de seguridad es fundamental.

Estos problemas definidos y priorizados proporcionan una guía clara para las acciones correctivas en cada área. Puedes abordar estos problemas en tu tesis, proponiendo soluciones y estrategias específicas para mejorar la gestión en cada dominio.

3.7 Selección de la Herramienta de Gestión

Basándonos en los problemas identificados y las necesidades específicas de OMEGATELCOM, podemos delimitar por qué Zabbix sería la herramienta ideal para la implementación en las áreas problemáticas identificadas:

Área de Fault Management (Gestión de Fallas):

1. Detección Eficiente:

- Zabbix ofrece una potente capacidad de monitoreo en tiempo real, permitiendo la detección eficiente de fallas a través de alertas automáticas y notificaciones instantáneas.

2. Comunicación Transparente:

- Zabbix proporciona informes detallados y tableros personalizables que facilitan la comunicación transparente sobre el estado de la red, mejorando la visibilidad y comprensión de las fallas.

3. Resolución Oportuna:

- La capacidad de respuesta rápida de Zabbix, junto con su capacidad para generar alertas específicas, facilita la resolución oportuna de fallas.

4. Transparencia en la Comunicación:

- Los informes detallados y la información transparente proporcionada por Zabbix son herramientas valiosas para mejorar la comunicación sobre las fallas con los usuarios.

Área de Configuration Management (Gestión de Configuración):

1. Procedimientos Claros:

- Zabbix facilita la creación de procedimientos claros mediante su interfaz intuitiva y documentación detallada.

2. Resolución Inmediata:

- Zabbix permite una resolución inmediata de problemas de configuración mediante alertas en tiempo real y registros detallados.

Área de Accounting Management (Gestión de Contabilidad):

1. Información Transparente:

- Zabbix proporciona informes detallados sobre el rendimiento y el uso de recursos, mejorando la transparencia sobre costos y tarifas.

2. Facturación Precisa:

- Zabbix ayuda a garantizar la precisión en la facturación al proporcionar una visión clara de los recursos utilizados y su impacto en los costos.

Área de Performance Management (Gestión de Rendimiento):

1. Mejora Continua:

- Zabbix respalda la mejora continua al proporcionar datos detallados sobre el rendimiento, lo que permite ajustes inmediatos y estrategias de mejora.

2. Monitorización Efectiva:

- Zabbix destaca por su monitorización efectiva, permitiendo visualizar el rendimiento del sistema de manera clara y en tiempo real.

Área de Security Management (Gestión de Seguridad):

1. Protección Cibernética:

- Zabbix cuenta con características avanzadas de seguridad, asegurando la protección cibernética de la red mediante monitoreo y alertas ante posibles amenazas.

2. Educación en Seguridad:

- Zabbix facilita la educación en seguridad al proporcionar informes y alertas sobre eventos de seguridad, permitiendo la capacitación continua del personal.

En resumen, Zabbix emerge como una herramienta integral que aborda las áreas problemáticas identificadas al ofrecer funcionalidades avanzadas de monitoreo, alertas en tiempo real, informes detallados y una interfaz intuitiva que facilita la gestión y colaboración eficientes

entre equipos. Su capacidad para adaptarse a entornos complejos y cambiantes lo convierte en una opción sólida para mejorar la gestión de OMEGATELCOM.

4. CAPITULO IV – MODELO DE GESTIÓN FCAPS DE LA ISO

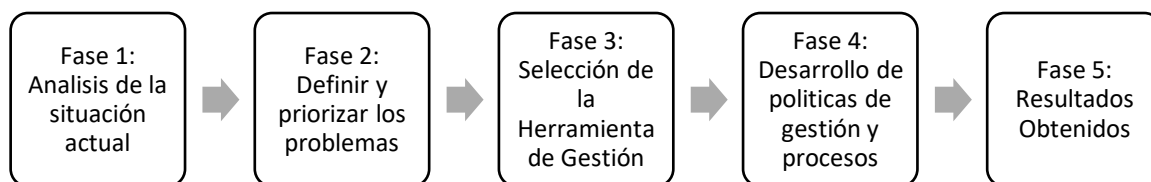
En este capítulo se desarrolla el modelo de gestión en el entorno de OMEGATELCOM. A través de políticas y procesos de gestión diseñadas a partir de las necesidades detectadas, manuales de procedimientos adaptados, junto con la recomendación del sistema de monitoreo Zabbix, para demostrar la efectividad del modelo de gestión planteado, ajustado a las necesidades específicas de la empresa de telecomunicaciones.

4.1 Fases de definición del modelo de gestión de OMEGATELCOM

Para la definición del modelo de gestión planteado, se debe llevar a cabo distintas fases a seguir para la aplicación de este modelo. A continuación, se describe el proceso realizado.

Figura 15

Fases de definición del modelo de gestión de la empresa OMEGATELCOM



Fuente: Autoría

Fase 1: Análisis de la Situación Actual

En esta etapa inicial, se realiza una evaluación de la infraestructura existente, los procesos operativos y el estado general de la red y los servicios de OMEGATELCOM. Se recopila información clave sobre el rendimiento, la disponibilidad, la seguridad y otros aspectos críticos por medio de entrevistas y encuestas, para comprender la situación actual de la empresa.

Fase 2: Definir y Priorizar los Problemas

Con la información recopilada en la fase de análisis, se identifican y definen claramente los problemas y desafíos que afectan la eficiencia y la calidad del servicio. Es crucial priorizar estos problemas para abordar primero aquellos que tienen un impacto más significativo en la operación y la satisfacción del cliente.

Fase 3: Selección de la Herramienta de Gestión

Ya priorizado los problemas en esta fase implica la evaluación y selección de la herramienta de gestión más adecuada para las necesidades analizadas de OMEGATELCOM. Se consideran aspectos claves como la gestión de fallas, rendimiento, la seguridad y otros criterios relevantes. La elección de una herramienta eficaz es esencial para implementar un modelo de gestión sólido.

Fase 4: Desarrollo de Políticas de Gestión y Procesos

Con la herramienta seleccionada, se desarrollan políticas de gestión claras y procesos eficientes. Esto incluye la definición de roles y responsabilidades, la creación de procedimientos estándar y la implementación de políticas que aseguren el cumplimiento de los objetivos de gestión establecidos.


Fase 5: Resultados Obtenidos

En esta fase final, se realiza pruebas de funcionamiento de las políticas y procesos, en el cual se monitorea de cerca su desempeño. Se ajustan los procesos según sea necesario, y se realizan pruebas para garantizar la integración efectiva con los sistemas existentes.

4.2 Establecimiento de las políticas de gestión para OMEGATELCOM

Una vez realizado el levantamiento de información realizado en el capítulo III Se definen políticas de gestión de red que abarquen las cinco áreas funcionales del modelo de gestión FCAPS, adaptándolas a las necesidades específicas de la empresa OMEGATELCOM.

Las políticas determinadas, que se detallan en los siguientes cuadros, no tienen la intención de ser reglas obligatorias, sino más bien servir como pautas para el administrador y el personal de red, con el propósito de mantener el funcionamiento adecuado de la red..

EMPRESA OMEGATELCOM S.A.		
PÓLITICAS DE GESTIÓN PARA LA RED		
	Elaborado por:	Jhonatan Jacome
	Revisado por:	Ing. Javier Lema Administrador de red
	Aprobado por:	Ing. Edgar Jaramillo
	Versión:	1.0
	Año de elaboración:	2024
I. OBJETIVO		
<p>Las políticas de gestión en OMEGATELCOM buscan garantizar el buen funcionamiento de las operaciones de la red de telecomunicaciones al minimizar interrupciones, mejorar la experiencia del cliente y la seguridad de la red. El personal a cargo de la administración de la red debe adherirse a estas políticas de gestión de red.</p>		
II. NIVELES ORGANIZACIONALES		
<p>a) El Director General: Tiene la responsabilidad de planificar, organizar y coordinar los procesos de la empresa, tomando decisiones clave sobre inversiones y alineando las operaciones de red con los objetivos propuestos en la empresa.</p>		

- b) **El Administrador de Red:** Supervisa la operación diaria, lidera equipos técnicos y ejecuta planes tácticos para el correcto funcionamiento de la red, coordinando la implementación de nuevas tecnologías.
- c) **Soporte Técnico:** Es el servicio especializado que proporciona asistencia y soluciones a usuarios o clientes para abordar inconvenientes vinculados al uso de tecnologías, software, hardware u otros productos informáticos.
- d) **Usuario:** Individuo que utiliza el servicio de internet u otro proporcionado por la organización.

III. GENERALIDADES

- **Compromiso del Responsable de la Gestión de Red:**

La persona encargada de la gestión de la red de datos asume el compromiso de cumplir rigurosamente todas las políticas detalladas en estos informes. Este compromiso es esencial para garantizar la coherencia y efectividad en la administración de la red.

- **Eficiencia**

El objetivo principal de estas políticas es mejorar la eficiencia operativa y reducir errores al establecer prácticas estandarizadas. El objetivo es simplificar la creación de plantillas para tareas específicas, posibilitando actualizaciones y modificaciones simultáneas en la red con el fin de mejorar su rendimiento.

- **Flexibilidad y Actualización Continua:**

Estas políticas sirven como guía fundamental y pueden actualizarse según sea necesario, con el personal autorizado para llevar a cabo modificaciones, siempre y cuando estén alineadas con los objetivos estratégicos de gestión.

IV. VIGENCIA

Estas políticas de la gestión para la red en general de OMEGATELCOM tendrán una vigencia determinada, la cual deberá basarse en factores como actualizaciones tecnológicas, cambios en la estructura organizativa y alineación con los objetivos de la empresa. Se recomienda establecer un periodo de revisión anual o según las necesidades que se presente.

V. REFERENCIA

Actualmente no existe un estándar en concreto para establecer políticas de gestión de red, Por lo tanto, se ha tomado como referencia las tesis llevadas a cabo en la empresa JASSA, por Rosa Hermosa, en el 2023, específicamente, se hace referencia a la tesis realizada por Jérica Báez en la UTN en el 2017, tomando como base el modelo FCAPS.

VI. ESTRUCTURA DE LAS POLÍTICAS DE GESTIÓN

1. Principios de las Políticas de Gestión de Red
 - 1.1 Objetivos de las Políticas de Gestión de Red
 - 1.2 Compromiso por parte de las Autoridades
2. Políticas para el manejo de Gestión de Fallos
 - 2.1 Manejo para Fallos
 - 2.2 Manejo para Incidentes
 - 2.3 Documentación para Incidentes y Fallos
 - 2.4 Mesa de Servicio
3. Políticas de Gestión de Configuración
 - 3.1 Ingreso de Dispositivos a la Red
 - 3.2 Configuración de Dispositivos
4. Políticas de Gestión de Contabilidad
 - 4.1 Inventario de Dispositivos de la red

4.2 Uso de los Servicios de la Red

5. Políticas de Gestión de Rendimiento

5.1. Informes de Rendimiento de Dispositivos

6. Políticas de Gestión de Seguridad

6.1. Acceso al Sistema de Red

VII. GLOSARIO

Red de Telecomunicaciones: Conjunto de dispositivos interconectados que permiten la transmisión de datos, voz y otros servicios de comunicación.

Gestión de Red: El conjunto de actividades, métodos y técnicas utilizados para administrar, monitorear y mantener una red de manera eficiente.

FCAPS: Acrónimo que representa los cinco aspectos clave de la gestión de red: Fault, Configuration, Accounting, Performance, y Security.

Mesa de Servicio: Es un centro de atención y soporte que brinda asistencia a los usuarios finales de una organización. Su función principal es recibir, registrar, priorizar y resolver solicitudes de servicio o incidentes, así como proporcionar información y asistencia técnica. La mesa de servicio actúa como un punto de contacto central entre los usuarios y los equipos de soporte técnico.

Fuente: Autoría

4.2.1 Políticas para el manejo de Gestión de Fallos

Las políticas de Gestión de Fallos implementadas se encuentran en el Anexo 2 para el caso del Manejo de Fallos se encuentra en el literal C con el código PLOGA-0003, Manejo de Incidentes en el literal D con el código PLOGA-0004, Documentación de Fallos e Incidentes en el literal E

con el código PLOGA-0005 y para la Mesa de Servicio en el literal F con el código PLOGA-0006. A continuación, se analiza cada una de las políticas mencionadas.

4.2.1.1 Manejo para Fallos

Objetivo. - Garantizar una operación eficiente y continua de la red de OMEGATELCOM mediante la identificación, diagnóstico, y resolución de cualquier fallo que afecte la calidad del servicio, minimizando el impacto en los usuarios y en la infraestructura.

Alcance. - El alcance del manejo de fallos abarca la totalidad de la red de OMEGATELCOM, incluyendo todos los equipos, sistemas, y servicios. Se extiende desde la detección temprana de anomalías hasta la resolución completa de los fallos, cubriendo tanto las áreas técnicas como operativas. Incluye la coordinación entre los equipos de soporte técnico, la actualización de registros de incidentes, y la implementación de medidas preventivas para evitar recurrencias. Este proceso se aplica a todos los fallos, desde la identificación inicial hasta la documentación y aprendizaje posterior.

4.2.1.2 Manejo para Incidentes

Objetivo. - Asegurar la pronta identificación, clasificación, y respuesta efectiva ante cualquier incidente que afecte la operación de la red de OMEGATELCOM. Minimizando así el impacto negativo en los servicios, y restaurar la normalidad operativa lo más rápido.

Alcance. - El alcance del manejo de incidentes se extiende a toda la infraestructura y servicios de la red de OMEGATELCOM. Incluye la detección temprana, evaluación, clasificación, y respuesta a eventos no planificados que puedan afectar la calidad del servicio. Se abarcan incidentes relacionados con fallos tecnológicos, amenazas de seguridad, eventos inesperados, y otros sucesos que puedan impactar la operación normal. El proceso cubre desde la identificación inicial hasta la resolución y posterior análisis para la mejora continua del sistema.

4.2.1.3 Documentación para Incidentes y Fallos

Objetivo. - Garantizar un registro detallado y preciso de todos los fallos e incidentes ocurridos en la red de OMEGATELCOM. El objetivo es facilitar un historial completo y accesible para el análisis post incidente, la toma de decisiones informada, y el establecimiento de medidas preventivas y correctivas.

Alcance. - El alcance de la documentación abarca todos los fallos e incidentes registrados en la red de OMEGATELCOM. Incluye la recopilación de información relevante como la descripción detallada del evento, acciones tomadas, responsables involucrados, tiempo de respuesta, soluciones aplicadas, y cualquier otro detalle significativo. El proceso de documentación se inicia desde la detección del fallo o incidente hasta la completa resolución y posterior análisis. La documentación se aplica a eventos relacionados con la tecnología, seguridad, rendimiento, y cualquier aspecto que pueda afectar la operación normal de la red. La información documentada es valiosa para la mejora continua del sistema y la prevención de futuros problemas.

4.2.1.4 Mesa de Servicios

Objetivo. - Asegurar un punto centralizado de recepción, registro, clasificación, y seguimiento de los fallos reportados por los usuarios, garantizando una atención eficiente y oportuna. El objetivo principal es restaurar los servicios afectados y minimizar el impacto en los usuarios, priorizando la resolución rápida y eficaz de los fallos.

Alcance. - La mesa de servicio abarca todas las actividades relacionadas con el manejo de fallos desde su detección hasta la resolución. Incluye la recepción de reportes de fallos por parte de los usuarios, el registro detallado de la información proporcionada, la clasificación y asignación de prioridades, la comunicación efectiva con los equipos de resolución, y el seguimiento continuo hasta la completa solución del fallo.

4.2.2 Políticas de la Gestión de Configuraciones

Las políticas de Gestión de Configuraciones implementadas se encuentran en el Anexo 2 para el caso del Ingreso de Equipos a la Red se encuentra en el literal G con el código PLOGA-0007, Configuración de Equipos en el literal H con el código PLOGA-0008. A continuación, se analiza cada una de las políticas mencionadas.

4.2.2.1 Ingreso de Dispositivos a la Red

Objetivo. - Garantizar un proceso controlado y seguro para la incorporación de nuevos equipos a la red, asegurando la compatibilidad y coherencia de la configuración, y minimizando posibles impactos negativos en la infraestructura existente.

Alcance. - El ingreso de equipos a la red abarca desde la planificación previa hasta la completa integración y puesta en funcionamiento de los dispositivos en la infraestructura. Esto incluye la definición de criterios de compatibilidad y requisitos técnicos, la evaluación de la capacidad de la red para recibir nuevos equipos y la verificación de conformidad con las normativas de seguridad.

4.2.2.2 Configuración de Dispositivos

Objetivo. - Asegurar que los equipos de la red se configuren de manera adecuada y controlada, cumpliendo con los estándares y requisitos establecidos por la empresa, para garantizar la estabilidad, disponibilidad y rendimiento óptimo de la infraestructura.

Alcance. - El proceso de configuración de equipos abarca desde la aprobación del equipo de TIC hasta la implementación y verificación de dicha configuración en los dispositivos de red. Esto incluye la creación y documentación de perfiles de configuración, la asignación de parámetros específicos, la actualización y gestión de contraseñas y la aplicación de políticas de seguridad. El

alcance también incorpora la gestión de cambios en la configuración, la actualización de la documentación correspondiente y la generación de informes.

4.2.3 Políticas de Gestión en Contabilidad

Las políticas de Gestión de Contabilidad implementadas se encuentran en el Anexo 2 para el caso del Inventario de Equipos se encuentra en el literal I con el código PLOGA-0009, Uso de los Servicios de Red en el literal J con el código PLOGA-0010. A continuación, se analiza cada una de las políticas mencionadas.

4.2.3.1 Inventario de Dispositivos de la red

Objetivo. - Garantizar un registro preciso y actualizado de todos los equipos de red, incluyendo detalles como su ubicación, estado, fecha de adquisición, y otros atributos relevantes. El objetivo es facilitar una gestión eficiente de los recursos y el cumplimiento de las normativas contables y de auditoría.

Alcance. – El proceso de inventario de equipos abarca desde la identificación y registro inicial de los dispositivos hasta la monitorización y actualización continua de la información relacionada. Esto incluye la creación de una base de datos centralizada para el inventario, la asignación de identificadores únicos a cada equipo, la documentación detallada de las características técnicas y la ubicación física. Además, el alcance implica la realización de inventarios físicos periódicos para validar la información del sistema y la generación de informes regulares para la toma de decisiones y la rendición de cuentas.

4.2.4.2 Uso de los Servicios de Red

Objetivo. - Optimizar la gestión de la contabilidad en el entorno de servicios de red y telecomunicaciones para garantizar la eficiencia operativa, la transparencia financiera y la competitividad del negocio.

Alcance. – Se pretende desarrollar e implementar políticas para la medición precisa en la utilización de los recursos de red, la tarificación para reflejar costos reales, la optimización de procesos de cobro y finanzas, la capacitación del personal, y la mejora de la transparencia financiera. Se busca mejorar la eficiencia operativa, garantizar la competitividad en el mercado, y transparencia financiera

4.2.4 Políticas de Gestión de Rendimiento

Las políticas de Gestión de Rendimiento implementadas se encuentran en el Anexo 2 para el caso del Informe de Rendimiento se encuentra en el literal K con el código PLOGA-0011. A continuación, se analiza cada una de las políticas mencionadas.

4.2.4.1 Informe de rendimiento de Dispositivos

Objetivo. - Proporcionar informes detallados y precisos sobre el rendimiento de la red, abarcando aspectos clave como la calidad de los servicios, la utilización de recursos, la detección de posibles cuellos de botella y la evaluación del cumplimiento de los niveles de servicio. El objetivo es ofrecer a los responsables en la toma de decisiones, una visión clara y completa del rendimiento de la red para tomar las mejores decisiones y anticipar problemas potenciales.

Alcance. – El proceso de informe de rendimiento abarca desde la recopilación y análisis de datos relacionados con el rendimiento de la red hasta la presentación estructurada de informes periódicos. Esto incluye la identificación y medición de parámetros clave, como ancho de banda, latencia, pérdida de paquetes y otros indicadores relevantes. El alcance también implica la definición de formatos de informes estandarizados, la programación de informes regulares para facilitar el monitoreo continuo y la adaptación de los informes según las necesidades específicas de los diferentes niveles de la organización.

4.2.5 Políticas de Gestión de Seguridad

Las políticas de Gestión de Seguridad implementadas se encuentran en el Anexo 2 para el caso del Acceso al Sistema de la Red se encuentra en el literal L con el código PLOGA-0012. A continuación, se analiza cada una de las políticas mencionadas

4.2.5.1 Acceso al Sistema de la Red

Objetivo. - Asegurar que el acceso al sistema de la red esté controlado y limitado a usuarios autorizados, garantizando la confidencialidad, integridad y disponibilidad de la información crítica y de los recursos de la red. El objetivo principal es prevenir accesos no autorizados y actividades maliciosas, minimizar riesgos de seguridad, y proteger la infraestructura y los datos sensibles almacenados en el sistema de gestión de la red.

Alcance. - El alcance abarca todas las actividades relacionadas con el acceso al sistema de gestión de la red, desde la autenticación de usuarios hasta la gestión de privilegios y la supervisión de actividades. Incluye la implementación de medidas de seguridad robustas, como contraseñas seguras, políticas de bloqueo de cuentas y la asignación de roles y permisos específicos según las responsabilidades y necesidades laborales. También se contempla la auditoría regular de registros de acceso para detectar posibles anomalías, capacitaciones de seguridad al personal y la respuesta inmediata a cualquier intento no autorizado.

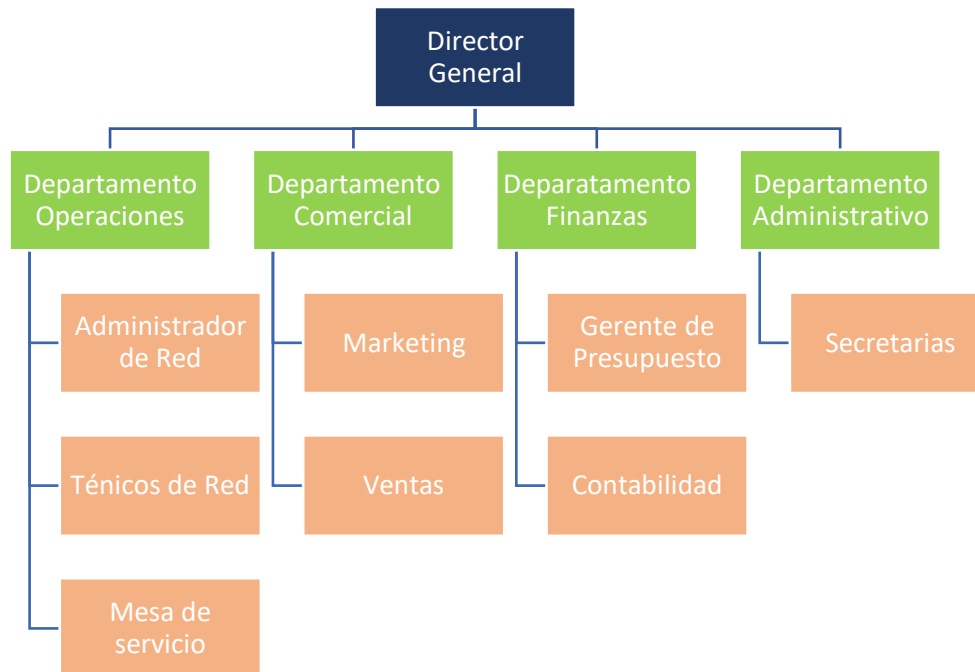
4.3 Levantamiento de Procesos de Gestión para OMEGATELCOM

Los manuales de procesos son documentos que describen de manera detallada los pasos y procesos que deben seguirse en la empresa OMEGATELCOM para llevar a cabo tareas específicas. Estos manuales son útiles para establecer estándares y asegurar la coherencia en la ejecución de diversas funciones. La Empresa OMEGATELCOM S.A. no cuenta con una estructura

empresarial bien diseñada y la asignación eficiente de habilidades, siendo crucial en una empresa de internet para su éxito. A continuación, la siguiente organización con la incorporación de una mesa de servicio y la cooperación entre departamentos, facilita la eficiencia operativa, impulsa el desarrollo de productos y servicios, garantiza una atención al cliente de calidad, promueve el crecimiento sostenible y contribuye a una sólida cultura empresarial. Al optimizar la distribución de tareas y talentos, la empresa puede posicionarse de manera competitiva en el dinámico entorno digital, asegurando no solo su supervivencia, sino también su crecimiento y prosperidad a largo plazo.

Figura 16

Recomendación de estructura empresarial para OMEGATELCOM S.A.



Fuente: Autoría

Gracias a una estructura empresarial estructurada la cual facilita la adaptación y mejora de los manuales de procesos en la empresa OMEGATELCOM S.A. Al tener roles y responsabilidades claramente definidos, se simplifica la documentación de procesos y procedimientos.

El manual de procesos que se presenta a continuación sigue la estructura del modelo de gestión FCAPS y se ha diseñado teniendo en cuenta las necesidades identificadas en la empresa. Este recurso está destinado a ser utilizado por el administrador de la red con el propósito de diagnosticar y solucionar inconvenientes.

4.3.1 Proceso para la Gestión en Fallos

Los procesos de Gestión de Fallos implementados se encuentran en el Anexo 2 para el manual de Manejo de Fallas se encuentra en el literal A con el código PROGA-001, Manejo de Incidentes se encuentra en el literal B con el código PROGA-002, Documentación de Fallos e Incidentes se encuentra en el literal C con el código PROGA-003 y Mesa de Servicio se encuentra en el literal D con el código PROGA-004. A continuación, se analiza cada uno de los procesos mencionados.

4.3.1.1 Manejo para Fallos

Este procedimiento tiene como objetivo establecer un marco para la identificación, manejo y resolución eficiente de fallas en la red de OMEGATELCOM, garantizando la continuidad del servicio y la satisfacción del cliente.

4.3.1.2 Manejo para Incidentes

La Gestión de Incidentes se centra en abordar eventos no planificados que impactan los servicios de red. La eficacia de este proceso radica en una identificación rápida, evaluación precisa y resolución oportuna de los incidentes para minimizar el impacto en los usuarios y garantizar la continuidad del servicio.

4.3.1.3 Documentación para Incidentes y Fallos

La Documentación de Fallos e Incidentes es esencial para analizar, aprender de experiencias pasadas y mejorar continuamente la gestión de la red. Este proceso se centra en recopilar, clasificar y archivar información detallada sobre fallos e incidentes para su posterior análisis y referencia.

4.3.1.4 Mesa de Servicio

La Mesa de Servicios es un componente esencial para gestionar eficientemente las solicitudes y problemas reportados por los usuarios. Este proceso se centra en recibir, registrar, clasificar y canalizar adecuadamente los incidentes y solicitudes de servicio.

4.3.2 Proceso para la Gestión de Configuración

Los procesos de Gestión de Configuración implementados se encuentran en el Anexo 2 para el manual de Ingreso de Equipos a la Red se encuentra en el literal E con el código PROGA-005 y Configuración de Equipos se encuentra en el literal F con el código PROGA-006. A continuación, se analiza cada uno de los procesos mencionados.

4.3.2.1 Ingreso de Dispositivos a la Red

El ingreso de equipos a la red es un proceso crítico para garantizar la seguridad y la eficiencia en la gestión de los activos de red. Este procedimiento abarca desde la solicitud de ingreso hasta la configuración y validación en la red.

4.3.2.2 Configuración de Dispositivos

La configuración de equipos es una fase crítica para garantizar el rendimiento óptimo y la seguridad en la red. Este procedimiento abarca desde la planificación de la configuración hasta la verificación de su correcta implementación.

4.3.3 Proceso para la Gestión de Contabilidad

Los procesos de Gestión de Contabilidad implementados se encuentran en el Anexo 2 para el manual de Inventario de Equipos se encuentra en el literal G con el código PROGA-007 y Uso de los Servicios de la Red se encuentra en el literal H con el código PROGA-008. A continuación, se analiza cada uno de los procesos mencionados.

4.3.3.1 Inventario de Dispositivos de la red

El inventario de equipos es esencial para mantener un control efectivo de los recursos en la red. Este procedimiento aborda desde la identificación de equipos hasta la actualización periódica del inventario.

4.3.3.2 Uso de los Servicios de la Red

Este procedimiento establece las actividades contables en OMEGATELCOM, siguiendo los lineamientos de la Recomendación M.3400 para garantizar la transparencia y precisión en el registro y control de recursos.

4.3.4 Proceso para la Gestión de Rendimiento

Los procesos de Gestión de Rendimiento implementados se encuentran en el Anexo 2 para el manual de Informe de Rendimiento se encuentra en el literal I con el código PROGA-009. A continuación, se analiza cada uno de los procesos mencionados.

4.3.4.1 Informe de Rendimiento de Dispositivos

Este procedimiento establece las actividades para generar informes de rendimiento en OMEGATELCOM, siguiendo buenas prácticas y la Recomendación M.3400 para evaluar y mejorar la eficiencia de los servicios.

4.3.5 Proceso para la Gestión de Seguridad

Los procesos de Gestión de Seguridad implementados se encuentran en el Anexo 2 para el manual de Acceso al Sistema de Red se encuentra en el literal J con el código PROGA-010. A continuación, se analiza cada uno de los procesos mencionados.

4.3.5.1 Acceso al Sistema de Red

Este procedimiento establece las medidas de seguridad y control de acceso al sistema de red de OMEGATELCOM para garantizar la confidencialidad, integridad y disponibilidad de la información.

4.4 Análisis de Resultados

En la fase de implementación de las políticas de gestión, manuales de procesos y la recomendación de la herramienta Zabbix en la infraestructura de OMEGATELCOM, se llevó a cabo un análisis de los diversos desafíos y problemas que enfrentaba la empresa. Para evaluar el impacto de estas implementaciones, se diseñó un cuadro que destaca los problemas identificados, las soluciones implementadas y los beneficios por obtener como resultado de estas acciones.

En el siguiente cuadro se visualiza de manera clara y estructurada cómo las medidas adoptadas han abordado los problemas clave en áreas críticas de la gestión de red como la gestión de fallos, la seguridad, la contabilidad, el rendimiento y la configuración. A través de este análisis, se busca demostrar cómo las estrategias aplicadas contribuirán a la mejora general del rendimiento, disponibilidad y administración de la red de OMEGATELCOM, proporcionando una visión clara de los resultados a lograr.

Tabla 7*Problema, Solución y Beneficio por obtener.*

Problema Identificado	Solución Implementada	Beneficios Por Obtener
1. Fallas recurrentes en la red	Implementación de políticas de manejo de fallos.	Reducción del tiempo de resolución de problemas.
	Configuración adecuada de equipos según políticas.	Menor impacto en la operación diaria.
	Uso de Zabbix para monitorizar y prevenir fallas.	Mayor visibilidad y alertas tempranas.
2. Problemas de seguridad	Establecimiento de políticas de seguridad robustas.	Reducción de intentos de acceso no autorizado.
	Implementación de capacitaciones en seguridad.	Respuesta rápida a problemas de seguridad.
	Uso de herramientas de seguridad recomendadas.	Mejora general en la postura de seguridad.
3. Ineficiencias en la contabilidad	Políticas de contabilidad en el manejo de los equipos en la red.	Control adecuado en la existencia y pérdida de equipos.
	Mejora en la transparencia de los registros financieros.	Identificación y reducción de costos innecesarios.
	Uso de herramientas recomendadas para contabilidad.	Información más clara sobre costos y tarifas.
4. Problemas de rendimiento	Políticas de gestión de rendimiento y calidad de servicio.	Mejora en la calidad y velocidad de los servicios.

	Monitoreo activo con Zabbix y otras herramientas.	Respuesta rápida ante problemas de rendimiento.
	Implementación de medidas preventivas identificadas.	Cumplimiento de expectativas de calidad de servicio.
5. Problemas de configuración	Establecimiento de políticas claras para la configuración.	Reducción de errores debido a configuraciones incorrectas.
	Procedimientos para resolver problemas de configuración.	Mejora en la estabilidad y consistencia de la red.

Fuente: Autoría

En este cuadro, cada problema identificado está asociado con las acciones tomadas para abordarlo y los beneficios que resultarán de la implementación de las soluciones. Esto proporcionará una visión clara de cómo las políticas, manuales y herramientas recomendadas contribuirán a mejorar la gestión de la red en OMEGATELCOM.

4.4.1 Optimización del Rendimiento, Disponibilidad y Administración en OMEGATELCOM

La implementación de las políticas de gestión, los manuales de procesos y la recomendación de Zabbix tendrá un impacto significativo en aspectos clave como el rendimiento, la disponibilidad y la administración de la red en OMEGATELCOM. A continuación, se detallan algunas de las estrategias y soluciones que contribuirán a mejorar estos aspectos:

Rendimiento:

Monitoreo Proactivo: Zabbix permite un monitoreo continuo y proactivo de los recursos de red, identificando posibles cuellos de botella y anomalías en tiempo real.

Análisis de Datos Históricos: Zabbix y los procesos proporcionan datos históricos detallados, facilitando la identificación de patrones de uso que realimentan a la planificación para mejorar el rendimiento.

Disponibilidad:

Gestión de Fallos Eficiente: Las políticas y procesos de gestión de fallos definirán procedimientos claros para la detección y resolución rápida de problemas, mejorando la disponibilidad de la red.

Configuración Redundante: Se implementaron configuraciones redundantes para garantizar la disponibilidad continua en caso de fallos.

Administración:

Automatización de Procesos: Manuales de procedimientos detallados y la herramienta Zabbix permitirán la automatización de numerosos procesos de administración, reduciendo la carga de trabajo manual.

Seguimiento y Documentación: Las políticas establecieron estándares para el seguimiento y documentación efectiva de cambios en la configuración, facilitando la administración a lo largo del tiempo.

La conjunción de estas estrategias resultará en una red más eficiente, resistente a fallos y gestionada de manera más efectiva, mejorando la experiencia operativa y la satisfacción del cliente en OMEGATELCOM.

CONCLUSIONES

La adopción del "Modelo de Gestión FCAPS de la ISO" en OMEGATELCOM S.A ha supuesto una transformación significativa en la forma en que la empresa gestionará su red. A través de la implementación de políticas claras, procesos eficientes y la recomendación de la herramienta de gestión Zabbix, se logrará mejoras sustanciales en el rendimiento, la disponibilidad y la administración de la infraestructura de red. Este enfoque permitirá a la empresa optimizar su rendimiento mediante la identificación proactiva y resolución de problemas, lo que se tradujo en una experiencia de usuario mejorada y tiempos de respuesta más rápidos.

La mejora en la disponibilidad de la red será evidente, gracias a una gestión más efectiva de los recursos y una reducción significativa en los períodos de inactividad. La implementación de políticas específicas de gestión de fallos e incidentes, respaldada por la recomendación de la herramienta Zabbix, fortalecerá la capacidad de respuesta ante situaciones críticas, asegurando una rápida identificación y resolución de problemas. Este enfoque también se tradujo en una administración más eficiente de los recursos, liberando tiempo y recursos para centrarse en iniciativas estratégicas.

La recomendación de la herramienta de gestión Zabbix en este proceso, proporcionará una visión integral de la red y facilitará una toma de decisiones informada. Su versatilidad y robustez demuestra ser crucial para el éxito de la implementación del modelo FCAPS. En conjunto, estos resultados destacan el impacto positivo y la eficacia de este enfoque integral en la gestión de redes empresariales, colocando a OMEGATELCOM S.A en una posición más fuerte y competitiva en el mercado.

RECOMENDACIONES

Basado en los resultados a obtener a través de la implementación del "Modelo de Gestión FCAPS de la ISO" en OMEGATELCOM S.A, respaldado por la adopción de políticas, procesos específicos y la herramienta de gestión Zabbix, se presentan las siguientes recomendaciones:

Se sugiere mantener un enfoque proactivo hacia la optimización continua de las políticas y procesos implementados. Esto implica la revisión periódica de los procedimientos, adaptándolos a los cambios en la infraestructura de red y en las demandas del mercado.

Se recomienda brindar capacitación constante al personal encargado de la gestión de la red. Esto incluye sesiones de formación sobre las mejores prácticas de uso de la herramienta Zabbix, así como la actualización en políticas y procedimientos para garantizar su correcta aplicación.

Es vital mantener un monitoreo constante del rendimiento de la red y la efectividad de las políticas implementadas. Esto se puede lograr mediante auditorías periódicas y revisiones de los informes generados por la herramienta Zabbix para identificar áreas de mejora y oportunidades de optimización.

Ante la evolución constante de las tecnologías de red, se sugiere la evaluación continua de nuevas soluciones y herramientas que puedan complementar o mejorar las capacidades actuales de la gestión de red. Esto garantizará la adaptabilidad de OMEGATELCOM frente a los avances tecnológicos.

Fortalecimiento de la Seguridad, dada la creciente importancia de la seguridad de la red, se recomienda fortalecer las políticas y procedimientos relacionados con la gestión de seguridad. Esto incluye la implementación de medidas proactivas y la actualización constante de las políticas de acceso y protección contra amenazas cibernéticas.

Se aconseja establecer canales de retroalimentación directa con los usuarios finales para evaluar su experiencia y satisfacción con los servicios de red. Esta retroalimentación puede ser valiosa para ajustar políticas y procedimientos según las necesidades y expectativas de los usuarios.

Considerando la dinámica del entorno empresarial y tecnológico, se sugiere una planificación estratégica a largo plazo. Esto implica anticipar posibles cambios en la infraestructura de red y adaptar las políticas y procesos en consecuencia.

GLOSARIO

ACL (Access Control List): Lista de Control de Acceso. Conjunto de reglas que especifican qué tráfico se permite o se niega en una red.

Ancho de Banda: Capacidad máxima de transmisión de datos en una red.

Cifrado: Proceso de codificación de datos para proteger la privacidad durante la transmisión.

CMIP (Common Management Information Protocol): Protocolo de Información de Gestión Común. Estándar de red para la gestión de dispositivos.

DNS (Domain Name System): Sistema de Nombres de Dominio. Traduce nombres de dominio legibles por humanos en direcciones IP.

Ethernet: Estándar de red de área local (LAN) que utiliza cables coaxiales o de fibra óptica.

FCAPS (Fault, Configuration, Accounting, Performance, Security): Framework que abarca cinco áreas fundamentales para la gestión de redes.

Firewall: Sistema de seguridad que controla el tráfico de red y protege contra amenazas.

Fibra Óptica: Medio de transmisión que utiliza hilos delgados de vidrio o plástico para enviar señales de luz.

IP Dinámica (Dynamic IP): Dirección IP asignada automáticamente por un servidor DHCP y puede cambiar con el tiempo.

IP Estática (Static IP): Dirección IP asignada manualmente y no cambia con el tiempo.

ISO (Organización Internacional de Normalización): Organismo que establece estándares internacionales en diversos campos, incluida la gestión de redes.

ISP (Proveedor de Servicios de Internet): Empresa que proporciona acceso a Internet a los usuarios.

ITU (Unión Internacional de Telecomunicaciones): Agencia especializada de las Naciones Unidas que se ocupa de cuestiones de tecnologías de la información y comunicación.

ITIL (Information Technology Infrastructure Library): Conjunto de prácticas recomendadas para la gestión de servicios de tecnología de la información.

Latencia: Retraso experimentado en la transmisión de datos.

Latencia de Propagación: Retardo causado por la distancia física entre el remitente y el destinatario.

Máscara de Subred: Número que separa la parte de red de la parte de host en una dirección IP.

MIMO (Entradas Múltiples, Salidas Múltiples): Tecnología que utiliza múltiples antenas para mejorar la transmisión y recepción de señales.

MIBs (Management Information Bases): Bases de Información de Gestión. Base de datos que almacena información de gestión de dispositivos de red.

NAT (Network Address Translation): Traducción de direcciones de red. Un método utilizado para cambiar las direcciones IP de los paquetes de datos que viajan a través de una red.

OID (Object Identifier): Identificador de Objeto. Número único que identifica un objeto gestionado en una MIB.

Protocolo de Comunicación: Conjunto de reglas que define cómo se transmiten datos entre dispositivos en una red.

Protocolo TCP/IP: Conjunto de protocolos que facilita la comunicación en Internet.

Proxy: Servidor intermedio que actúa como intermediario entre los usuarios y otros servidores.

Puerta de Enlace (Gateway): Dispositivo que conecta diferentes redes para dirigir el tráfico entre ellas.

QoS (Quality of Service): Calidad de servicio. Un conjunto de tecnologías y estándares diseñados para gestionar y mejorar el rendimiento de una red.

Router: Dispositivo que dirige el tráfico de datos entre redes.

Router Inalámbrico: Dispositivo que permite la conexión de dispositivos a una red sin necesidad de cables.

RPC (Remote Procedure Call): Llamada de Procedimiento Remoto. Protocolo que permite a un programa ejecutarse en otra computadora como si estuviera local.

Servidor: Computadora o sistema que proporciona servicios, recursos o datos a otras computadoras en la red.

Telecomunicaciones: Transmisión de información a distancia mediante señales eléctricas, ópticas o electromagnéticas.

TICs (Tecnologías de la Información y Comunicación): Conjunto de tecnologías utilizadas para el manejo y procesamiento de información.

Topología de Red: Configuración física o lógica de una red de comunicaciones.

VLAN (Virtual Local Area Network): Red de Área Local Virtual. Una red que agrupa dispositivos lógicamente, aunque puedan estar físicamente en ubicaciones diferentes.

VPN (Red Privada Virtual): Tecnología que crea una conexión segura a través de Internet para acceder a una red privada.

Wi-Fi: Tecnología que permite la conexión inalámbrica a redes de área local.

WPA (Wi-Fi Protected Access): Acceso Wi-Fi Protegido. Protocolo de seguridad para redes inalámbricas.

WPA2 (Wi-Fi Protected Access 2): Versión mejorada de WPA con mayores medidas de seguridad.

XML (Extensible Markup Language): Lenguaje de Marcado Extensible. Formato de archivo que define reglas para codificar documentos en un formato legible por humanos y máquinas.

4G y 5G: Generaciones de tecnología móvil que proporcionan mayor velocidad y capacidad de conexión.

Bibliografía

- (OGC), O. o. (2011). *ITIL Service Operation*. London: Crown Copyright 2007.
- Anttalainen, T. (2003). *Introduction to Telecommunications Network Engineering*. Norwood: Artech House.
- Arroyave Arredondo, A. (2013). *Implementación del área de seguridad del modelo FCAPS en la infraestructura de red en la alcaldía de Envigado*. Colombia: Institución Universitaria de Envigado.
- AWS, A. (17 de Julio de 2023). *Qué es la latencia de red*. Obtenido de AWS: <https://aws.amazon.com/es/what-is/latency/>
- Barba Martí, A. (14 de julio de 1999). *GESTIÓN DE RED EN OSI*. Obtenido de ujaen: <http://www4.ujaen.es/~mdmolina/grr/Tema%204.pdf>
- Barreto, J., & Patrón, J. (2008). *CONGESTIÓN EN LAS REDES DE DATOS*. CARTAGENA DE INDIAS, D. T. Y C: UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.
- Boutaba, R. y. (2001). *Proyectar FCAPS a redes activas*. En 2001 *Actas de la Conferencia de Redes Empresariales, Aplicaciones y Servicios*. IEEE.
- Burke, J. R. (2004). *Network Management: Concepts and Practice, A Hands-On Approach*. Upper Saddle River: Prentice Hall.
- Clemm, A. (2007). *Network Management Fundamentals*. Indianápolis: Cisco Press.
- Cloghrie, & Rose, M. T. (1991). *Concise MIB definitions*. RFC Editor.
- Czegel, B. (2015). *Running an Effective Help Desk*. Boston: Auerbach Publications.
- Del Pozo Barrezueta, H. (2015). *Ley Orgánica de Telecomunicaciones*. Quito.
- Enns, R., Björklund, M., Bierman, A., & Schönwälder, J. (30 de Junio de 2011). *RFC 6241: Network Configuration Protocol (NETCONF)*. Obtenido de IETF Datatracker: <https://datatracker.ietf.org/doc/html/rfc6241>
- Fedor, M., Schoffstall, M. L., Davin, J. R., & Case, J. D. (1 de Mayo de 1990). *RFC 1157: Simple network management protocol (SNMP)*. Obtenido de IETF Datatracker: <https://datatracker.ietf.org/doc/html/rfc1157>
- Gartner. (2022). *Coste del tiempo de inactividad de servicios: ¿cuánto le cuesta a tu empresa una interrupción informática?* Argentina: invgate.
- Goyal, P. M. (2009). *FCAPS en el modelo de tejido de servicios empresariales*. En 2009, *18 talleres internacionales del IEEE sobre tecnologías habilitadoras: infraestructuras para empresas colaborativas*. IEEE.

- Hermosa Torres, R. L. (2015). *Modelo de gestión de red basado en el modelo de gestión FCAPS de la ISO que permita mejorar la disponibilidad y rendimiento de la red de la empresa JASSA TELECOM*. Ibarra: UTN.
- Huston, G. (1995). *ISP Survival Guide: Strategies for Running a Competitive ISP*. New York: Wiley.
- Huston, G. (1998). *The ISP Survival Guide: Strategies for Running a Competitive ISP*. San Francisco: Addison-Wesley.
- ITU-T. (1993). *X.700 Marco de gestión para la interconexión de sistemas abiertos para aplicaciones del CCITT*. Obtenido de Unión Internacional de Telecomunicaciones: <https://www.itu.int/rec/T-REC-X.700-199209-I/es>
- Johnson, M. (2019). *Network Performance Optimization: Strategies and Techniques*. Editorial IT Solutions.
- Kurose, J. F. (2017). *Redes informáticas: un enfoque de arriba hacia abajo*. Pearson.
- libreNMS. (09 de Septiembre de 2023). *Documentos de LibreNMS*. Obtenido de <https://docs.librenms.org/Support/Features/>
- Manolo. (2005). *Modelos de Gestión de red*. España: Unirversidad de Vigo.
- Michael E. Whitman, H. J. (2018). *Principles of Information Security*. Boston: Cengage Learning.
- Molero, L. (2010). *Planificación y Gestión de Red*. Maracaibo: Universidad "Dr. Rafael Belloso Chacín.
- Morris, C. (2018). *Network Configuration Management: Best Practices and Tools*. Editorial Networking World.
- Nagios. (28 de Abril de 2020). *Nagios Documentos*. Obtenido de <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html#whatis>
- Pérez, E. D. (2019). *Implementación de una Herramienta de Monitoreo de la Red Universitaria*. Mexico: UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO.
- Peterson, L. (2017). *Network Fault Management and Troubleshooting Guide*. Editorial TechPress.
- Redmond, J. (2020). *Network Security: Concepts and Best Practices*. Editorial Cyber Defense.
- Rose, M. T., & McCloghrie, K. (14 de Julio de 2023). *MIBs*. Obtenido de Cinvestav.mx.: <https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf>

- Stallings, W. (2013). *Administración de redes: principios y práctica*. Pearson.
- Suarez-Tapia, J. C., Carvajal-Gómez, B. E., & Carreto-Arellano, C. (2015). *Transmisión de video simultaneo en ancho de banda limitado aplicando esteganografía*. Ciudad de Mexico: Universidad Tecnológica de México.
- Subramanian, M. (2000). *Network Management: Principles and Practice*. Boston: Addison-Wesley.
- Tanenbaum, A. S. (2011). *Redes de computadoras (5ª ed.)*. Pearson Educación.
- Terán Escanta, J. G. (2020). *Sistema de gestión de configuración para la infraestructura de Networking de la empresa pública YACHAY E.P.* Ibarra: UTN.
- Torres Chicaiza, L. E. (2015). *Administración y gestión de la red inalámbrica del gobierno autónomo descentralizado (GADIP) del cantón Cayambe basada en el modelo funcional FCAPS de la ISO*. Ibarra: UTN.
- X.137, U.-T. (2021). *Valores de disponibilidad para redes públicas*. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES.
- Zabbix, S. (7 de Marzo de 2023). *Zabbix Documentation*. Obtenido de <https://www.zabbix.com/documentation/current/es/devel>
- ZTE. (2013). *ZXA10 C300 Datasheet - GPON ZTE*. Shenzhen: ZTE Corporation.

ANEXOS

Anexo 1: Formato de Encuestas

A. Encuesta dirigida al personal de la empresa OMEGATELCOM S.A



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Encuesta dirigida al Personal de la Empresa OMEGATELCOM S.A

A través de esta encuesta, se busca recopilar información detallada y fundamentada sobre cada una de las áreas de gestión FCAPS: Fault (Fallas), Configuration (Configuración), Accounting (Contabilidad), Performance (Rendimiento) y Security (Seguridad). Esto permitirá una evaluación técnica de la red, desde la detección y resolución de fallas hasta la configuración, la contabilidad precisa de recursos, la optimización del rendimiento y la seguridad de la red.

La información obtenida servirá como un recurso valioso para el desarrollo del proyecto " MODELO DE GESTIÓN FCAPS DE LA ISO PARA MEJORAR EL RENDIMIENTO, DISPONIBILIDAD Y ADMINISTRACIÓN DE LA RED DE LA EMPRESA OMEGATELCOM S.A," ya que proporcionará datos técnicos que respaldarán la toma de decisiones en cada una de las áreas de gestión.

De acuerdo con las instrucciones, la persona entrevistada debe responder cada pregunta con honestidad

PREGUNTAS

Área de Fault Management (Gestión de Fallas):

#	Pregunta	SI	No	Tal vez
1	¿Crees que sus procedimientos de detección y resolución de fallas en la red son efectivos?			
2	¿Se comunica de manera eficiente la información sobre las fallas en la red?			
3	¿Se abordan de manera oportuna las fallas en la red?			
4	¿Se realizan pruebas de recuperación y contingencia para prevenir futuras fallas?			
5	¿Hay transparencia y comunicación efectiva sobre las fallas que afectan nuestros servicios?			

Área de Configuration Management (Gestión de Configuración):

#	Pregunta	SI	No	Tal vez
1	¿Los procedimientos de configuración de la red son claros y fáciles de seguir?			
2	¿Has experimentado problemas debido a errores de configuración en la red?			
3	¿La documentación y seguimiento de cambios de configuración son adecuados?			
4	¿Se resuelve de manera inmediata problemas de configuración?			
5	¿Existe buena colaboración entre los equipos de configuración en la red?			

Área de Accounting Management (Gestión de Contabilidad):

#	Pregunta	SI	No	Tal vez
---	----------	----	----	---------

1	¿Te sientes informado sobre los costos y tarifas asociados a los servicios que ofrecemos?			
2	¿Has notado problemas en el registro de recursos utilizados en la red?			
3	¿Es precisa la facturación de servicios?			
4	¿Tienes ideas para reducir costos innecesarios en sus operaciones?			
5	¿La empresa tiene transparencia en el registro de actividades y gastos?			

Área de Performance Management (Gestión de Rendimiento):

#	Pregunta	SI	No	Tal vez
1	¿La calidad y velocidad de nuestros servicios de Internet y telecomunicaciones cumplen con tus expectativas?			
2	¿Has experimentado congestión en la red que afecte el rendimiento?			
3	¿Se visualiza de forma gráfica el rendimiento del sistema?			
4	¿La monitorización de la red y el rendimiento son efectivos?			
5	¿Se están cumpliendo con las expectativas de calidad de servicio?			

Área de Security Management (Gestión de Seguridad):

#	Pregunta	SI	No	Tal vez
1	¿Sientes que la red está adecuadamente protegida contra amenazas de seguridad cibernética?			
2	¿Has experimentado intentos de acceso no autorizado a la red?			
3	¿Crees que las políticas de seguridad son efectivas para proteger la red?			
4	¿Tienen capacitaciones en seguridad?			
5	¿Se ha resuelto de manera rápida problemas de seguridad?			

Enlace de encuesta: https://docs.google.com/forms/d/e/1FAIpQLSe7OI3eg_QvIqMSxjOVxd-ETZ044hgF_ndUAVqjdWuhiJfvXA/viewform

Realizado por
Jhonatan Jacome

Revisado y Aprobado por
ING. Edgar Jaramillo

B. Encuesta dirigida a los usuarios de la empresa OMEGATELCOM S.A



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Encuesta dirigida a los usuarios de la empresa OMEGATELCOM S.A

Esta encuesta está diseñada para recopilar su opinión y experiencia en relación con la futura implementación del Modelo de gestión FCAPS en los servicios de telecomunicaciones de OMEGATELCOM S.A. Su participación es esencial, ya que ayudará a entender diversos aspectos, desde la calidad del servicio hasta la rapidez en la resolución de problemas. Su comentario ayudará directamente en la toma de decisiones futuras y contribuirán a fortalecer la calidad de los servicios que se ofrece.

De acuerdo con las instrucciones, la persona debe responder cada pregunta con honestidad.

PREGUNTAS

#	Pregunta	SI	No	Tal vez
1	¿El servicio de internet de OMEGATELCOM cumple con sus expectativas de calidad?			
2	¿Experimenta interrupciones frecuentes en su conexión de internet?			
3	¿Considera que los problemas técnicos relacionados con su servicio de internet se resuelven rápidamente?			
4	¿Ha experimentado demoras significativas en la resolución de problemas previos?			
5	¿Puede identificar fallas comunes en su servicio de internet?			
6	¿Recibe notificaciones oportunas sobre fallas o interrupciones planificadas en su servicio de internet?			
7	¿Se siente satisfecho con la forma en que se resuelven los problemas en su servicio de internet?			
8	¿La información sobre el estado de las fallas es transparente?			
9	¿El soporte técnico está disponible y accesible cuando surge un problema?			
10	¿Ha notado una mejora en la prontitud de respuesta del soporte técnico con el tiempo?			
11	¿Las configuraciones de su servicio de internet son consistentes y bien gestionadas?			
12	¿Ha experimentado problemas relacionados con configuraciones incorrectas?			
13	¿Está generalmente satisfecho con el servicio de internet proporcionado por OMEGATELCOM?			


Enlace de encuesta: <https://forms.gle/qkwx9BpS4WpGsqzx7>

Realizado por
Jhonatan Jacome

Revisado y Aprobado por
ING. Edgar Jaramillo

Anexo 2: Manuales de las políticas de gestión para la empresa OMEGATELCOM

A. Principios de las Políticas de Gestión de Red

EMPRESA OMEGATELCOM S.A.		
	1. Políticas de gestión de red	
	Política:	1.1 Objetivos de las Políticas de Gestión de Red
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0001
	Versión:	1.0
<p>Pol. 1. Proporcionar a los responsables de la gestión de la red y al administrador de la red, la información necesaria acerca de las políticas y procedimientos que deben seguirse con el fin de asegurar el funcionamiento adecuado de la red.</p> <p>Pol. 2. Comunicar de manera clara a los usuarios recién incorporados que están accediendo a los servicios de la red, la información indispensable para que puedan utilizar los servicios de manera adecuada.</p> <p>Pol. 3 Establecer medidas y directrices para salvaguardar los intereses de la empresa en el contexto de su red de telecomunicaciones.</p>		


Fuente: Autoría

B. Compromiso por parte de las Autoridades

EMPRESA OMEGATELCOM S.A.		
	1. Políticas de gestión de red	
	Política:	1.2 Compromiso por parte de las Autoridades
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0002
	Versión:	1.0
<p>Pol. 4 El Area de Tecnologías y Comunicación (TIC’s) de OMEGATELCOM, en calidad de administrador de la red de telecomunicaciones y fundador de las políticas de gestión, asume la puesta en marcha de implementar e informar los parámetros de este documento.</p> <p>Pol. 5 Las autoridades de OMEGATELCOM se comprometen a supervisar de manera activa la implementación y cumplimiento de las políticas de gestión de red.</p> <p>Pol. 6 Se compromete a asignar los recursos indispensables, tanto monetarios como técnicos, para la implementación efectiva de las políticas de gestión de red.</p>		


Fuente: Autoría

C. Políticas para el Manejo para Fallos

EMPRESA OMEGATELCOM S.A.	
	2. Políticas de Gestión de Fallas
	Política: 2.1 Manejo para Fallas
	Revisado por: Ing. Javier Lema “Administrador de red”
	Código: PLOGA-0003
	Versión: 1.0
<p>Pol. 7 El administrador de red deberá detectar la falla en la red mediante la herramienta de gestión, ya sea a través de una llamada o un mensaje al personal.</p> <p>Pol. 8 Todas las fallas detectadas se clasificarán y priorizarán según su impacto en los servicios y la infraestructura. Esto garantizará que se aborden primero las fallas críticas para minimizar el tiempo de inactividad y optimizar la eficiencia operativa.</p> <p>Pol. 9 Todas las fallas detectadas serán registradas y documentadas detalladamente. Esto incluirá información sobre la naturaleza de la falla, tiempo de detección, tiempo de resolución y cualquier acción correctiva tomada. La documentación servirá como base para análisis y mejora continua.</p> <p>Pol. 10 Al existir una nueva falla, se debe documentar el fallo y el procedimiento de solución entre las personas que ayudaron en la falla.</p>	

Fuente: Autoría

D. Políticas para el Manejo para Incidentes

EMPRESA OMEGATELCOM S.A.		
	3. Políticas de Gestión de Fallas	
	Política:	2.2 Manejo para Incidentes
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0004
	Versión:	1.0

Pol. 11 Se establece la definición clara de lo que constituye un incidente en el contexto de la red de OMEGATELCOM. Esto incluirá eventos no deseados, interrupciones de servicio y cualquier situación que pueda cambiar la operación normal de la red.

Pol. 12 Se establecerá un proceso de reporte inmediato para que cualquier miembro del personal que detecte un incidente lo informe de inmediato al equipo de gestión de incidentes. La rapidez en la notificación es crucial para una respuesta eficiente.

Pol. 13 Todos los incidentes serán clasificados y priorizados según su gravedad y consecuencias potenciales. Esto permitirá asignar recursos de manera efectiva, centrándose primero en resolver aquellos incidentes que tienen un mayor impacto en la operación y la seguridad.

Tipo de Fallo	Prioridad	Tiempo de Solución
Falla de Red	Critico	Dentro de 1 hora
Caída de Servicio	Critico	Dentro de 1 hora
Problemas de Seguridad	Alto	Dentro de 2 horas
Fallos en Equipos Críticos	Alto	Dentro de 2 horas
Problemas de Conectividad	Media	Dentro de 4 horas
Errores de Configuración	Baja	Dentro de 8 horas
Dispositivo Funcionando	Baja	Dentro de 24 horas

Pol. 14 Se debe establecer equipos de respuestas a incidentes (IRT) que estará disponible las 24 horas para abordar incidentes críticos. Este equipo tiene que estar estructurado por personal capacitado y experimentado en la resolución de incidentes de seguridad y operacionales.


Pol. 15 Todos los incidentes serán objeto de una investigación para entender la causa subyacente. Se llevará a cabo un análisis post-incidente con el cual podamos identificar lecciones aprendidas y medidas preventivas para prevenir incidentes futuros.

Pol. 16 Se establecerá un protocolo de notificación y comunicación para informar a todas las partes interesadas relevantes sobre la naturaleza y el impacto de un incidente. La transparencia en la comunicación es esencial para mantener la confianza del cliente y las autoridades.

Pol. 17 El personal involucrado en la gestión de incidentes recibirá capacitación regular y participará en simulacros para garantizar que estén preparados para abordar incidentes de manera efectiva y coordinada.

Fuente: Autoría


E. Políticas para la Documentación de Incidentes y Fallos

EMPRESA OMEGATELCOM S.A.		
	2. Políticas de Gestión de Fallas	
	Política:	2.3 Documentación para Incidentes y Fallas
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA -0005
	Versión:	1.0
<p>Pol. 18 Todo fallo o incidente identificado deberá ser registrado de manera detallada en un sistema de registro centralizado. Esto incluirá información como la hora de detección, la naturaleza del fallo o incidente, los pasos tomados para abordarlo y cualquier solución implementada</p> <p>Pol. 19 Los fallos e incidentes serán categorizados de acuerdo con su naturaleza y gravedad. Esto permitirá una organización efectiva de la información y facilitará la posterior análisis y generación de informes.</p> <p>Pol. 20 Se designarán roles y responsabilidades claros para la documentación de fallos e incidentes. Cada miembro del equipo tendrá la responsabilidad de documentar adecuadamente cualquier evento.</p> <p>Pol. 21 El acceso a la documentación de fallos e incidentes estará controlado y restringido a personal autorizado.</p> <p>Pol. 22 La documentación se actualizará de manera continua a medida que se desarrolla la gestión de fallos e incidentes.</p> <p>Pol. 23 Después de la resolución de un fallo o incidente, se llevará a cabo un análisis posterior que incluirá una revisión de la documentación. Este análisis ayudará a identificar áreas de mejora y a perfeccionar los procedimientos para futuros eventos similares.</p>		

Pol. 24 La documentación de fallos e incidentes se respaldará de manera segura para asegurar su disponibilidad en caso de pérdida de datos.

Fuente: Autoría

F. Políticas para la Mesa de Servicio

EMPRESA OMEGATELCOM S.A.	
	2. Políticas de Gestión de Fallas
	Política: 2.4. Mesa de Servicio
	Revisado por: Ing. Javier Lema “Administrador de red”
	Código: PLOGA-0006
	Versión: 1.0
<p>Pol. 25 La mesa de servicio estará operativa las 24 horas del día, los 7 días de la semana, para garantizar la atención ininterrumpida de los usuarios y la gestión de eventos en la red.</p> <p>Pol. 26 El servicio al cliente debe ser rápido, por lo cual debe ser respaldado por herramientas tecnológicas de fácil interacción como: llamada telefónica, redes sociales entre otras.</p> <p>Pol. 27 La mesa de servicio debe intentar resolver los problemas de forma remota, antes de realizar una visita técnica.</p> <p>Pol. 28 La mesa de servicio mantendrá una comunicación transparente y continua con los usuarios afectados.</p> <p>Pol. 29 La mesa de servicio realizará un seguimiento continuo de los incidentes desde su recepción hasta su resolución.</p> <p>Pol. 30 Todas las acciones tomadas para resolver incidentes serán registradas de manera detallada.</p>	


Fuente: Autoría

G. Políticas para Ingresar Dispositivos a la Red

EMPRESA OMEGATELCOM S.A.		
	3. Políticas de Gestión de Configuraciones	
	Política:	3.1 Ingreso de Dispositivos a la Red
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0007
	Versión:	1.0
<p>Pol. 31 Los equipos que desee ser conectado a la red de OMEGATELCOM debe contar con la aprobación previa del área de Tecnologías de la Información y Comunicación (TIC).</p> <p>Pol. 32 Todos los componentes que forman parte de la red serán registrados en un sistema de inventario y de igual manera los nuevos equipos.</p> <p>Pol. 33 El tráfico generado por los nuevos equipos será monitoreado de manera continua para detectar posibles anomalías.</p>		


Fuente: Autoría

H. Políticas para la Configuración de Dispositivos

EMPRESA OMEGATELCOM S.A.		
	4. Políticas de Gestión de Configuraciones	
	Política:	3.2 Configuración de Dispositivos
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0008
	Versión:	1.0
<p>Pol. 34 Todos los equipos conectados a la red de OMEGATELCOM deberán seguir estándares de configuración establecidos por el departamento de Tecnologías de la Información y Comunicación (TIC).</p> <p>Pol. 35 Antes de realizar cambios en la configuración de cualquier equipo, se realizará un respaldo completo de las configuraciones existentes.</p> <p>Pol. 36 Antes de implementar cambios significativos en la configuración de equipos críticos, se requerirá una revisión y aprobación por parte del equipo de TIC.</p> <p>Pol. 37 El acceso a las configuraciones de los equipos estará restringido a personal autorizado.</p> <p>Pol. 38 Todo cambio de configuración realizada de ser documentada.</p> <p>Pol. 39 El personal responsable de la configuración de equipos recibirá capacitación continua sobre las políticas y procedimientos vigentes de la organización.</p>		


Fuente: Autoría

I. Políticas para el Inventario de Dispositivos

EMPRESA OMEGATELCOM S.A.		
	4. Políticas de Gestión de Contabilidad	
	Política:	4.1 Inventario de Dispositivos
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0009
	Versión:	1.0
<p>Pol. 40 Se mantendrá un registro detallado de todos los equipos gestionados en la red de OMEGATELCOM. Este registro incluirá información específica, como el tipo de equipo, número de serie, fecha de adquisición, y ubicación física.</p> <p>Pol. 41 El inventario se actualizará de forma continua para reflejar los cambios en la red. Cualquier adición, modificación o retiro de equipos será registrada de manera inmediata para garantizar la precisión de la información.</p> <p>Pol. 42 Se realizarán auditorías periódicas del inventario para verificar su precisión.</p> <p>Pol. 43 Los equipos dados de baja o retirados de la red serán debidamente documentados en el inventario.</p> <p>Pol. 44 El acceso al inventario estará restringido a personal autorizado.</p>		


Fuente: Autoría

J. Políticas para el Uso de los Servicios de Red

EMPRESA OMEGATELCOM S.A.		
	4. Políticas de Gestión de Contabilidad	
	Política:	4.2 Uso de los Servicios de Red
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0010
	Versión:	1.0
<p>Pol. 45 Implementar sistemas de medición de la utilización que capturen de manera precisa y oportuna la cantidad de recursos de red utilizados por cada cliente.</p> <p>Pol. 46 Realizar auditorías periódicas para garantizar la confiabilidad de los datos de medición de utilización.</p> <p>Pol. 47 Establecer políticas claras de tarificación basadas en los costos de la prestación de servicios y considerando la demanda del mercado.</p> <p>Pol. 48 Revisar periódicamente las estructuras de precios para garantizar la competitividad y la alineación con los objetivos financieros.</p> <p>Pol. 49 Establecer procedimientos eficientes de facturación y cobro para asegurar una gestión financiera efectiva.</p> <p>Pol. 50 Implementar mecanismos para gestionar de manera adecuada los pagos pendientes y reducir los riesgos de incumplimiento.</p> <p>Control de la Empresa:</p> <p>Pol. 51 Establecer controles internos sólidos para garantizar la integridad de los datos financieros y de contabilidad.</p> <p>Pol. 52 Realizar auditorías regulares de los procesos de gestión de la contabilidad para cumplir con las normativas y estándares.</p>		


Fuente: Autoría

K. Políticas para el Informe de Rendimiento de Dispositivos

EMPRESA OMEGATELCOM S.A.		
	5. Políticas de Gestión de Rendimiento	
	Política:	5.1 Informe de Rendimiento de Dispositivos
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0011
	Versión:	1.0
<p>Pol. 53 Todos los equipos gestionados en la red de OMEGATELCOM serán sometidos a monitoreo continuo para evaluar su rendimiento. Esto incluirá aspectos como velocidad capacidad entre otros.</p> <p>Pol. 54 Se establecerán claramente los parámetros y métricas de rendimiento que se medirán en cada equipo. Estos parámetros pueden incluir tiempo de respuesta, ancho de banda utilizado, latencia, entre otros.</p> <p>Pol. 55 Se configurarán alertas automáticas para notificar al personal de TI sobre cualquier degradación significativa en el rendimiento de los equipos.</p> <p>Pol. 56 Se realizarán revisiones periódicas del rendimiento de los equipos. Estas revisiones pueden incluir evaluaciones programadas, revisiones mensuales o auditorías específicas, según sea necesario.</p> <p>Pol. 57 Se realizará los reportes según la información que necesite por el administrador o las requeridas por la empresa.</p>		

Fuente: Autoría

L. Políticas para el Acceso al Sistema de Red

EMPRESA OMEGATELCOM S.A.		
	6. Políticas de Gestión de Seguridad	
	Política:	6.1 Acceso al Sistema de Red
	Revisado por:	Ing. Javier Lema “Administrador de red”
	Código:	PLOGA-0012
	Versión:	1.0
<p>Pol. 58 Todos las personas que accedan al sistema de administración de red deberán autenticarse mediante credenciales únicas.</p> <p>Pol. 59 Se asignarán roles y permisos específicos a cada usuario según sus responsabilidades y funciones.</p> <p>Pol. 60 Se implementará una política robusta de contraseñas que incluirá requisitos de longitud, complejidad y caducidad. Los usuarios serán responsables de mantener contraseñas seguras y cambiarlas periódicamente.</p> <p>Pol. 61 Se mantendrá un registro detallado de todos los accesos al sistema de administración de la red. Este registro incluirá información sobre el usuario, la hora de acceso, las acciones realizadas y cualquier intento de acceso no autorizado.</p> <p>Pol. 62 Se realizarán auditorías periódicas del sistema de gestión de red para identificar y abordar cualquier vulnerabilidad en el acceso.</p> <p>Pol. 63 Se implementará un proceso regular de actualización y aplicación de parches de seguridad en todos los sistemas y aplicaciones para mantener la resistencia contra vulnerabilidades conocidas</p>		

Pol. 64 Los dispositivos móviles que acceden al sistema estarán sujetos a políticas de seguridad que incluyan la protección con PIN, cifrado y la habilidad de borrar datos de forma remota en caso de pérdida.

Pol. 65 Se establecerá un plan de respuesta a incidentes que defina roles en caso de violaciones de seguridad, garantizando una acción rápida y efectiva.

Pol. 66 Establecer procedimientos claros para desconectar rápidamente a usuarios o dispositivos en caso de una amenaza inminente.


Pol. 67 Se implementarán herramientas de monitoreo para encontrar actividades sospechosas y responder proactivamente a posibles amenazas.

Pol. 68 Todo el personal con acceso al sistema de red recibirá capacitación en prácticas de seguridad, conciencia sobre amenazas y procedimientos seguros de acceso.

Fuente: Autoría

Anexo 3: Manuales de Procesos de Gestión para la empresa OMEGATELCOM S.A

A. Proceso de Manejo para Fallos

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Fallos		
	Dirigido a:	Administrador de la red
	Proceso:	Manejo para Fallos
	Año de elaboración:	2024
	Código:	PROGA-001

Descripción:

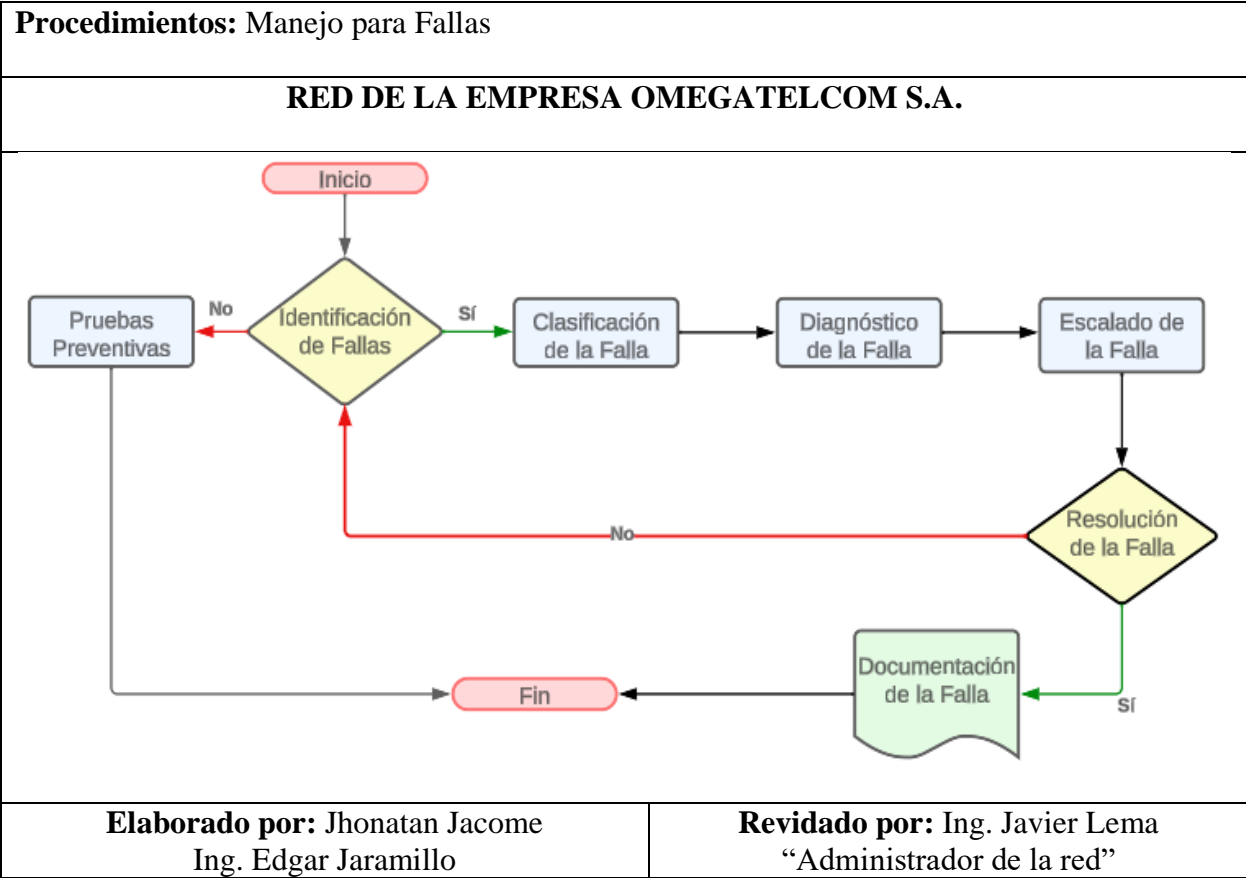
Este procedimiento tiene como objetivo establecer un marco para la identificación, manejo y resolución eficiente de fallas en la red de OMEGATELCOM, garantizando la continuidad del servicio y la satisfacción del cliente.

Detalle del Proceso


Actividad	Detalle	Área Responsable
1. Identificación de Fallas	Recepción y análisis de reportes de fallas por parte de usuarios o monitoreador de la red.	Mesa de Servicio
2. Clasificación de la Falla	Categorización de la falla según su naturaleza y gravedad.	Mesa de servicio
3. Diagnóstico de la Falla	Análisis detallado para determinar la causa de la falla.	Mesa de Servicio
4. Escalado de la Falla	En caso de necesitar la intervención de equipos especializados, se realiza el escalado adecuado.	Administrador de Red, Soporte Técnico

5. Resolución de la Falla	Implementación de medidas correctivas para solucionar la falla y restaurar el servicio.	Administrador de Red, Soporte Técnico
6. Documentación de la Falla	Registro detallado de la falla, acciones tomadas y soluciones aplicadas para futuras referencias.	Mesa de Servicio

Diagrama de Flujo



B. Proceso de Manejo para Incidentes

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Fallos		
	Dirigido a:	Administrador de la red
	Proceso:	Manejo para Incidentes
	Año de elaboración:	2024
	Código:	PROGA-002

Descripción

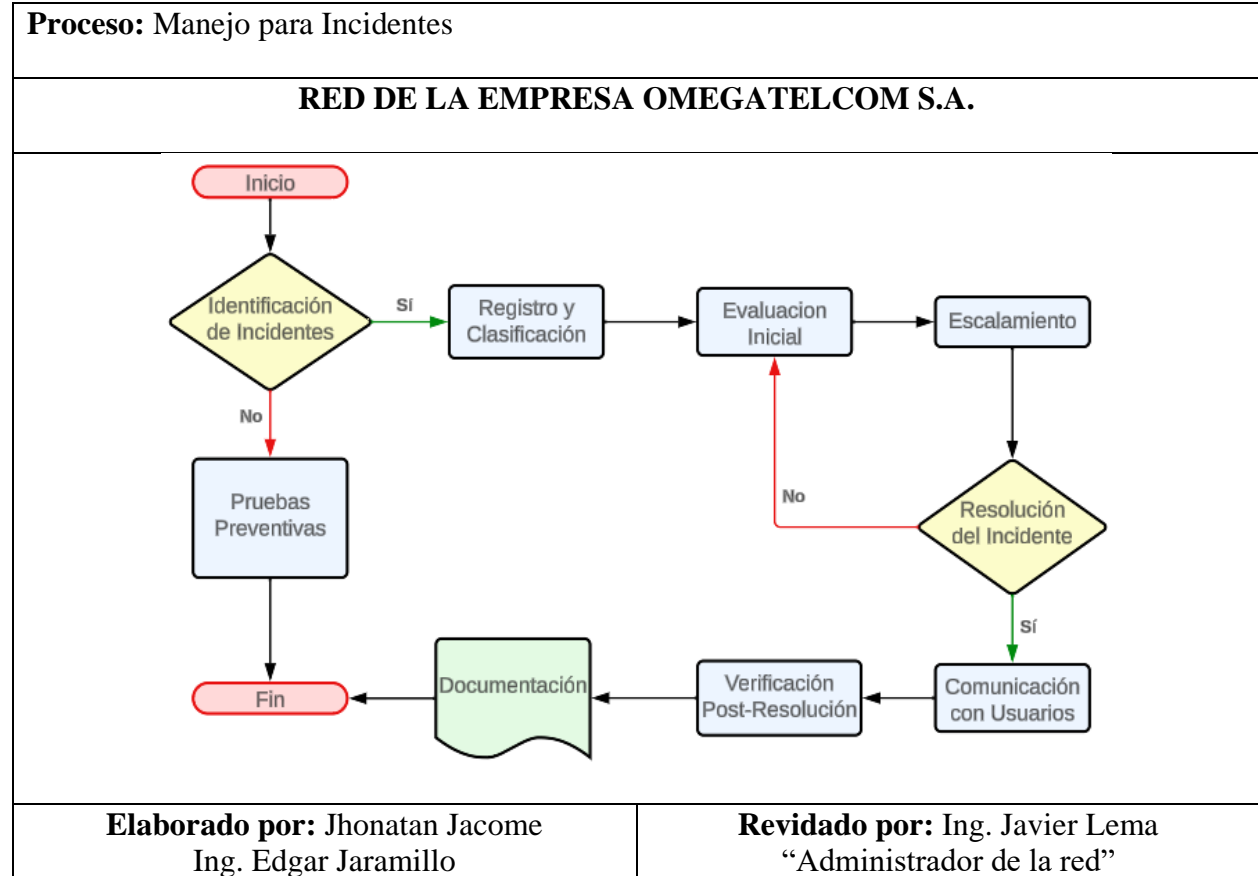
La Gestión de Incidentes se centra en abordar eventos no planificados que impactan los servicios de red. La eficacia de este proceso radica en una identificación rápida, evaluación precisa y resolución oportuna de los incidentes para reducir al mínimo el impacto en los abonados y garantizar la continuidad del servicio.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Identificación de Incidentes	Los incidentes se pueden detectar mediante monitoreo constante, informes de usuarios, o alertas automáticas del sistema.	Mesa de Servicio
2. Registro y Clasificación	Cada incidente se registra con detalles específicos y se clasifica según su naturaleza y prioridad.	Mesa de Servicio
3. Evaluación Inicial	Se realiza una evaluación inicial para comprender la magnitud y urgencia del incidente.	Equipo Técnico
4. Escalamiento	Según la gravedad, los incidentes se escalan y	Mesa de Servicio

	notifican a los equipos especializados correspondientes.	
5. Resolución del Incidente	Se implementan medidas correctivas para abordar y resolver el incidente de manera eficiente.	Equipo Técnico Especializado
6. Comunicación con Usuarios	Se mantiene una comunicación transparente con los usuarios afectados, proporcionándoles actualizaciones y estimaciones de resolución.	Mesa de servicio
7. Verificación Post-Resolución	Después de la resolución, se realiza una verificación para asegurar que el incidente se haya corregido satisfactoriamente.	Equipo Técnico
8. Documentación	Todos los pasos del proceso y los detalles del incidente se documentan cuidadosamente para análisis y mejora continua.	Mesa de Servicio

Diagrama de Flujo



C. Proceso de Documentación para de Incidentes y Fallos

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Fallos		
	Dirigido a:	Administrador de la red
	Proceso:	Documentación de para Incidentes y fallos
	Año de elaboración:	2024
	Código:	PROGA-003

Descripción

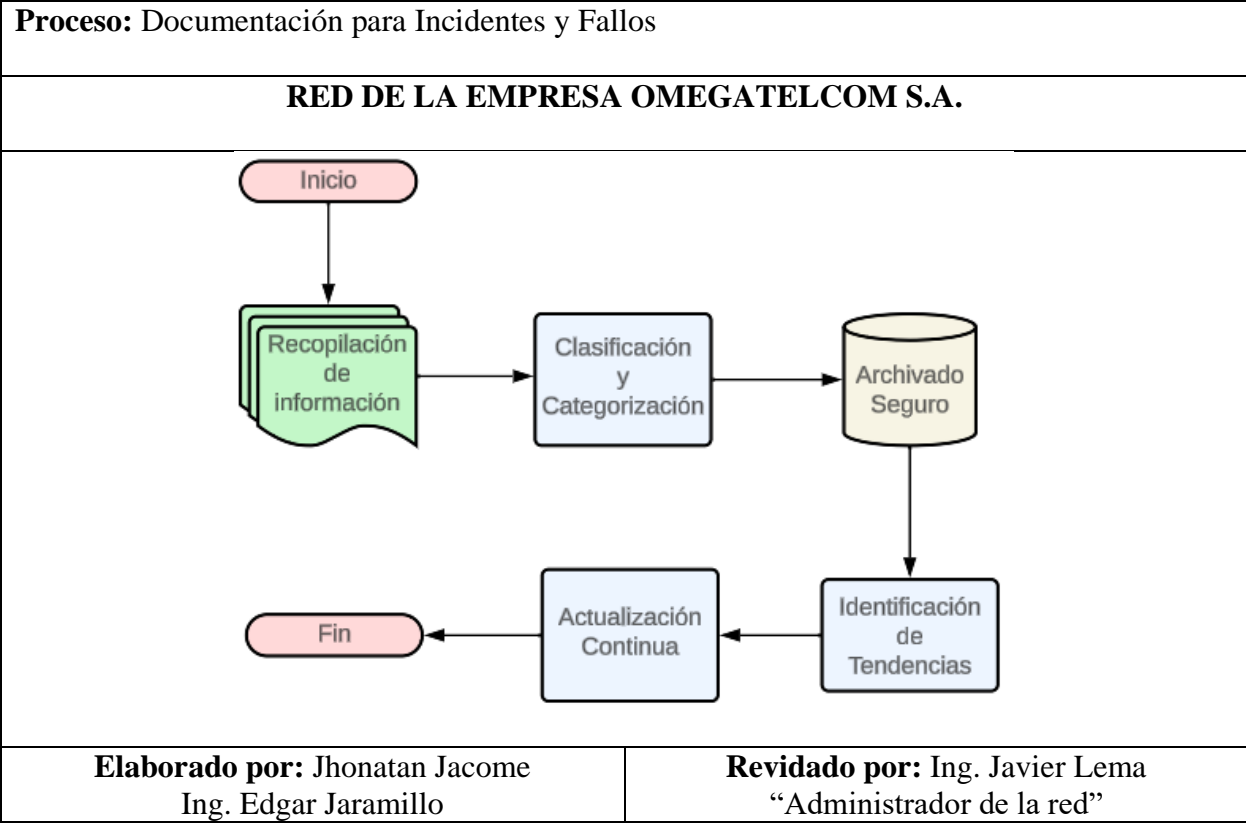
La Documentación de Fallos e Incidentes es esencial para analizar, aprender de experiencias pasadas y mejorar continuamente la gestión de la red. Este proceso se centra en recopilar, clasificar y archivar información detallada sobre fallos e incidentes para su posterior análisis y referencia.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Recopilación de información	Toda la información relevante sobre fallos e incidentes se recopila, incluyendo descripción, impacto, acciones tomadas y resultados.	Mesa de Servicio
2. Clasificación y Categorización	Se clasifican los fallos e incidentes según su naturaleza y se categorizan para facilitar la recuperación y análisis.	Equipo Técnico
3. Archivado Seguro	La información recolectada se almacena de forma protegida y accesible para aquellos que necesiten revisarla.	Responsable de Documentación

4. Identificación de Tendencias	Se realiza un análisis periódico de los registros para identificar patrones o tendencias que puedan requerir medidas preventivas.	Administrador de Red
5. Actualización Continua	Los registros se actualizan regularmente para reflejar el estado más reciente de la red y sus eventos.	Mesa de Servicio

Diagrama de Flujo



D. Proceso de Mesa de Servicio

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Fallos		
	Dirigido a:	Administrador de la red
	Proceso:	Mesa de Servicio
	Año de elaboración:	2024
	Código:	PROGA-004

Descripción

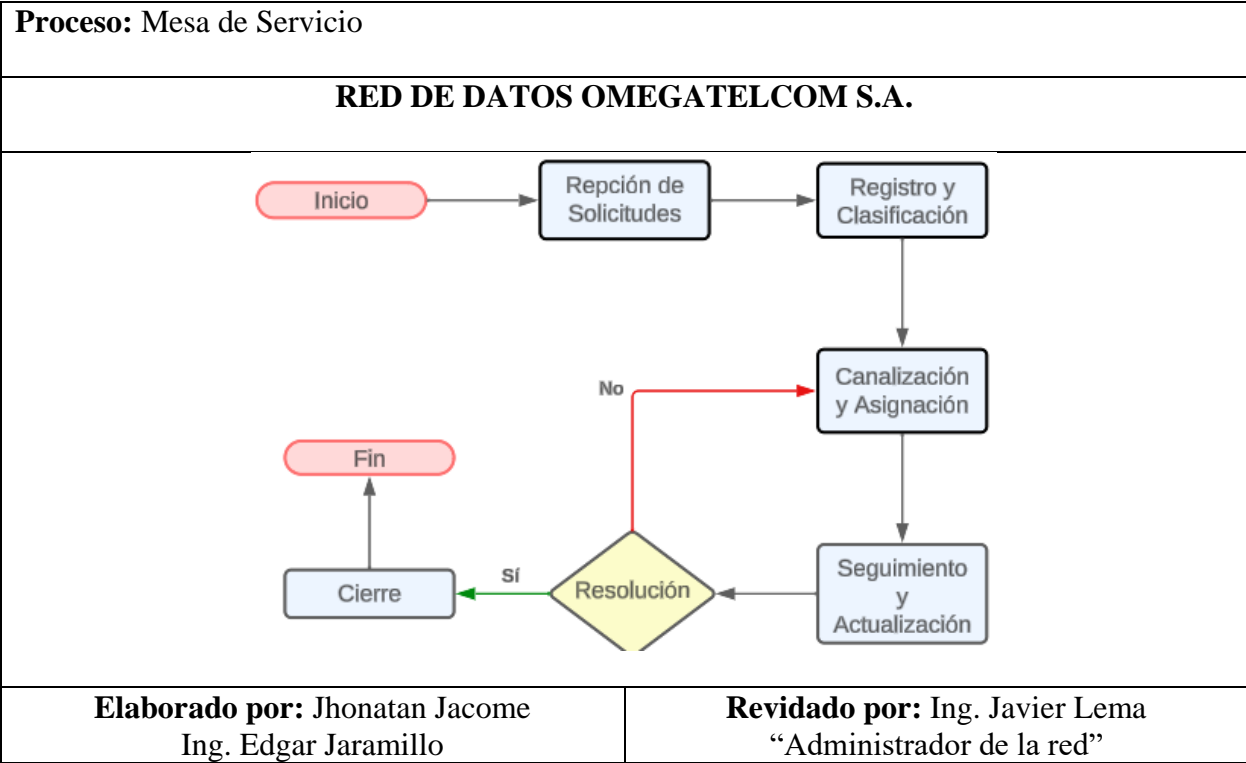
La Mesa de Servicios es un componente esencial para gestionar eficientemente las solicitudes y problemas reportados por los usuarios. Este proceso se centra en recibir, registrar, clasificar y canalizar adecuadamente los incidentes y solicitudes de servicio.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Recepción de Solicitudes	La Mesa de Servicios recibe las solicitudes de servicio, incidentes o consultas de los usuarios.	Agente de Mesa de Servicio
2. Registro y Clasificación	Cada solicitud se registra, clasifica y se asigna un número de seguimiento.	Agente de Mesa de Servicio
3. Canalización y Asignación	Las solicitudes se canalizan al equipo correspondiente y se asignan a los técnicos responsables.	Agente de Mesa de Servicio
4. Seguimiento y Actualización	La Mesa de Servicios realiza un seguimiento continuo de las solicitudes, actualizando a los usuarios sobre el progreso.	Agente de Mesa de Servicio

5. Resolución y cierre	Una vez resueltos, los incidentes se cierran formalmente y se notifica a los usuarios	Agente de Mesa de Servicio
------------------------	---------------------------------------------------------------------------------------	----------------------------

Diagrama de Flujo



E. Ingreso de Dispositivos a la Red

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Configuración		
	Dirigido a:	Administrador de la red
	Proceso:	Ingreso de Dispositivos a la Red
	Año de elaboración:	2024
	Código:	PROGA-005

Descripción

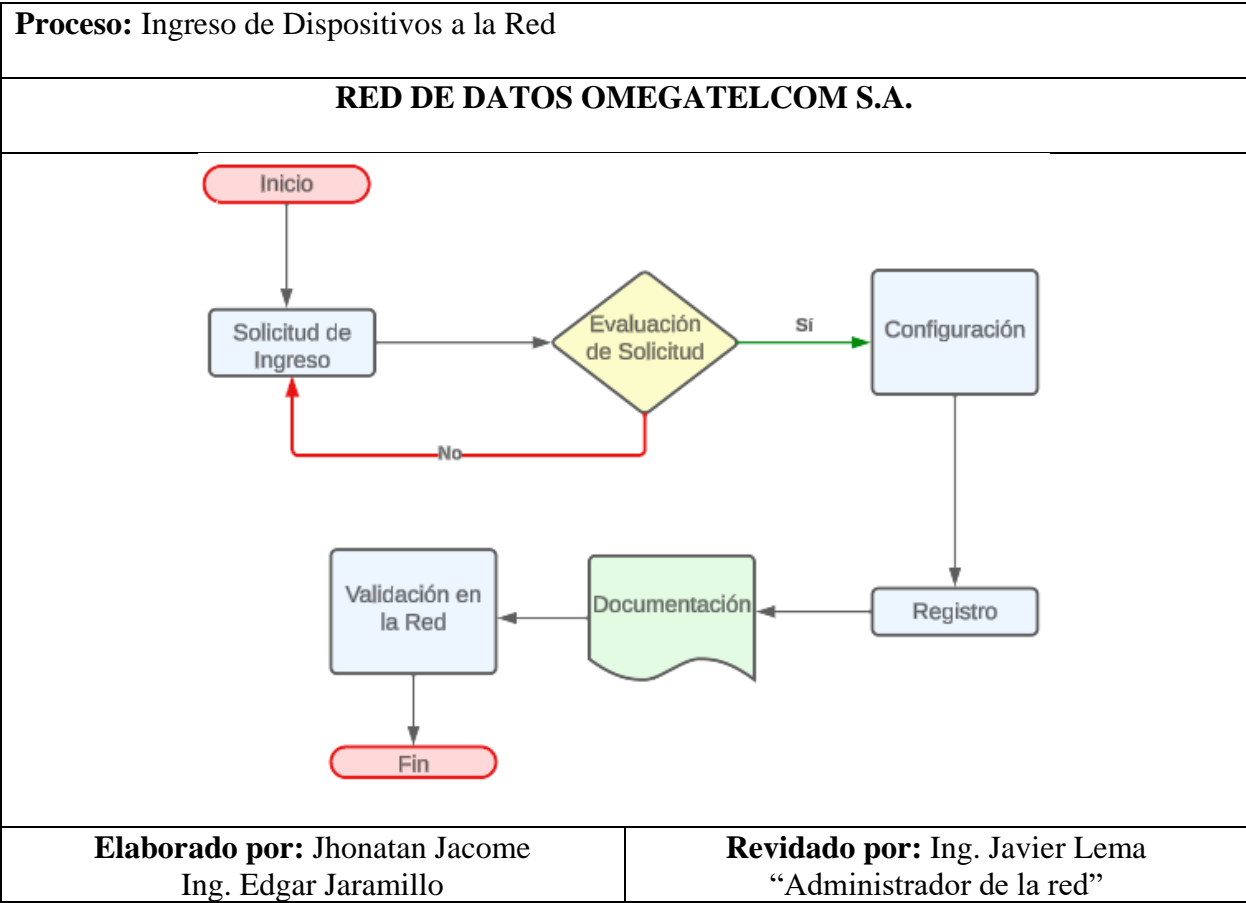
El ingreso de componentes a la red es una actividad crítica para garantizar la seguridad y la eficiencia en la gestión de los activos de red. Este procedimiento abarca desde la solicitud de ingreso hasta la configuración y validación en la red.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Solicitud de ingreso	Los usuarios autorizados presentan una solicitud formal para el ingreso de nuevos equipos a la red.	Usuario Autorizado
2. Evaluación de la Solicitud	El departamento encargado evalúa la solicitud, verificando la idoneidad y compatibilidad del equipo con la red existente. La rúbrica para evaluar los equipos se encuentra en el ANEXO 4.	Mesa de Servicio
3. Configuración	Se realiza la configuración necesaria del equipo para cumplir con los estándares de seguridad y rendimiento de la red.	Técnico de Red

4. Registro y Documentación	Cada equipo ingresado se registra en una BD y se documenta su configuración.	Mesa de Servicio
5. Validación en la Red	Se realiza una prueba de validación en la red para asegurar que el equipo funcione correctamente y no afecte el rendimiento general.	Técnico de Red

Diagrama de Flujo



F. Configuración de los Dispositivos

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Configuración		
	Dirigido a:	Administrador de la red
	Proceso:	Configuración de Dispositivos
	Año de elaboración:	2024
	Código:	PROGA-006

Descripción

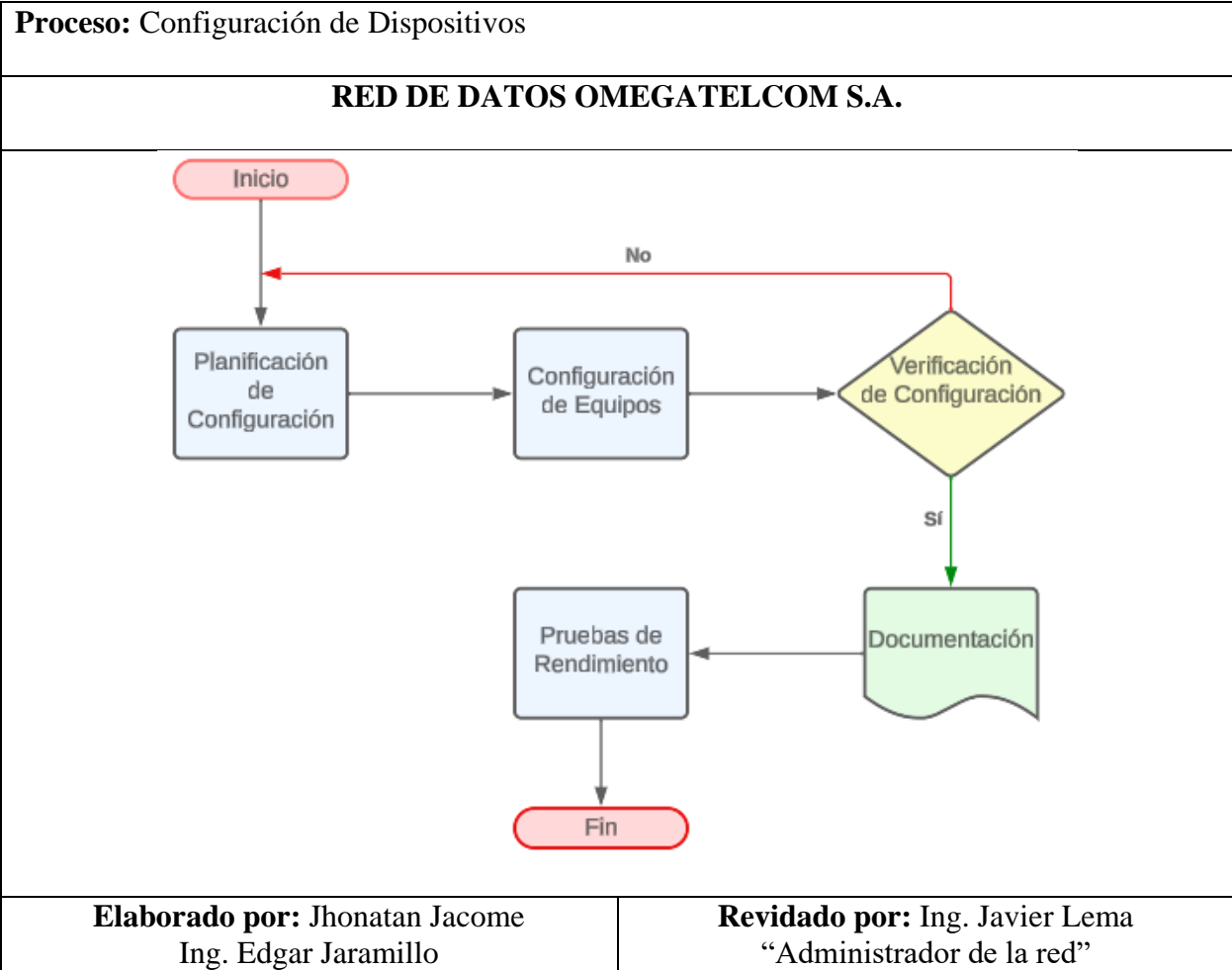
La configuración de equipos es una fase crítica para garantizar el rendimiento óptimo y la seguridad en la red. Este procedimiento abarca desde la planificación de la configuración hasta la verificación de su correcta implementación.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Planificación de Configuración	Se realiza una planificación detallada de la configuración requerida, considerando los estándares de seguridad y rendimiento. Los parámetros de Configuración para Equipos se encuentran en el ANEXO 5.	Técnico de Red/ Administrador de red
2. Configuración del Equipo	Se lleva a cabo la configuración del equipo según las configuraciones establecidas en la fase de planificación.	Técnico de Red/ Administrador de red
3. Verificación de Configuración	Se realiza una verificación exhaustiva para garantizar que	Técnico de Red/ Administrador de red

	la configuración se haya implementado correctamente.	
4. Documentación de Configuración	Se documentan los detalles de la configuración, incluyendo cambios realizados y parámetros específicos.	Técnico de Red/ Administrador de red
5. Pruebas de Rendimiento	Se ejecutan pruebas de rendimiento para evaluar el impacto de la configuración en la red.	Técnico de Red/ Administrador de red

Diagrama de Flujo



G. Inventario de Dispositivos de la red

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Contabilidad		
	Dirigido a:	Administrador de la red
	Proceso:	Inventario de Dispositivos de la red
	Año de elaboración:	2024
	Código:	PROGA-007

Descripción

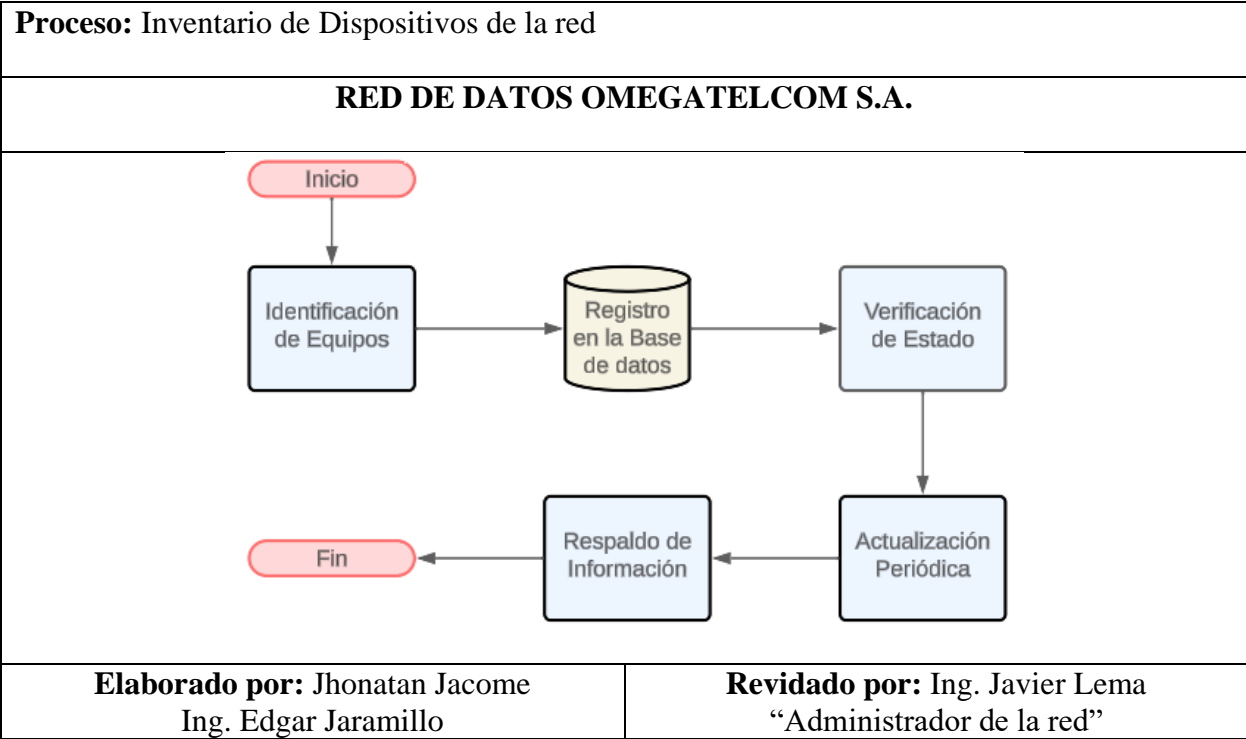
El inventario de equipos es esencial para mantener un control efectivo de los recursos en la red. Este procedimiento aborda desde la identificación de equipos hasta la actualización periódica del inventario.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Identificación de Equipos	Se identifican todos los equipos conectados a la red, asignándoles un número único y registrando sus características.	Personal Administrativo
2. Registro en la Base de datos	La información recopilada se ingresa y actualiza en una base de datos centralizada para el inventario.	Personal Administrativo
3. Verificación de Estado	Se verifica el estado operativo de cada equipo y se registra cualquier problema o necesidad de mantenimiento.	Técnico de Red
4. Actualización Periódica	Se establece un cronograma para actualizar regularmente	Personal Administrativo

	el inventario, incluyendo cambios en la configuración y adiciones o retiros de equipos.	
5. Respaldo de Información	Se realiza un respaldo periódico de la información del inventario para evitar pérdidas de datos críticos.	Personal Administrativo

Diagrama de Flujo



H. Uso de los Servicios de la Red

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Contabilidad		
	Dirigido a:	Administrador de la red
	Proceso:	Uso de los Servicios de la Red
	Año de elaboración:	2024
	Código:	PROGA-008

Descripción

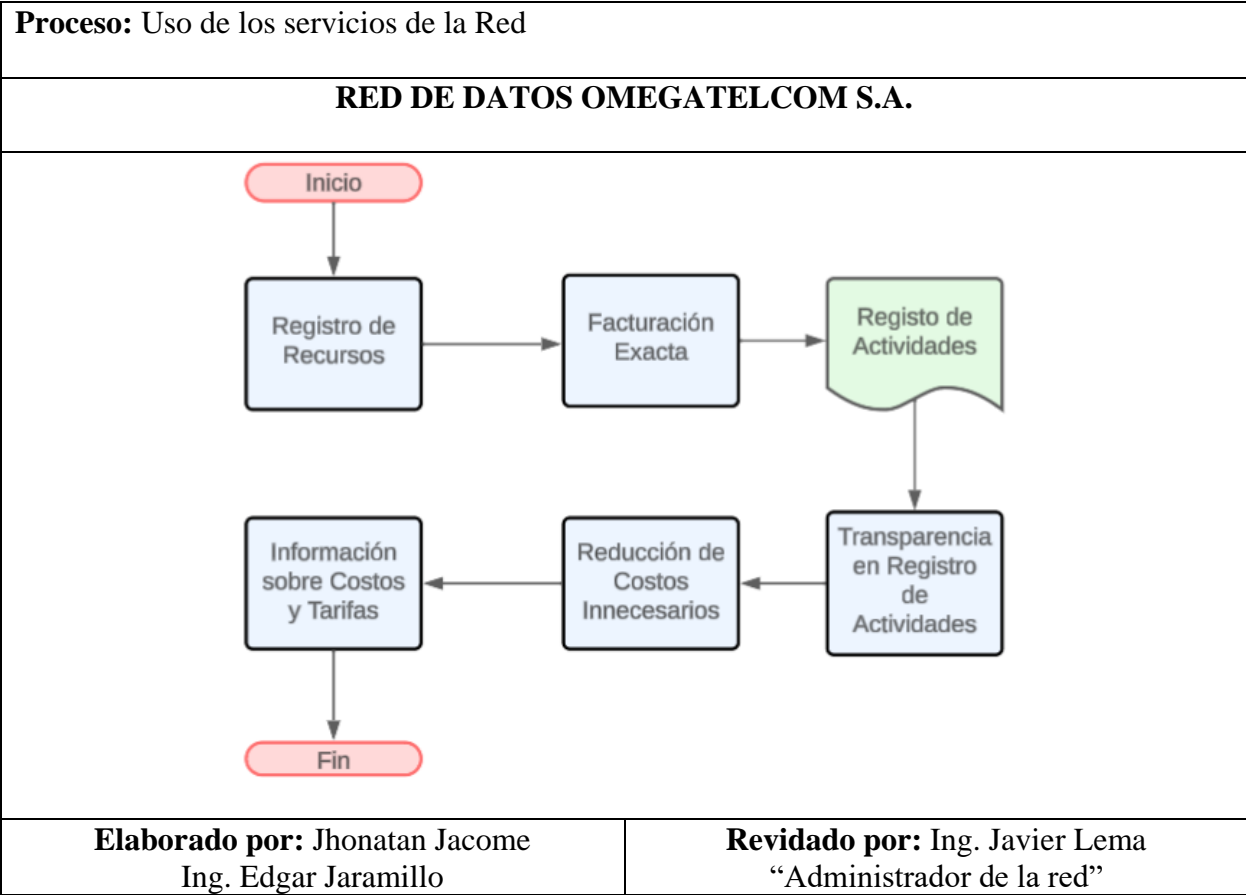
Este procedimiento establece las actividades contables en OMEGATELCOM, siguiendo los lineamientos de la Recomendación M.3400 para garantizar la transparencia y precisión en el registro y control de recursos.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Registro de Recursos	Se realiza el registro preciso de los recursos utilizados en la red, incluyendo equipos, ancho de banda y otros insumos.	Secretaria
2. Facturación Exacta	La facturación de servicios se realiza de manera precisa, reflejando los costos reales asociados a los servicios ofrecidos.	Secretaria
3. Transparencia en Registro de Actividades	Se mantiene un registro transparente de todas las actividades y gastos asociados a la gestión de la red.	Secretaria

4. Reducción de Costos Innesarios	Se identifican oportunidades para reducir costos innesarios sin comprometer la calidad de los servicios.	Contabilidad
5. Información sobre Costos y Tarifas	Se informa de manera clara a los usuarios sobre los costos y tarifas asociados a los servicios ofrecidos.	Contabilidad

Diagrama de Flujo



I. Informe de Rendimiento de Dispositivos

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Rendimiento		
	Dirigido a:	Administrador de la red
	Proceso:	Informe de Rendimiento de Dispositivos
	Año de elaboración:	2024
	Código:	PROGA-009

Descripción

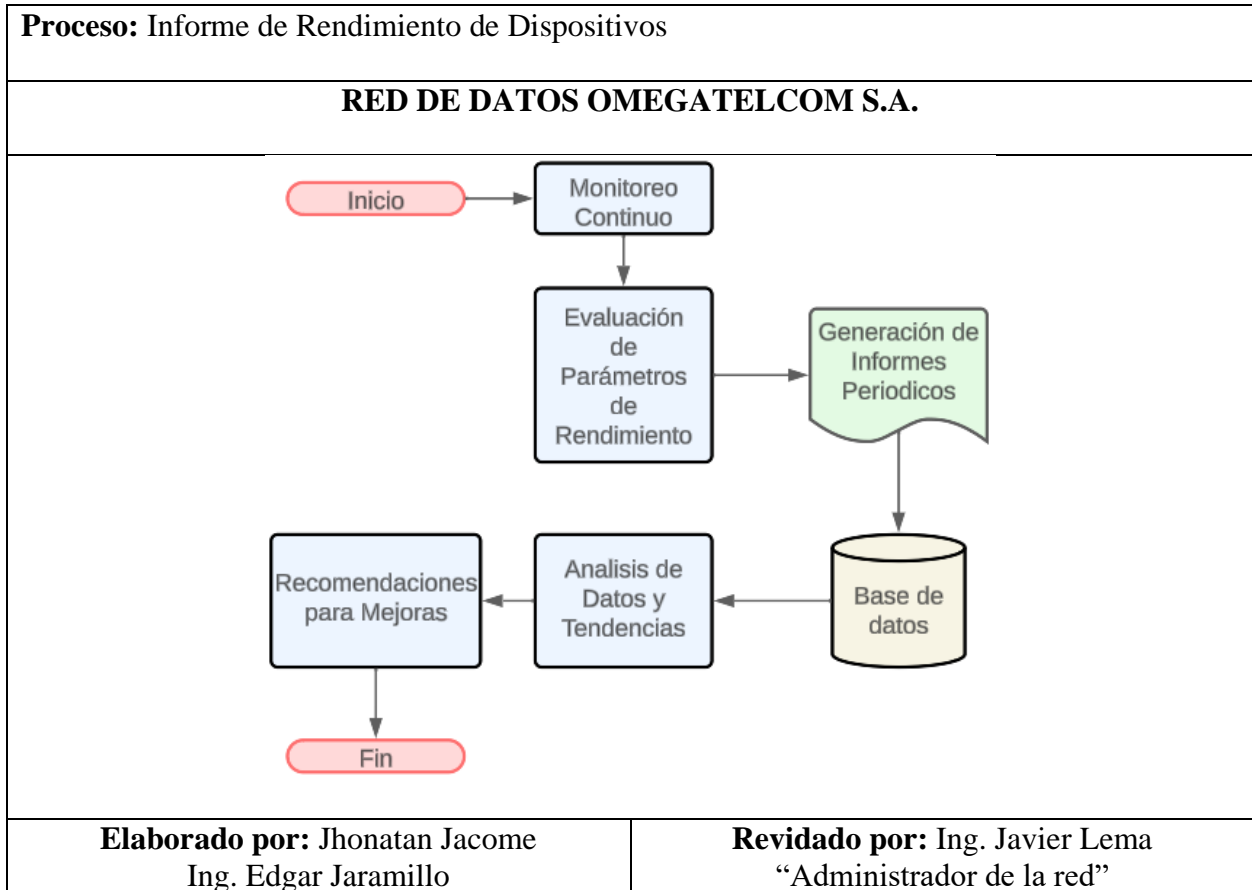
Este procedimiento establece las actividades para generar informes de rendimiento en OMEGATELCOM, siguiendo buenas prácticas y la Recomendación M.3400 para evaluar y mejorar la eficiencia de los servicios.

Detalle del Proceso


Actividad	Detalle	Responsable
1. Monitoreo Continuo	Se realiza un monitoreo constante de los servicios para recopilar datos relevantes sobre el rendimiento de la red.	Administrador de la Red
2. Evaluación de Parámetros de Rendimiento	Se evalúan parámetros clave como la velocidad de conexión, la latencia y la disponibilidad para determinar el rendimiento general.	Administrador de la Red
3. Generación de Informes Periódicos	Se generan informes periódicos que resumen el rendimiento de la red, destacando áreas de mejora y cumplimiento de objetivos. La	Administrador de la Red

	información se guarda en una base de datos	
4. Análisis de Datos y Tendencias	Se realiza una evaluación detallada de los informes para identificar tendencias, patrones y áreas que requieren atención especial.	Administrador de la Red
5. Recomendaciones para Mejoras	Se proponen recomendaciones basadas en el análisis de los informes, con el objetivo de mejorar la calidad y eficiencia del servicio.	Administrador de la Red

Diagrama de Flujo



J. Acceso al Sistema de la Red

EMPRESA OMEGATELCOM S.A.		
Proceso para la Gestión de Seguridad		
	Dirigido a:	Administrador de la red
	Proceso:	Acceso al Sistema de Red
	Año de elaboración:	2024
	Código:	PROGA-010

Descripción

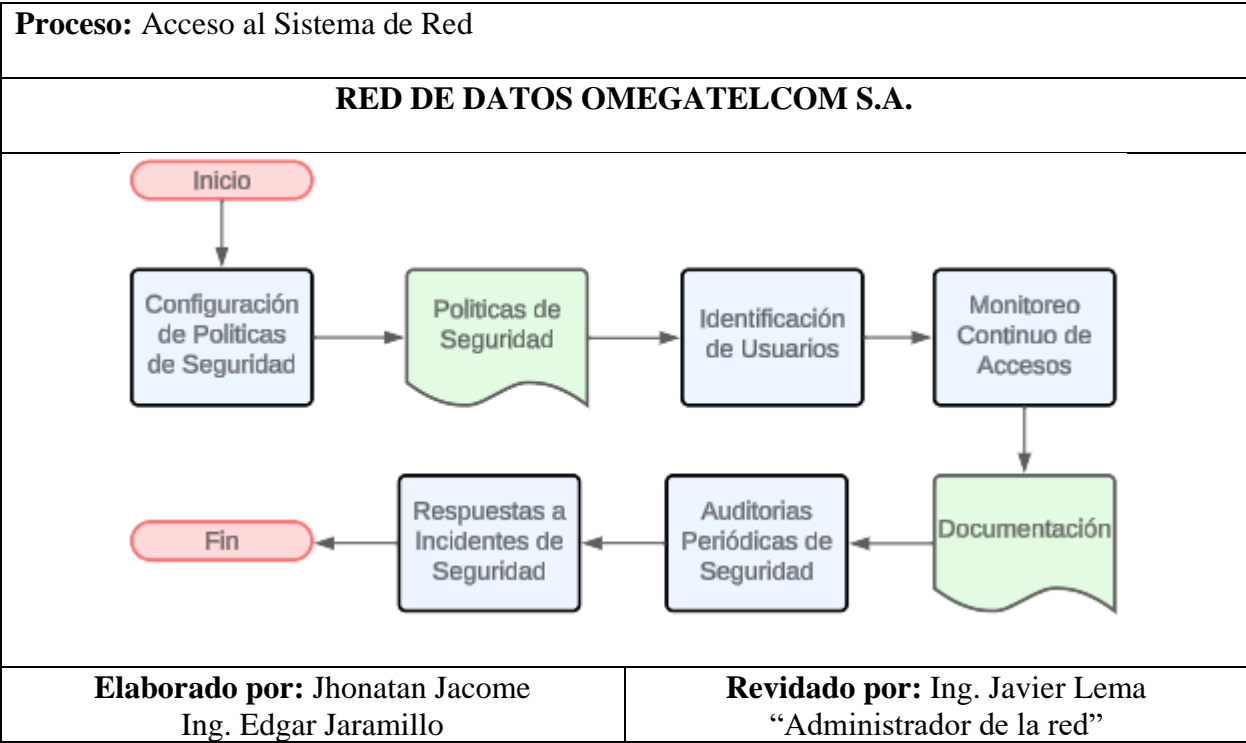
Este procedimiento establece las medidas de protección y control de acceso al sistema de red de OMEGATELCOM para garantizar la confidencialidad y disponibilidad de la información.

Detalle del Proceso

Actividad	Detalle	Responsable
1. Configuración en las políticas de Seguridad	Se establecen políticas de seguridad que incluyen la gestión de contraseñas, control de acceso y cifrado de datos. Editar documentación actual de Políticas en caso de ser necesario.	Administrador de la Red
2. Identificación de Usuarios	Se implementa un sistema de identificación de usuarios que garantice la autenticidad y autorización adecuada.	Administrador de la Red
3. Monitoreo Continuo de Accesos	Se realiza un monitoreo constante de los accesos al sistema para detectar posibles intrusiones o comportamientos anómalos. En caso de existir se debe documentar.	Administrador de la Red

4. Auditorias Periódicas de Seguridad	Se realizan auditorías regulares para evaluar la efectividad de las medidas de protección y llevar a cabo ajustes según sea necesario.	Administrador de la Red
5. Respuesta a Incidentes de Seguridad	Se establece un protocolo de respuesta a incidentes para abordar de manera rápida y efectiva cualquier amenaza o violación de seguridad.	Administrador de la Red

Diagrama de Flujo



ANEXO 4. Rubrica de Evaluación para ingresar Equipos en la red de OMEGATELCOM

S.A.

La aprobación del ingreso de equipos en la red debería basarse en una evaluación integral que considere varios factores. A continuación, se presentan algunas características a ser consideradas para el ingreso de equipos a la red.

Responda si cumple o no cumple dependiendo de las características del equipo:

Requisito	Si	No	Observaciones
1. Compatibilidad Técnica:			
El equipo es compatible con la infraestructura existente de la red.			
Cumple con los estándares de la red.			
2. Seguridad:			
El equipo no representa riesgos de seguridad significativos.			
Cumple con las políticas de seguridad de la empresa.			
3. Necesidad Operativa:			
Existe una clara justificación operativa para el ingreso del equipo.			
Aborda una necesidad o problema específico en la red.			
4. Costo-Beneficio:			
Se realizó un análisis de costos y beneficios para determinar la viabilidad financiera.			
El valor agregado del equipo justifica los costos asociados.			
5. Documentación Completa:			
Proporciona toda la documentación necesaria, incluyendo manuales, certificaciones y licencias.			
La información técnica y operativa es clara y completa.			
6. Impacto en el Rendimiento de la Red:			
Fue evaluado para minimizar cualquier impacto negativo potencial en el rendimiento de la red.			
Existe planes para mitigar cualquier problema potencial.			

7. Capacidad de Escalabilidad:			
El equipo es escalable en la adaptación al crecimiento futuro de la red.			
Se integra fácilmente con futuras expansiones o actualizaciones.			
8. Alineación con Estrategias Organizacionales:			
El equipo esta alineado con las estrategias y metas generales de la empresa.			
Contribuye a largo plazo de los objetivos de la empresa.			
9. Evaluación del Proveedor:			
El proveedor externo que suministra el equipo ha sido evaluado en cuanto a su reputación y confiabilidad.			
Se ha considerado las garantías y servicios postventa del proveedor.			

Fuente: Autoría

La combinación de estas características proporcionará una base sólida para tomar elecciones informadas sobre la aprobación del ingreso de equipos a la red. Es importante adaptar estas características según las necesidades y políticas específicas de la empresa OMEGATELCOM.

ANEXO 5. Parámetros para la Configuración de Equipos de OMEGATELCOM S.A.

La configuración de equipos en OMEGATELCOM considerara diversos parámetros para asegurar un despliegue eficiente y protegido de los dispositivos en la red. Aquí se proporciona una lista de parámetros a ser considerados según las necesidades que exista en la empresa.

Responda si cumple o no cumple dependiendo las características del equipo.

Pregunta	Si	No	Observaciones
1. Configuración IP:			
Asignación de direcciones IP estáticas o dinámicas.			
Reserva de direcciones IP para dispositivos específicos.			
Configuración de máscaras de subred.			
Configuración de la puerta de enlace.			
Configuración de servidores DNS primarios y secundarios.			
2. Configuración de VLAN (Redes Locales Virtuales):			
Asignación de VLAN para segmentar la red.			
3. Calidad de Servicio (QoS):			
Configuración de QoS para priorizar tráfico.			
4. Seguridad:			
Configuración de reglas de firewall.			
Configuración de VPN (opcional).			
5. Actualizaciones Automáticas:			
Configuración para actualizaciones automáticas de firmware o software.			
6. Seguridad Inalámbrica (si aplica):			
Configuración de seguridad para redes inalámbricas (WPA, WPA2, etc.).			
7. NAT (Traducción de Direcciones de Red):			
Configuración de NAT para mapeo de direcciones privadas a públicas.			
8. Servicios Activados/Desactivados:			

Configuración de servicios específicos activados o desactivados según las necesidades.			
9. Monitoreo y Registro:			
Configuración de registros de eventos y monitoreo de rendimiento.			
10. Cifrado y Autenticación:			
Configuración de métodos de cifrado y autenticación.			
11. Administración Remota:			
Configuración de acceso remoto seguro para la gestión del equipo.			
12. Sincronización de Tiempo:			
Configuración de servidores de tiempo para sincronización.			
13. Respaldo de Configuración:			
Configuración de rutinas automáticas de respaldo de configuración.			
14. Control de Acceso:			
Configuración de listas de control de acceso (ACL) si es necesario.			
15. Configuración de Políticas de Seguridad:			
Establecimiento de normas de seguridad específicas.			
16. Configuración de Proxy (si aplica):			
Configuración de servidores proxy para controlar el acceso a Internet.			

Fuente: Autoría

Estos parámetros deben adaptarse a las necesidades específicas de OMEGATELCOM. Además, es fundamental implementar procesos de revisión y actualización periódica de la configuración para garantizar su idoneidad y seguridad a lo largo del tiempo. El documento debe ser archivado como línea base para posibles problemas o cambios que puedan presentarse a futuro.