UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA

Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA

"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"

AUTOR: Rosa Lila Hermosa Torres

DIRECTOR: Ing. Fabián Geovanny Cuzme Rodríguez, MSc

IBARRA- ECUADOR

2023

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 DEL CONTACTO	
Cédula de identidad	100273667-4
Apellidos y nombres	Hermosa Torres Rosa Lila
Dirección	Salinas 9-65 y Liborio Madera
E-mail	rlhermosat@utn.edu.ec
Teléfono móvil	0992375286
Teléfono Fijo	062640249
DATOS DE LA OBRA	
TITULO:	MODELO DE GESTION DE RED BASADO EN EL MODELO DE GESTION FCAPS DE LA ISO QUE PERMITA MEJORAR LA DISPONIBILIDAD Y RENDIMIENTO DE LA RED DE LA EMPRESA JASSA TELECOM.
AUTOR:	Rosa Lila Hermosa Torres
FECHA	11 de enero del 2023
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA	☒ **PREGRADO** ☐ **POSGRADO**
TITULO	Ingeniera en Electrónica y Redes de Comunicación
DIRECTOR	Ing. Fabián Geovanny Cuzme Rodríguez, MSc.

2. CONSTANCIAS

El autor manifiesta 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 el titular de los derechos patrimoniales, por lo que sume la responsabilidad sobre contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 3 días del mes de Marzo de 2023

EL AUTOR:

Rosa Lila Hermosa Torres

100273667-4

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER FABIÁN GEOVANNY CUZME RODRÍGUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación "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". Ha sido desarrollado por la Señorita Rosa Lila Hermosa Torres, bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

Ing. Fabián Geovanny Cuzme Rodríguez, MSc.

CC: 1311527012

DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

El presente trabajo de investigación lo dedico a Dios, por no dejarme decaer y mantener mi fe, por darme fortaleza para seguir adelante en este proceso y culminar esta meta.

A mis padres, en especial a mi madre Ulvia Torres, quien ha sido el pilar fundamental en mi vida, por brindarme su apoyo incondicional y su confianza, por sus palabras de aliento que me han ayudado a no rendirme, sin ella no lo hubiera logrado.

A mis hijas Allison y Valentina, por ser mi fuente de inspiración y darme el valor para seguir adelante y crecer profesionalmente, quienes tuvieron que entender que durante el desarrollo de esta tesis fue necesario sacrificar situaciones y momentos a su lado, son mi motor y mi gran motivación para superarme cada día.

A mis hermanos Patricia, Grace y Eduardo por su paciencia y apoyo, por los buenos y malos momentos, en los que siempre encontramos ese cariño y fortaleza, que nos enseñan a unirnos más como familia.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTOS

Gracias a Dios por ayudarme a no renunciar en los momentos más difíciles y permitirme culminar este proyecto de tesis.

A mi familia por su cariño, comprensión y paciencia durante todo este tiempo, gracias infinitas.

Un especial agradecimiento a mi tutor, MSc. Fabián Cuzme por su dedicación, paciencia y profesionalismo, quien me supo dirigir durante todo este tiempo, para desarrollar con éxito este proyecto.

A la empresa JASSA TELECOM. CIA. LTDA. en especial a los Ingenieros Alexander Trejo por darme la oportunidad de realizar este proyecto y al Ing. Miguel Bravo por su apoyo en todo momento.

A mis amigos en especial a Diana y Ronny quienes han sido un gran apoyo en este caminar; a Darwin por ser ese amigo incondicional cuando más necesité de una guía, gracias por tu ayuda de manera desinteresada.

CONTENIDO

ÍNDICE DE FIGURAS

ANEXO F

ANEXO G

ANEXO H

ANEXO I

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de investigación se desarrolló ante la necesidad de aplicar un sistema de monitoreo para la empresa JASSA TELECOM CIA LTDA. El problema surge debido a que la empresa no dispone de guías y herramientas de monitoreo para el manejo apropiado y eficaz de sus recursos de red; ocasionando que la entidad ejecute sus operaciones de manera desorganizada.

El análisis técnico situacional reveló que la empresa carece de un sistema de monitoreo, así como también de manuales y procedimientos a ejecutar por el departamento de TI. Por otro lado, se determinó que no se da mayor relevancia al manejo de solicitudes hacia los usuarios internos.

En base a la investigación teórica conceptual, se elaboró la propuesta que contempla el estudio metodológico de las FCAPS de la ISO, de la biblioteca de las mejores prácticas ITIL v3, formulación de políticas y procedimientos que le servirán de guía en la ejecución de sus actividades. Además, se realiza la instalación de las herramientas de monitoreo para la detección y mitigación de errores, apoyándose del servidor de correo para la notificación de fallos al administrador; así como la instalación de la mesa de servicio GLPI que permitirá la generación de tickets y la atención oportuna de las solicitudes de los usuarios internos.

El trabajo incluye el análisis costo-beneficio en el que se determinó la viabilidad del proyecto puesto en marcha. Como resultado, se concluyó que la propuesta mejoró significativamente la gestión de la red y, en consecuencia, la optimización de los recursos, brindando un servicio totalmente disponible.

ABSTRACT

This research work was developed because of the necessity to apply a monitoring system for the company JASSA TELECOM CIA LTDA. The problem appeared because the company does not have controlling guides and monitoring tools for the appropriate and effective of network resources management; this causes that the company operates in a disorganized way.

The situational technical analysis showed that the company does not have a monitoring system, as well as manuals and correct processes to be made by the IT department. On the other hand, it was established that the requests management of to internal users are not seriously considered.

Based on the theoretical research, this proposal includes the ISO FCAPS methodological study and best practices of ITIL v3 library, besides, a policies formulation and procedures that will work as a guide in their activities execution.

In addition, the monitoring tools for the detection and reduction of mistakes will be installed, sustained in the mail server for the notification of failures to the administrator; plus, the installation of the GLPI service that will allow the tickets generation and the quick requests attention to the internal users.

The work includes the cost-benefit analysis that supports the viability of the Project. As a result, the conclusion was that the proposal improved significantly the network management and, consequently, the resources optimization provide a totally available service.

1. CAPITULO I

PRESENTACIÓN DEL PROYECTO

En este capítulo se encuentran detalladas las bases del desarrollo del presente trabajo de titulación, siendo éstos: el tema, el problema, los objetivos, el alcance y la justificación, que actúan en el desarrollo del presente proyecto, sobre qué está sustentado, al igual que sus limitaciones, con la finalidad de desarrollar un modelo de gestión de red congruente a las necesidades de la empresa JASSA TELECOM.

En todos los casos, el modelo funcional se constituye en la base para especificar las funcionalidades que se deben ejecutar en un sistema de gestión de telecomunicaciones y el primer paso para determinar los modelos de comunicación y de información que conforman la arquitectura de gestión

1.1 Tema

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.

1.2 Problema

Las tecnologías de la información (TI), han transformado la manera de trabajar y gestionar los recursos de las organizaciones. Actualmente, “las TI son un elemento clave para hacer que el trabajo sea más productivo, agilizando las comunicaciones, sustentando el trabajo en equipo, incrementando la producción, reduciendo tiempos de respuesta entre los procesos internos”, (Cano-Pita, 2018) proporcionando así una ventaja competitiva a las empresas que realizan una gestión eficiente de los recursos de TI.

JASSA TELECOM es una empresa dedicada a brindar soluciones tecnológicas de información y comunicación que ha logrado posicionarse en el mercado a nivel nacional, situada en la ciudad de Quito, ofreciendo a los usuarios un "portafolio de servicios que brinda asistencia de diseño, supervisión, implementación, construcción y venta de soluciones tecnológicas" (JASSATELECOM, 2019). La empresa JASSA TELECOM para brindar una adecuada atención y logística a sus clientes corporativos ha adquirido progresivamente infraestructura tecnológica que le permita automatizar y cumplir los procesos internos y misionales de la organización.

Dentro de sus procesos de mejora continua la empresa JASSA TELECOM ha identificado falencias en el funcionamiento diario de su infraestructura tecnológica, relacionado con la latencia, perdida de conectividad, virus, robo de información y datos, ataque de denegación de servicio, incidentes relacionados con cableado estructurado, manejo inadecuado en cuanto a gestión y monitoreo de la red de datos, inexistencia de políticas y procedimientos para gestión de incidentes. Esto derivado de un crecimiento desorganizado de la red de telecomunicaciones y el no cumplimiento de buenas prácticas y normas para una adecuada gestión y monitoreo de los servicios de TI de la organización.

Debido a la tendencia de mejora de servicios y falta de gestión de procesos en el departamento de TI de la empresa, se ve en la necesidad de buscar mecanismos que permitan la detección, mitigación de problemas en la red y la obtención de mejores tiempos de respuesta en el acceso a servicios de TI.

En este contexto es fundamental el desarrollo de un modelo de gestión de red que permita planificar, administrar, mantener, monitorear la red y los servicios de telecomunicaciones de la organización mediante la implementación y gestión de un Service Desk (mesa de servicio), que se encuentre alineada con el Framework de Red de Gestión de Telecomunicaciones

(FCAPS) y las mejores prácticas de la biblioteca de la infraestructura de tecnologías (ITIL v3).

1.3 Objetivos

1.3.1 Objetivo general

Diseñar y desarrollar un modelo de gestión de red y servicios de telecomunicaciones para la empresa JASSA TELECOM, basado en el Framework de red de gestión de telecomunicaciones (FCAPS) y las mejores prácticas de la biblioteca de la infraestructura de tecnologías (ITIL v3).

1.3.2 Objetivos específicos

- Analizar el Framework de red de gestión de telecomunicaciones (FCAPS) de ISO y los procesos del Ciclo de Vida del Servicio de ITIL v3.
- Realizar el levantamiento de información de la situación actual y requerimientos técnicos de la red de telecomunicaciones, a través de técnicas e instrumentos para la recolección de información.
- Diseñar el modelo de gestión de red y servicios de telecomunicaciones, basado en políticas y procedimientos que permita planificar, mantener y administrar la red y los servicios de telecomunicaciones.
- Realizar un análisis Costo-Beneficio de la implementación del modelo propuesto que permita una adecuada gestión de red y monitoreo de los servicios de telecomunicaciones.

1.4 Alcance

Este proyecto tiene como finalidad desarrollar un modelo gestión de red que permita planificar, mantener y administrar la red y los servicios de telecomunicaciones de la empresa JASSA TELECOM, basado en el Framework de red de gestión de telecomunicaciones (FCAPS) y las mejores prácticas de la biblioteca de la infraestructura de tecnologías (ITIL v3), que facilite a las personas responsables del área de TI sobre un manejo eficiente de la red, las peticiones de los usuarios internos, además de establecer registros de las solicitudes realizadas diariamente que permitan tener estadísticas del soporte a realizar para simplificar la administración de la red. Además de realizar un análisis y elección de las herramientas tecnológicas de gestión de red, que se adapten al cumplimiento de las áreas funcionales del modelo seleccionado para la empresa, para mejorar la disponibilidad y maximizar el rendimiento de la red.

Se efectuará una revisión bibliográfica de cada una de las áreas funcionales de las FCAPS que se detallan a continuación:

- Gestión de Fallos
- Gestión de Configuración
- Gestión de Contabilidad
- Gestión de Prestaciones
- Gestión de Seguridad

Y las fases del ciclo de vida de las buenas prácticas (ITIL) como son:

- Estrategia del Servicio
- Diseño del Servicio
- Transición del Servicio

- Mejora Continua del servicio
- Operación del Servicio

Que permita crear lineamientos adecuados para el desarrollo del modelo de gestión de red.

El análisis de los marcos de referencia y buenas prácticas van a determinar las áreas funcionales necesarias del modelo de gestión de red que permitan planificar, mantener y administrar la red, adaptados a las necesidades de la empresa, permitiendo mejorar la gestión de requerimientos.

Se procederá a analizar la situación actual y requerimientos técnicos de la empresa JASSA a través del uso de técnicas e instrumentos para la recolección de datos realizando inventarios y encuestas que serán elaboradas manualmente, con el fin de identificar el estado físico y lógico de la red para luego poder establecer normas que guíen el proceso del modelo de gestión de red.

Se integrarán las áreas funcionales del Framework de red de gestión de telecomunicaciones (FCAPS), las buenas prácticas, fases, procesos, funciones y herramientas que contemplan el ciclo de vida del servicio basado en ITIL v3. Posterior a la identificación de los procesos y herramientas se implementará la mesa servicios, luego se determinará las políticas y procedimientos basadas en el modelo propuesto con la finalidad de tener una adecuada gestión y administración de la red de telecomunicaciones y servicios de TI, así mismo los procedimientos establecidos nacerán a partir de la información para tener una guía adecuada que cumplan con el modelo establecido y las necesidades de la empresa.

Conjuntamente, se elaborará manuales específicos para mantener y administrar la red de datos y los servicios de telecomunicaciones de la empresa JASSA TELECOM, que cubran

los parámetros de administración que determine el modelo FCAPS y las mejores prácticas (ITIL v3).

Finalmente se efectuará un análisis costo beneficio posterior implementación del modelo de gestión en base al modelo de gestión (FCAPS) de ISO e ITIL v3.

1.5 Justificación

Las tecnologías de la información y comunicación han cambiado la forma en la que interactúan en el entorno, sus avances no solo permiten una rápida transmisión de datos, sino el proceso de elaboración, planificación y desarrollo de diversas actividades productivas dentro de las instituciones. Este sector en su evolución, ha ido generando diversos conjuntos de mejores prácticas que ayudan a las organizaciones a gestionar procesos fundamentales, en donde el soporte y provisión de servicios de TI mejore los procedimientos de incidencias.

La correcta implementación de los principios de FCAPS y las buenas prácticas de ITIL a través de la gestión de una mesa de servicio permitirá reducir los costos de TI en la organización, esto en concordancia con un estudio denominado “Presencia de la metodología ITIL en América Latina” en el cual indica que respecto al factor económico y social el 68% de las empresas encuestadas consideran importante la implementación de ITIL dentro de sus organizaciones (Lago, N. & Sánchez, N., 2018). Como aporte del trabajo de investigación la empresa adquirirá factores positivos como procesos de TI con mayor madurez, generación de mayor productividad (menos errores en la operatividad de la infraestructura tecnológica), mejora en los tiempos de resolución de incidentes, mayor calidad en los procesos diarios de TI (hacer las actividades siempre igual), apalancando a una mejor imagen corporativa de la empresa y posibilitando el incremento de la cartera de clientes corporativos.

De acuerdo a lo mencionado anteriormente, la investigación y desarrollo a realizarse constituye un aporte para mejorar los procesos interno de la unidad de TIC y la imagen corporativa de la empresa, permitiendo que tenga un control total de la infraestructura tecnológica, garantizando la operatividad, el manejo eficiente de recursos y la satisfacción del cliente interno como algunos de los aspectos clave que se pueden administrar a través de la mesa de servicios. De igual manera la presente investigación puede ser la base de futuros trabajos de investigación dentro de la organización relacionados con Gobierno de TI, Sistemas de seguridad de la información (SGSI) y procesos de certificación para la empresa en la ISO/IEC 20000 - norma internacional sobre Gestión de servicios de TI (ITSM)

Como autora del presente trabajo de investigación y estudiante de la carrera en Electrónica y Redes de Comunicación, cuento con los conocimientos técnicos como tecnológicos de análisis para poder llevar a cabo la investigación propuesta, fortaleciendo la relación entre la empresa privada y la academia.

2. CAPITULO II

FUNDAMENTO TEÓRICO

El cambio y crecimiento heterogéneo constante de las TI han llevado a las empresas a gestionar de una mejor manera los requerimientos y mecanismos de adaptación, para llegar al usuario, fomentando así el mejoramiento de las condiciones del servicio y la productividad de la gestión de los servicios de TI. Este capítulo se centra en el desarrollo de los conceptos básicos de los modelos de Gestión de redes y servicios de telecomunicaciones, el Framework de red FCAPS y las mejores prácticas de la biblioteca de la infraestructura de tecnologías (ITIL v3), que servirán de sustento en el desarrollo del proyecto.

2.1 Gestión de red

La Gestión de red se define como el conjunto de actividades dedicadas al control, supervisión y organización de recursos de telecomunicación para garantizar un nivel de servicio adecuado. Los objetivos primordiales de la gestión de redes es garantizar un nivel de servicio en los recursos gestionados con el mínimo coste, mejorar la disponibilidad y rendimiento además incrementar la efectividad de la red. (Molina Robles, 2010).

2.2 Evolución de la gestión de red

Desde sus inicios las redes de datos han evolucionado debido a la necesidad de compartir información y variedad de servicios, para cubrir requerimientos de sus usuarios, de forma indeleble y sin ninguna interrupción. En sus primeros pasos la gestión de red estableció como norte la monitorización del tráfico de red y el establecimiento de Calidad de Servicio (QoS), a su vez ofrecer la detección de errores que se pudiesen producir en la red, el cómo identificarlos y resolverlos (Universidad Dr. Rafael Belloso Chacín (URBE, 2010).

Las primeras redes conocidas como autónomas contaban con sistemas de gestión local y propietario, en su evolución, surgió la gestión homogénea en donde el sistema de gestión fue centralizado y propietario, acompañada del abaratamiento y mejora de equipos. Con el paso del tiempo las redes se digitalizaron, evolucionando hacia los sistemas heterogéneos, en donde la gestión era centralizada y propietaria de cada red, surgiendo la necesidad de interconexión de productos heterogéneos (variedad de interfaces de usuarios, aplicaciones y posible inconsistencia de la gestión), dificultando alcanzar el objetivo de gestión de red a un coste razonable. Finalmente, en su evolución nace la gestión integrada, exigiendo que haya un marco de elementos (protocolos, estándares, entre otros) que permite un control permanente de red.

Siendo así la gestión integrada una solución a los problemas de la gestión heterogénea (Orozco, 2010).

2.3 Elementos de la gestión de red

Son los encargados de supervisar y controlar todas las acciones que realizan los dispositivos administrados de la red, utilizando protocolos de administración. A continuación, se presentan los elementos de la gestión de red:

- Estación de gestión de red o (NMS)
- Gestor
- Agente
    - ✓ MIB
- Dispositivos administrados
- Protocolo de gestión de red

2.3.1 Estación de gestión de red (NMS)

Conocido como un Sistema de Gestión de redes (NMS) que ejecuta aplicaciones que supervisan y controlan permanentemente todos los dispositivos administrados, facilitando las operaciones de gestión. Interactúa con el administrador de la red y sirve como punto de control central para los dispositivos.

2.4 Gestor

El gestor es la consola a través de la cual el administrador de red realiza funciones de gestión de red, envía instrucciones de gestión y recibe notificaciones y respuestas.

2.4.1 Agente

Software de administración de red situado en la unidad para que pueda ser gestionado. Contiene a la MIB (Base de Datos de Información para Gestión), que se organiza en jerarquías y se traduce a un formato apropiado de acuerdo con el protocolo administrativo del sistema (URBE, 2010).

2.4.1.1 Base de datos de información de gestión (MIB)

Base de datos que contiene información jerárquica y describe las propiedades de cada componente en un dispositivo de red.

2.4.2 Dispositivos Administrativos

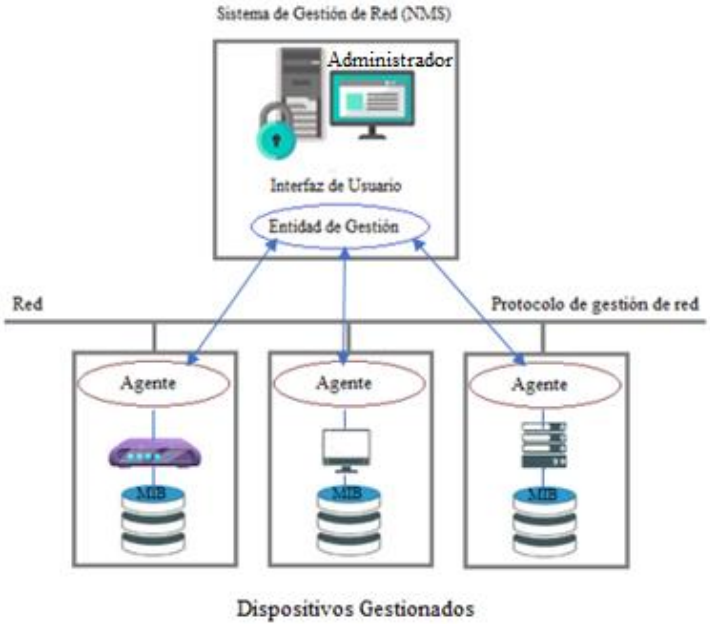
Cualquier dispositivo que tenga un agente SNMP y sea parte de una red administrada. Recopilan y almacenan datos de control y monitoreo, que luego se ponen a disposición de los administradores a través de protocolos de administración de red (URBE, 2010).

2.4.3 Protocolo de gestión de red

Es el conjunto de reglas y acuerdos que actúa como mediador para establecer la comunicación y el intercambio de datos dentro de un sistema de gestión. En la figura 1 se muestra un ejemplo de un sistema de gestión de red bajo el paradigma gestor-agente.

Figura 1

Elementos de un sistema de gestión de red



Nota. Adaptado de (Millán Tejedor R. J., 2003;2015)

2.5 Centro de gestión de red

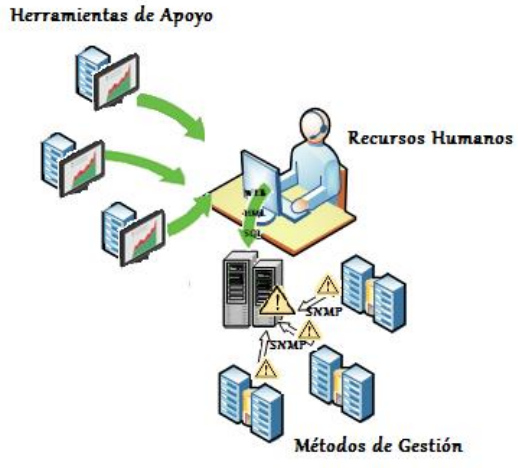
La gestión de red se concentra en un centro de gestión, donde se dirige, controla y monitorea el correcto funcionamiento de los equipos integrados, permitiendo coordinar todas las operaciones de forma eficiente (Calvo, 2016). Un centro de gestión de red dispone de tres tipos principales de recursos:

- **Métodos de gestión. -** Proporciona pautas de comportamiento de los otros componentes del centro de administración de red en situaciones específicas.

- **Recursos Humanos. -** Persona responsable del buen funcionamiento del centro de gestión de red.
- **Herramientas de apoyo. -** Software que facilita a los operadores humanos la realización de tareas de gestión y permite reducir el número de estos operadores (Montoya, Duarte, & Lobo, 2011). Se muestran en la figura 2.

Figura 2

Recursos de un Centro de Gestión



Nota. Adaptado de (Circutor, 2021)

2.6 Componentes de la gestión de red

La gestión de red se apoya en tres componentes básicos:

- Componente Organizacional
- Componente Técnico
- Componente Funcional

2.6.1 Componente Organizacional.

Define la estructura para el proceso de gestión y la estrategia apropiada para llevarlo a cabo de acuerdo con las necesidades del negocio. Este componente combina cuatro aspectos

principales que realizan una serie de actividades, donde la responsabilidad de estas tareas se diferencia en función del tiempo de actuación.

- Control operacional. - Mantiene de forma dinámica el nivel de servicio de red.
- Administración. - Actividades orientadas al seguimiento de las tareas de control operacional.
- Análisis. - Actividades cuyo objetivo es garantizar la calidad del servicio.
- Planificación. - Actividades que determinan las características principales que debe tener la red en función de las características de la empresa.

2.6.2 Componente Técnico

Define las herramientas que se utilizarán para la administración, el monitoreo y la instalación de la infraestructura. El intercambio de información entre elementos a través de un protocolo de gestión es la base del funcionamiento del sistema. Se basan en dos procesos fundamentales que trabajan juntos para completar múltiples tareas.

2.6.2.1 Proceso de monitoreo

Proceso encargado de almacenar la información del comportamiento de todos los recursos gestionados, permitiendo un análisis recurrente a fin de establecer posibles mejoras de la configuración de red y sus componentes, para garantizar y optimizar el servicio. El monitoreo establece las funciones de lectura las cuales observan y analizan el estado y el comportamiento de las configuraciones de red y sus componentes. Cuenta con 4 fases:

- ✓ Definición de la información de gestión que se monitoriza.
- ✓ Acceso a la información de monitorización.
- ✓ Diseño de mecanismos de monitorización.
- ✓ Procesado de la información de monitorización

(Orozco, 2010) Señala que la información estática no varía con la actividad de la red y se almacena en el dispositivo monitorizado, mientras que la información dinámica es almacenada en el dispositivo o en otros equipos especializados y cambia con la actividad de la red. Por otro lado, la información estadística se obtiene desde la información dinámica y se encuentra en el mismo lugar.

2.6.2.2 Proceso de control

Proceso encargado de evaluar y mejorar el desempeño de los servicios de la red, llegando a establecer criterios óptimos de operatividad. (URBE, 2010)

2.6.3 Componente Funcional

Define las funciones de gestión que debe realizar el componente organizacional al utilizar las herramientas de gestión (Jiménez, 2015).

Modelos de Gestión de Red

Actualmente existen tres modelos de gestión integrada definidos por organismos internacionales de normalización.

- Modelo de gestión de Red OSI
- Modelo TMN
- Modelo de gestión Internet o TCP/IP

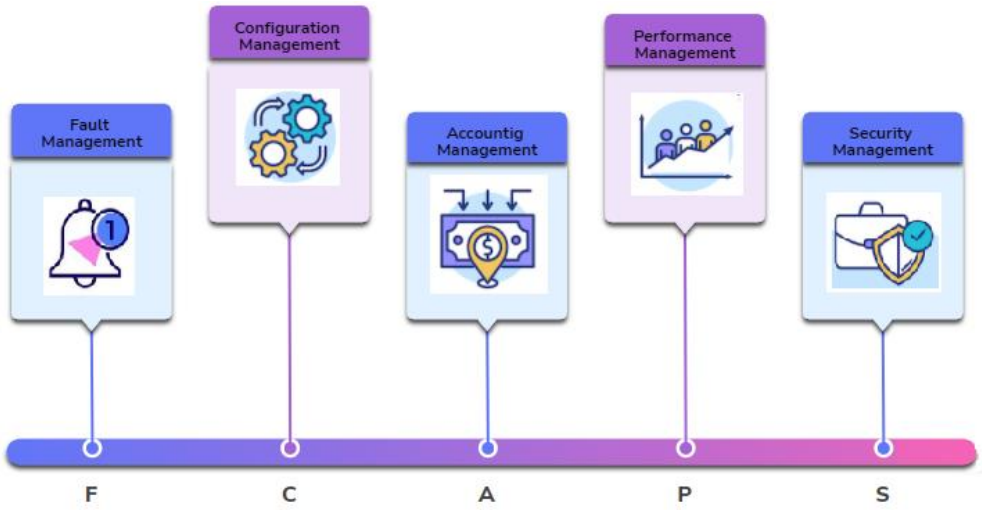
2.6.4 Modelo de gestión de Red OSI

Las FCAPS de la ISO son el modelo y Framework de red de gestión de telecomunicaciones, introducido en el año de 1992 por la ITU-T con la finalidad de establecer un estándar de administración de TI y cubrir aspectos importantes de la gestión de

redes. Este modelo está dividido en cinco áreas funcionales que serán descritas a continuación en la figura 3.

Figura 3

Áreas funcionales FCAPS de la ISO



Nota. Adaptado de (Solís, 2014)

El modelo funcional proporciona las bases para desarrollar librerías de soluciones de administración parciales y facilitar la delegación de funciones administrativas a varias personas (Mega & Nurul, 2019).

2.6.4.1 Gestión de fallos (F)

La gestión de fallos tiene por objetivo fundamental identificar problemas a través del monitoreo de toda la red, encontrar fallas en dispositivos administrados, operaciones de red, para que puedan determinar la causa y tomar medidas correctivas de inmediato. La gestión de problemas de red implica las siguientes tareas:

- Garantía de la calidad (fiabilidad, disponibilidad y supervivencia)
    - Detección de fallas
    - Corrección de fallas

    - Aislamiento de fallas
    - Recuperación de red
- Vigilancia de alarmas.
    - Manejo de alarmas
- Localización de averías.
    - Filtrado de alarmas
- Reparación de averías.
    - Generación de alarmas
- Pruebas.
    - Correlación limpia
- Administración de anomalías.
    - Test de diagnóstico
    - Registro de errores
    - Manejo de errores
    - Estadísticas de errores

En este proceso se debe encontrar una solución pronta para garantizar la disponibilidad de la red.

2.6.4.2 Gestión de contabilidad (A)

La gestión de contabilidad tiene como misión determinar los costos asociados al uso de los recursos de la red, que permitiendo elaborar las facturas necesarias para sus clientes. Entre las tareas que se deben realizar en esta área, están:

- Medición de la utilización.
    - Seguimiento de servicio/Uso de recursos

- Tarificación/fijación de precios.
    - Costo por servicios
    - Límite de contabilización
- Cobros y finanzas.
    - Uso de cuotas
- Control de la empresa.
    - Auditorias
    - Reporte de fraudes
    - Combinación de costos de múltiples recursos
    - Soporte de diferentes modos de contabilidad

2.6.4.3 Gestión de rendimiento (P)

La gestión de prestaciones o del rendimiento tiene como objetivo principal el mantener el nivel de servicio que la red ofrece a sus usuarios, garantizando el funcionamiento de manera eficiente en todo momento. La gestión de prestaciones se basa en cuatro tareas:

- Garantía de la calidad de funcionamiento.
    - Porcentaje de utilización y relación de errores
- Supervisión de la calidad de funcionamiento.
    - Recolección de datos de desempeño
    - Nivel consistente de desempeño
- Control de la gestión de la calidad de funcionamiento.
    - Análisis de datos de desempeño
- Análisis de la calidad de funcionamiento.
    - Reporte de problemas
    - Planeación de capacidad

- Generación de reportes de desempeño
- Mantenimiento y evaluación de logs históricos.

2.6.4.4 Gestión de configuración (C)

El objetivo de la gestión de la configuración es recopilar datos de red y usarlos para agregar, mantener y eliminar varios componentes y recursos a la red. Se deben completar las siguientes tareas fundamentales:

- Planificación e ingeniería de la red.
  - Inicialización de recursos
  - Aprovisionamiento de red
- Instalación.
  - Autodescubrimiento
- Planificación y negociación de servicios.
  - Respaldo y restauración
  - Apagado de recursos
  - Manejo de cambios
- Provisión.
  - Pre-aprovisionamiento
- Situación y control.
  - Manejo de inventario/activos
  - Copia de configuración
  - Configuración remota
  - Distribución automática de software
  - Iniciación de trabajo, seguimiento y ejecución

2.6.4.5 Gestión de seguridad (S)

Según (Mega & Nurul, 2019), la misión de la gestión de la seguridad es proporcionar mecanismos que faciliten el mantenimiento de las políticas de seguridad (dirigidas a la protección contra ataques de intrusión). Entre las funciones que llevan a cabo los sistemas de gestión de seguridad se encuentran:

- Prevención.
    - Acceso selectivo a recursos
- Detección.
    - Logs de acceso
- Contenencia y recuperación.
    - Privacidad de datos
    - Revisión de los privilegios de acceso de usuario
- Administración de la seguridad.
    - Auditoria de seguridad, seguimiento de logs
    - Alarmas de Seguridad/Reporte de eventos
    - Protección de brechas de seguridad y de intentos de intrusión
    - Seguridad relacionada con la distribución de información.

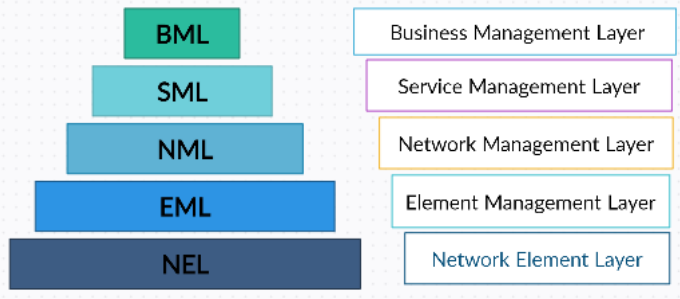
2.6.5 Modelo de gestión de red de telecomunicación TMN

TMN (Telecommunications Managed Network) fue desarrollado por la UIT/T, como un paradigma de gestión universal, proporcionando una estructura de red organizada diseñada para proporcionar interconectividad y comunicación a través de sistemas heterogéneos. Las funciones de TMN contienen una estructura jerárquica de capas lógicas que ofrecen escalabilidad, eficiencia y operación óptima en la administración y gestión de empresas y

redes de telecomunicaciones (Quispe & Ramírez, 2017). En la figura 4 se muestran los niveles lógicos TMN.

Figura 4

Pirámide TMN



Nota. Tomada de (Quispe & Ramírez, 2017)

Cada una de las capas cumple con las siguientes funciones:

Capa de gestión empresarial (BML). - Analiza tendencias en la red, calidad de servicio (QoS), facturación e informes financieros.

Capa de gestión de servicios (SML). - Gestiona los servicios ofrecidos por un proveedor de servicios a los clientes o incluso a otros proveedores de servicios de red (minoristas). Debajo de esta capa, tenemos servicios como facturación, procesamiento de pedidos, manejo de quejas y emisión de boletos de problemas. El ticket de problema, también llamado informe de problema es un mecanismo que se utiliza en una organización para realizar un seguimiento de la detección, notificación y resolución de problemas en una red.

Capa de administración de red (NML). - Ayuda a realizar funciones integradas de administración de fallas y provisión de servicios de red como control de ancho de banda, control de desempeño, control de congestión de red y control de calidad de servicio (Subramanian, 2000).

Capa de gestión de elementos (EML). - Contiene funciones manejadas por elementos de red individuales. Estas funciones incluyen la supervisión de la red, la gestión de inventarios, el aprovisionamiento de la red y la garantía del servicio.

Capa de elemento de red (NEL). – En esta capa se encuentran dispositivos conmutadores, enrutadores, puentes y otras instalaciones de transmisión.

Varela (2003) define las siguientes funciones del modelo de gestión TMN:

- Administración remota de los elementos del sistema.
- Proveer al cliente una interfaz amigable y de fácil interacción.
- Incrementar la automatización al momento de solucionar problemas que involucren a los clientes y servicios.
- Brindar integración e interoperabilidad entre diferentes protocolos y tecnologías.

2.7 Protocolos de gestión de red

De acuerdo con (Calvo, 2016), los protocolos de gestión son reglas que definen la comunicación entre la entidad gestora y el agente de gestión.

Existen distintos protocolos de gestión de red, dentro de los cuales se destaca SNMP, es el protocolo a utilizar en redes empresariales, pues todos los equipos lo soportan, y, de hecho, puede ser considerado un estándar de facto. Otro protocolo estándar, es el CMIP, de la familia de protocolos OSI de la ISO, que, si bien no está muy establecido en la empresa, está presente en la mayoría de los operadores de los servicios de telecomunicación para su gestión de redes.

2.7.1 Protocolo común de gestión de información CMIP

Protocolo estándar para la administración de redes a través de objetos administrados que proporciona seguridad de red avanzada e informa sobre condiciones de red inusuales. El protocolo CMIP se desarrolló para simplificar y mejorar las deficiencias y capacidades administrativas del protocolo SNMP.

CMIS/CMIP es un protocolo de gestión de red definido en la capa de aplicación del modelo de comunicación OSI: interconexiones de sistemas abiertos.

Permite la gestión de equipos de red locales y remotos tanto en entornos públicos como privados. Se compone de dos partes:

CMIS Common Management Information Service. - Servicio de información de gestión común, proporciona servicios a las aplicaciones de gestión.

De acuerdo con (Orozco, 2010), el CMIP presenta las siguientes características:

- Requiere gran cantidad de memoria y capacidad de procesamiento
- Genera largas cabeceras en los mensajes.
- Comunicación con los agentes orientada a conexión.
- Estructura de funcionamiento distribuida.
- Permite jerarquía de sistemas de operación.
- Asegura que los mensajes llegan a su destino.
- Orientado a gestión por eventos

CMIP ofrece soporte en términos de seguridad tales como:

- Control de acceso.
- Soporte para autorizaciones.

- Archivos de registros de seguridad (Logs).
- Reportes de condiciones de red inusuales.

Las desventajas de CMIP para el usuario es que se utiliza diez veces más recursos de red respecto a SNMP (Bastidas , et al., 2011), esto quiere decir que se requiere mayor capacidad de procesamiento y de memoria en los routers y servidores, complejidad en su implementación, la cual conlleva a precios elevados.

2.7.2 Protocolo Simple de Gestión de Red (SNMP)

En 1988, el Comité de Actividades Internet IAB creó el protocolo de gestión SNMP, con la idea de un protocolo para el seguimiento del funcionamiento de redes, detección y análisis de fallos, configuración de los dispositivos de red, y que provocara poca sobrecarga en la red. Al ser un protocolo sencillo ayuda a reducir tiempo y costos al momento de desarrollar nuevas aplicaciones y actualizaciones. SNMP opera en el nivel de capa aplicación, utilizando TCP/IP (Calvo, 2016)**.**

Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de los parámetros de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

SNMP trabaja comúnmente sobre el protocolo UDP y tiene la ventaja de soportar otros protocolos como OSI CLNS, DDP, AppleTalk, entre otros.

Versiones SNMP

- SNMPv1: Diseñado a mediados de los 80. Fue una solución temporal hasta la llegada de protocolos de gestión de red más completos.
- SNMPv2: Es la evolución del protocolo SNMPv1 que apareció en el año 1993. A diferencia de la primera versión SNMPv2 cuenta con un mayor número de colecciones de datos, códigos de error y operaciones.
- SNMPv3: Es la última versión del protocolo SNMP creada en 1997. Esta versión no es un reemplazo de sus antecesoras SNMPv1 y SNPv2, sino que debe ser usada en conjunto con éstas para suministrar mejores prestaciones en cuanto a seguridad y administración.

2.8 Biblioteca de infraestructura de tecnologías de información (ITIL v3)

ITIL (Information Technology Infraestructura Library) es un marco de referencia de mejores prácticas para la gestión de servicios de TI de una organización, aplicada en empresas del sector público y privado. ITIL brinda las herramientas necesarias a organizaciones o empresas para que alcancen sus objetivos y lograr transformar, aumentar el éxito y crecimiento, reduciendo costos de operación.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de cada organización (2010).

2.8.1 Ciclo de vida de servicio

El Ciclo de Vida del Servicio consta de cinco fases que se muestran a continuación en la figura 5.

Figura 5

Ciclo de vida de los servicios ITIL v3

Nota. Recuperado de (Kaiser, 2011)

Las cinco fases del ciclo de vida de los servicios que propone ITIL v3 se estructuran de la siguiente manera:

2.8.1.1 Estrategia de servicio

Se ocupa del diseño, desarrollo e implantación de la gestión de servicios de TI que responda a una necesidad de las ramas de la organización. Se apoya en un grupo de procesos, funciones y actividades:

- Gestión de la relación con el negocio
    - Mantener las relaciones con los clientes
    - Identificar los requerimientos del servicio
    - Definir servicios estándares con los clientes
    - Encuestas de satisfacción del cliente
    - Manejar las quejas de los clientes
    - Monitorear las quejas de los clientes

- Gestión de la Estrategia de Servicio
    - Evaluación de la estrategia del servicio
    - Definición de la estrategia del servicio
    - Ejecución de la estrategia del servicio
- Gestión del Portafolio de Servicio.
    - Definir y analizar servicios nuevos y/o sus cambios

2.8.1.2 Diseño del servicio:

Se encarga del diseño y desarrollo de los servicios y de los correspondientes procesos necesarios para apoyar dichos servicios. Entre los procesos del diseño de servicios figuran:

- Coordinación del diseño
    - Soporte de coordinación del diseño
    - Servicio de Planificación de diseño
    - Coordinación del diseño del servicio y Monitoreo
    - Diseño del servicio técnico y organizacional
    - Servicio de Revisión de Diseño y Presentación RFC
- Gestión del Catálogo de Servicio
- Gestión de los Niveles de Servicio (SLM)
    - Mantenimiento del marco de SLM
    - Identificación de los requisitos del servicio
    - Acuerdos Sign-Off y activación de servicios
    - Servicio de Monitoreo de Nivel del Servicio y Reportes
- Gestión del Riesgo
    - Apoyo a la Gestión de Riesgos
    - Análisis de Impacto en el Negocio y de Riesgos

    - Evaluación de la Mitigación de Riesgos requerida
    - Seguimiento del Riesgo
- Gestión de la Capacidad
    - Gestión de la Capacidad del Negocio
    - Servicio de Gestión de la capacidad
    - Componente de Gestión de la capacidad
    - Informes de la gestión de la capacidad
- Gestión de la Disponibilidad
    - Servicio de diseño de la disponibilidad
    - Pruebas de disponibilidad
    - Monitoreo e informes de la disponibilidad
- Gestión de la Continuidad del Servicio de IT (ITSCM)
    - Soporte ITSCM
    - Servicios de diseño para la continuidad
    - Entrenamiento y Pruebas de ITSCM
    - Evaluación de ITSCM
- Gestión de la Seguridad de Información
    - Diseño de los Controles de Seguridad
    - Pruebas de Seguridad
    - Gestión de incidentes de seguridad
    - Evaluación de Seguridad
- Gestión de las regulaciones
- Gestión de la arquitectura de TI
- Gestión de Proveedores

2.8.1.3 Transición del servicio

Se ocupa del desarrollo y la puesta en producción de los nuevos servicios, además de mejorar los servicios en funcionamiento. Entre estos procesos de transición se encuentran:

- Gestión de Cambios
  - Soporte para la Gestión de Cambios
  - Evaluación de Cambios propuestos
  - RFC Logging y Pre-Evaluación
  - Evaluación e implementación de cambios de emergencia
  - Evaluación de cambios por el administrador de cambios
  - Evaluación de cambios por el consejo de asesores de cambios (CAB)
  - Programación de cambios y montaje de autorización
  - Autorización de despliegue de cambios
  - Despliegue de cambios menores
  - Revisión Post Implementación y cierre de cambios
- Evaluación de cambios
  - Evaluación de cambios previa a planeación
  - Evaluación de cambios antes de montaje
  - Evaluación de cambios previa a la implementación
  - Evaluación de cambios después de la implementación
- Planeación y soporte de la transición
  - Iniciación de proyecto
  - Planeación de proyecto y coordinación
  - Control de proyecto
  - Reportes de proyecto y comunicación

- Personalización y desarrollo de aplicaciones
- Gestión de versiones y liberación
    - Soporte a la gestión de liberación
    - Planeación de la liberación Versión de lanzamiento
    - Implementación de liberación
    - Soporte vital inicial
    - Cierre de liberación
- Validación y pruebas del servicio
    - Definición del modelo de pruebas
    - Adquisición de componentes de liberación
    - Pruebas de liberación
    - Pruebas de aceptación del servicio
- Gestión de la Configuración y de los activos del servicio
    - Identificación de configuración
    - Control de Configuración
    - Verificación y auditoria de la Configuración
- Gestión del Conocimiento No definido

2.8.1.4 Operaciones de servicio

Se ocupa de la coordinación, las actividades y los procesos necesarios para gestionar los servicios destinados a usuarios y clientes de empresas dentro de los niveles de servicio acordados. Los procesos de las operaciones de servicio son los siguientes:

- Gestión de eventos
    - Mantenimiento de los mecanismos de supervisión de eventos y reglas
    - Filtrado de eventos y correlación de primer nivel

    - Correlación de Segundo nivel y selección de respuesta
    - Revisión de eventos y cierre
- Gestión de Incidentes
    - Soporte a la gestión de incidentes
    - Registro de Incidentes y categorización
    - Resolución de incidentes inmediatos por soporte de primer nivel
    - Resolución de incidentes por soporte de Segundo nivel
    - Manejo de incidentes mayores
    - Monitoreo de incidentes y escalamiento
    - Cierre de incidente y evaluación
    - Información de usuarios Pro-Activa
    - Reporte de gestión de incidentes
- Gestión de Requerimientos
    - Soporte de solicitudes de requerimientos
    - Registro de solicitudes y categorización
    - Modelo de ejecución de solicitudes
    - Monitoreo de solicitudes y escalamiento
    - Cierre y evaluación de solicitudes
- Gestión de Accesos
    - Mantenimiento del catálogo de los roles de usuario y perfiles de acceso
    - Procesamiento de solicitudes de acceso de usuarios
- Gestión de Problemas
    - Identificación proactiva de problemas
    - Categorización de problemas y priorización
    - Diagnóstico de problemas y resolución

    - Control de Problemas y errores
    - Cierre y evaluación de Problemas
    - Revisión de problemas mayores
    - Reporte de gestión de Problemas
- Control de las Operaciones de TI
- Gestión del ambiente físico
- Gestión de las Aplicaciones
- Gestión Tecnológica

2.8.1.5 Mejora continua del servicio

Se ocupa de mejorar los servicios de forma constante para garantizar a las organizaciones que los servicios responden a las necesidades del negocio. La mejora continua trata sobre cómo mejorar el servicio, los procesos y las actividades de cada una de las fases del ciclo de vida. (BAUD, 2016)

- Revisión del servicio
- Evaluación de los procesos
    - Soporte a la gestión de procesos
    - Proceso de evaluación comparativa
    - Proceso de evaluación de madurez
    - Proceso de Auditoria
    - Control y revisión de procesos
- Definición de las iniciativas del CSI
- Monitoreo de las iniciativas del CSI

2.9 Análisis del modelo de gestión OSI e ITIL v3

Dado que las organizaciones dependen cada vez más de la tecnología de la información (TI) para lograr el objetivo comercial, es conveniente que los administradores de red estén familiarizados con los modelos de administración de redes, que sean capaces de administrar redes escalables para minimizar el tiempo de inactividad. Sin embargo, la capacidad para identificar potenciales problemas y rectificar el tiempo que toma reparar un fallo del sistema o componente, es una distinción característica de la dinámica de la red de gestión requerida para una TI sostenida y brindar servicios a una organización.

Por lo tanto, este estudio intenta realizar una radiografía de la estructura operativa del modelo de administración de red FCAPS (falla, configuración, contabilidad, rendimiento, seguridad), de La Biblioteca de Infraestructura de Tecnologías de Información ITIL, un mapeo de sus enfoques y cómo se relacionan entre sí para brindar TI sostenida y servicio para la mejora empresarial de la organización.

Los modelos de gestión de TI, están enfocados a brindar pautas y crear lineamientos orientados a las mejores prácticas de gestión y gobierno de TI. Los modelos de gestión de red establecen protocolos y áreas funcionales que deben ser gestionadas en una red de comunicación, por lo que es necesario combinarlos para obtener un modelo completo que cumpla los dos aspectos. Es necesario un análisis de los modelos de gestión de red estándar que permitan adaptar las principales ventajas de cada modelo y asociarlo a las mejores prácticas de gestión de TI. El modelo ITIL es un proceso para establecer prácticas de buen uso que determina una clasificación en diferentes grupos de gestión. Sirve para cualquier proceso de negocio relacionado con las tecnologías de la información, de esos grupos se puede escoger las FCAPS (Felicio, Alexandre, & Jacomo, 2014). A continuación, se muestra en la tabla 1 una comparativa FCAPS e ITIL (Tabla 1).

Tabla 1

Comparación de ITIL v3 y FCAPS

FCAPS	ITIL v3
Funciones de gestión categorizadas 5	Funciones de gestión categorizadas en 5 de prestación de servicios y soporte de servicios para ITIL v3. ITIL hizo hincapié en la gestión de servicios.
FCAPS hace hincapié en la gestión de tecnología (redes)	Las actividades de gestión del rendimiento de FCAPS están a cargo de la gestión de la capacidad, la gestión de la disponibilidad, la gestión de la continuidad y la gestión del nivel de servicio de ITIL.
Actividades de gestión de rendimiento	
Actividades de gestión de contabilidad	Las actividades de gestión contable de FCAPS están a cargo de la gestión financiera de ITIL.
Operaciones de gestión de la configuración	Las actividades de gestión de la configuración de FCAPS están a cargo de la gestión de cambios de gestión de configuración de ITIL y la gestión de versiones.
Operación de gestión de fallos	Las actividades de gestión de fallas de FCAPS están a cargo de la gestión de incidentes y problemas de ITIL.
Operaciones de gestión de seguridad	Las actividades de gestión de seguridad de FCAPS están a cargo de la gestión de seguridad de TI de ITIL.
FCAPS tiene su origen en TMN, ISO e ITU-T	ITIL tiene su origen en OGC[1] y el gobierno británico

Nota. Adaptado de (Lorge, Ricci, & Iglesias, 2020), (Iqbal & Nieves, 2011)

[1] OGC.- Oficina de Comercio Gubernamental del Reino Unido. Su objetivo es definir estándares y proporcionar las mejores prácticas orientadas a procesos para la gestión de servicios de TI.

FCAPS divide la función de administración en cinco categorías que consisten en fallas, configuración, contabilidad, desempeño y seguridad. Sin embargo, estas cinco categorías describen solo los cinco tipos diferentes de información que maneja el sistema de gestión y no los roles con respecto al negocio.

La tarea y la responsabilidad de administrar una red es una actividad que involucra diversas áreas de conocimiento, por lo cual los administradores de red se enfrentan, a un reto de elegir el modelo, norma y marco de referencia correcto para obtener una eficiente administración de la red de datos, debido a la variedad de enfoques y marcos de referencia alternativos que existen en el mercado.

La unión de FCAPS con el conjunto de buenas prácticas de ITIL v3, permiten tener un conjunto de procesos y lineamientos, específicos que guían hacia una correcta administración de la red de datos y garantizar que los servicios de TI se proporcionen de acuerdo a los niveles de servicio acordados con el cliente.

Tabla 2

Mapeo de funciones ITIL v3 al modelo FCAPS

	Funciones FCAPS				
Categoría de funciones ITIL	Fallos	Configuración	Contabilidad	Rendimiento	Seguridad
Administración de incidentes (O)	X				
Manejo de problemas (O)	X				
Gestión de configuración (T)		X			
Gestión del cambio (T)		X			
Gestión de la liberación (T)		X			
Gestión financiera (E)			X		
Gestión de capacidad (D)				X	
Gestión de continuidad (D)				X	

Administración de disponibilidad (D)	X	
Gestión de nivel de servicio (D)	X	
Gestión de seguridad de TI (D)		X

Nota. Adaptado de (Lorge, Ricci, & Iglesias, 2020), (Iqbal & Nieves, 2011)

Tanto FCAPS como ITIL se superponen en sus conceptos individuales, es decir, todos juntos muestran los mismos conceptos, pero con diferente enfoque y abstracción. Si bien FCAPS pone mayor énfasis en la tecnología, ITIL tiene su punto focal en el servicio comercial (tabla 2).

En el ANEXO A se detalla una descripción completa del mapeo entre FCAPS e ITIL v3.

2.10 Mejores Prácticas Corporativas

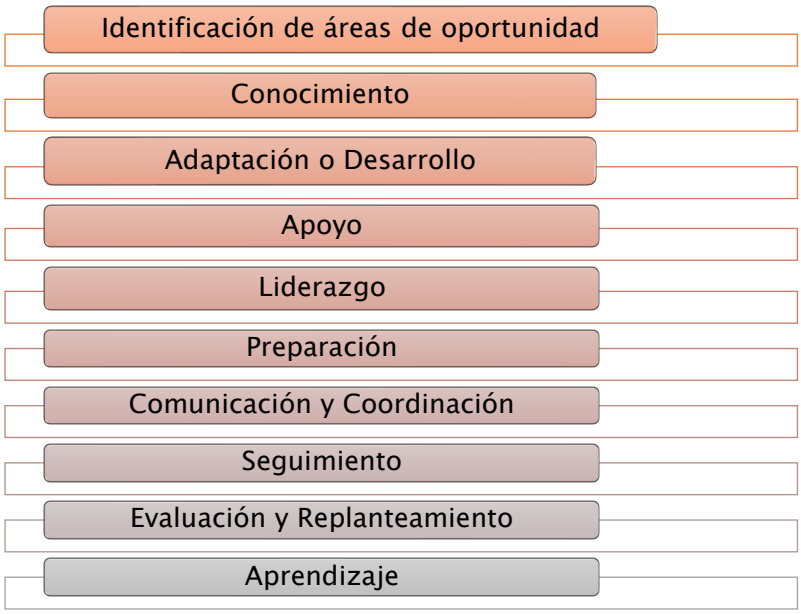
El Instituto Mexicano De Mejores Prácticas (IMMPC, 2021) se refiere a las Mejores Prácticas Corporativas como una recopilación de metodologías, sistemas, herramientas y procesos que han sido utilizadas y probadas con resultados sobresalientes en negocios que han sido reconocidos como de clase mundial.

Sin embargo, es cierto que este concepto no debe limitarse a lo que este tipo de negocios ha implementado, sino que también debe incluir las prácticas que las pequeñas, medianas, grandes y locales empresas han desarrollado e implementado para lograr mejores resultados, o aquellas que han sido tomados, adaptados y transformados para satisfacer sus necesidades.

A lo largo de la evolución de la gestión, el control y la gobernanza empresarial, han surgido conceptos que hoy sirven como base de lo que llamamos "Mejores Prácticas Corporativas", y que son necesarios para mejorar el desempeño organizacional en términos de conocimiento y comprensión, permitiendo a cada empresa evaluar la forma en que se pueden implementar y que en un futuro podrán contribuir a ampliar la base de Mejores Prácticas existentes.

Figura 6

Factores críticos de éxito para la implementación de Mejores Prácticas Corporativas



Nota. Adaptado de (IMMPC, 2021)

La implementación de las mejores prácticas en las empresas permite potencializar procesos estratégicos, operativos y administrativos de forma metódica.

Empresas que se han enfrentado a la necesidad de buscar y encontrar la forma de afrontar sus retos de forma más ordenada como resultado de su nivel operativo, de crecimiento y competitivo han dado lugar a proyectos o iniciativas que han emprendido para lograrlo, contribuyendo potencialmente a un crecimiento más ordenado.

Con el paso del tiempo, estas prácticas han sido documentadas, depuradas y publicadas, ya sea por la misma empresa o por especialistas dedicados a la investigación de diversas escuelas de negocios, institutos, instituciones o asociaciones de diversas especialidades o ámbitos. Muchos más proceden de investigadores o especialistas que los han utilizado, adaptado y perfeccionado a lo largo del tiempo en diversas organizaciones (IMMPC, 2021).

2.11 Trabajos Relacionados

A continuación, se detallan algunos trabajos de investigación afines al tema de investigación.

Muharman (2020), en su trabajo, Optimización de la gestión del rendimiento con FCAPS e ITIL v3: Oportunidades y obstáculos, realizado en Indonesia, propone un escenario de prueba de dos diseños de topología de red (cableada e inalámbrica) con el propósito de mejorar la calidad de los servicios de red en el gobierno rural, especialmente para mejorar el rendimiento y facilitar o gestionar la infraestructura y los servicios de red. Las pruebas se realizaron utilizando escenarios para el análisis de salida y la pérdida de paquetes como parámetros. En base a la investigación llevada a cabo en el análisis y optimización de la infraestructura de red en el gobierno rural utilizando el marco FCAPS, presenta un estándar de referencia para la implementación de la gestión del desempeño basado en el diseño de servicios ITIL y un diseño de actividades de gestión del desempeño utilizando el marco FCAPS.

En el trabajo de Enose (2012), realizado en Kollam - India, plantea un sistema que es una combinación del Sistema de administración de redes de telecomunicaciones (NMS) y el Sistema de administración de infraestructura de servicios públicos. Este sistema de gestión se basa en el modelo probado y aceptado por la industria de FCAPS (es decir, gestión de fallos, gestión de la configuración, gestión contable, gestión del rendimiento, gestión de la seguridad) junto con el conjunto de mejores prácticas para la gestión de servicios de TI (ITIL). Esta combinación de conceptos en una vista de panel único proporcionaría una mejor plataforma para administrar la compleja infraestructura de Smart Grid.

El proyecto realizado por Estrada, Romero, & Vera (2014), mediante un estudio teórico, se desarrollan las diferentes áreas funcionales del modelo de gestión de red FCAPS, se muestra

el porqué de la necesidad de implementar un modelo de gestión en una organización y se definen una serie de indicaciones o conclusiones para llevar a cabo una buena gestión de los recursos. Además, se introduce los distintos módulos del software SolarWinds para llevar a cabo una buena gestión de red.

Como aporte de este trabajo de investigación la empresa adquirirá factores positivos como procesos de TI con mayor madurez, generación de mayor productividad (menos errores en la operatividad de la infraestructura tecnológica), mejora en los tiempos de resolución de incidentes, mayor calidad en los procesos diarios de TI (hacer las actividades siempre igual), apalancando a una mejor imagen corporativa de la empresa y posibilitando el incremento de la cartera de clientes corporativos.

Esto constituye un aporte para mejorar los procesos interno de la unidad de TIC y la imagen corporativa de la empresa, permitiendo que tenga un control total de la infraestructura tecnológica, garantizando la operatividad, el manejo eficiente de recursos y la satisfacción del cliente interno como algunos de los aspectos clave que se pueden administrar a través de la mesa de servicios.

2.12 Software de Gestión

El software de gestión está diseñado para ayudar en la configuración, administración y monitoreo de redes informáticas, es decir reducir la complejidad de grandes proyectos y tareas, que simplifican los procesos operativos, productivos y administrativos de una organización. Las aplicaciones de software de red están disponibles para administrar y monitorear redes de todos los tamaños, desde pequeñas redes domésticas hasta grandes redes comerciales (Beal, 2021).

2.13 Estándar ISO / IEC / IEEE 29148: 2018

Esta norma incluye disposiciones para procesos y productos relacionados con la ingeniería de requisitos para sistemas, productos y servicios de software a lo largo del ciclo de vida de un producto. Define los elementos de una buena solicitud, proporciona atributos y características de la solicitud y examina la aplicación iterativa y recursiva de los procesos de solicitud a lo largo del ciclo de vida, el detalle de cada sección se encuentra en el ANEXO B. Esta norma proporciona un ejemplo práctico figura 7, de una especificación de requisitos de software (SRS).

Figura 7

Documento de especificación de requisitos de software (SRS)

1. **Introducción**
   - 1.1 Propósito
   - 1.2 Alcance
   - 1.3 Descripción general del producto
     - 1.3.1 Perspectiva del producto
     - 1.3.2 Funciones del producto
     - 1.3.3 Características del usuario
     - 1.3.4 Limitaciones
   - 1.4 Definiciones
2. **Requisitos Específicos**
   - 2.1 Interfaces externas
   - 2.2 Requisitos funcionales
   - 2.3 Requisitos de usabilidad
   - 2.4 Requisitos de rendimiento
   - 2.5 Requisitos de la base de datos
   - 2.6 Atributos del sistema
3. **Siglas y Abreviaturas**
4. **Referencias**

Nota. Adaptado de (ISO, IEC, & IEEE, 2011)

2.14 Plataformas de gestión

Hoy por hoy existen varias herramientas disponibles para gestionar redes; sin embargo, la implementación de estas herramientas en las instituciones u organizaciones que las requieran depende de algunos factores:

- Orientación de la institución.
- Disponibilidad de recursos económicos.
- Equipos de red disponibles en la institución.
- Personal a cargo de la administración de la red.

Existen múltiples herramientas de tipo comercial y software libre, varias de ellas se enfocan en las necesidades específicas del administrador y otras son más generales.

2.14.1 Herramientas de gestión comercial

Son muy completas y complejas, adaptables a grandes redes, costos adicionales por adición de componentes o utilidades, soluciones cerradas, es decir no permiten la personalización de funcionalidades.

2.14.1.1 HP OpenView

Es un software de gestión de red que proporciona un conjunto de soluciones de software para administrar y optimizar los servicios de red en una infraestructura de tecnologías de imagen, voz y datos. Descubre todos los elementos a los que tiene acceso y los agrega a la topología, muestra además un sistema de alertas de los que tiene configurados. La suite de OpenView incluye elementos que cubren los siguientes aspectos:

- ✓ Automatización del centro de datos.
- ✓ Gestión de almacenamiento.

- ✓ Gestión de configuración.
- ✓ CMDB universal.
- ✓ Service Desk
- ✓ Analizador de transacciones.

A pesar de que este es un sistema muy completo, el costo de implementación es muy elevado. Además, para que el software funcione correctamente, se requiere una máquina sumamente “eficaz” (PandoraFMS, 2021).

2.14.1.2 SolarWinds

Una de las herramientas de monitoreo de red más conocidas. Se distingue por su mapeo automático de redes y nodos, lo que elimina la necesidad de acciones manuales. Posee una interfaz gráfica muy robusta que le permite ver fácilmente la topología de la red y su estado actual. SolarWinds permite integrar máquinas virtuales en su monitoreo.

Es una excelente opción para las pequeñas empresas, pero deben poder pagar el precio de sus licencias (que se encuentran entre las más caras del mercado) (Pandora FMS team, 2021).

2.14.1.3 IBM Tivoli

IBM Tivoli Monitoring supervisa y gestiona aplicaciones de red y sistemas en una amplia gama de sistemas operativos, realiza un seguimiento de la disponibilidad y el rendimiento del sistema y proporciona informes para realizar un seguimiento de las tendencias y resolver problemas (IBM, 2013).

2.14.2 Herramientas de gestión libre

Es cualquier programa donde el usuario goce de las libertades para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software.

2.14.2.1 Nagios

Nagios es un software de código abierto diseñado para el monitoreo continuo y automatizado de sistemas informáticos y tecnologías de infraestructura de comunicación.

Sus características principales son:

- ✓ Monitorización de servicios de red.
- ✓ Monitoreo de recursos (CPU, Memoria, Discos, etc.)
- ✓ Le permite especificar contactos para la entrega de notificaciones.
- ✓ Permite que la gestión de eventos se realice de forma proactiva.
- ✓ Registro de eventos.
- ✓ Visualización a través de una interfaz web (contributors, EcuRed, 2016).

2.14.2.2 Cacti

Cacti es una interfaz web escrita en PHP, se basa en RRDTool[2] y MySQL[3], Recopila y guarda la información necesaria para crear gráficos, mantiene fuentes de datos, archivos rotativos y genera gráficos basados en los datos recopilados.

Incluye la gestión de usuarios, con diferentes permisos de visualización y creación de nuevos gráficos asignados a cada usuario (The Cacti Group, n.d.). Puede usarse en Linux, Solaris, BSD e incluso Windows. Algunas de sus características son:

- ✓ Permite la creación de usuarios y la adición de permisos
- ✓ Agrega un número ilimitado de elementos a cada gráfico.

[2] RRDTool.- Es un sistema de registro de datos de alto rendimiento estándar de la industria OpenSource para datos de series temporales.

[3] MySQL.- Es un servicio de base de datos completamente administrado para implementar aplicaciones nativas de la nube.

- ✓ Admite la creación de scripts personalizados.
- ✓ Permite la organización de datos en estructuras jerárquicas
- ✓ Basado en soporte SNMP.
- ✓ Permite la creación de usuarios y la adición de permisos

2.14.2.3 Zabbix

Es un software de monitoreo de red escrito en código fuente abierto. Es posible recopilar datos de miles de servidores, máquinas virtuales y dispositivos de red simultáneamente con esta herramienta. Dispone de almacenamiento de datos, características de visualización versátiles (vistas panorámicas, mapas, gráficos, pantallas, etc.), así como una amplia gama de métodos de análisis de datos para detectar y alertar problemas (Zabbix LLC, 2016).

- ✓ La recopilación de datos
- ✓ Verificaciones de disponibilidad y rendimiento
- ✓ Soporte para SNMP (captura y sondeo), IPMI, JMX, supervisión de VMWare
- ✓ Controles personalizados
- ✓ Recuperación de los datos deseados a intervalos predeterminados

2.14.2.4 Zenoss

Es un software híbrido de monitoreo y análisis de TI, que proporciona las funciones necesarias para administrar de manera eficiente la configuración, la estabilidad y el rendimiento de la red. Cuenta con una versión gratuita y dos versiones comerciales (Pandora FMS team, 2021). Sus principales características son:

- ✓ La detección de dispositivos es automática
- ✓ Tiene una interfaz web.
- ✓ Generación automática de eventos

- ✓ Envío de correo electrónico y SMS
- ✓ Tablero personalizado
- ✓ Genera informes multigráfico.

Las herramientas utilizadas para monitorear una red pueden variar según las necesidades de la organización, como dispositivos que analizan los datos que fluyen a través de la red o monitores que rastrean todo el tráfico de las conexiones, sistemas de inventarios, herramientas de notificación de alertas y alarmas, entre otras. Estas son herramientas que ayudan a los dispositivos a realizar un trabajo adicional (Robles, 2014).

De acuerdo a la investigación denominada "Implementación de los Sistemas de Gestión de la red en dos universidades americanas" describe herramientas asociadas a las áreas del modelo FCAPS (Tabla 3), las cuales se tomarán en cuenta para la selección de las herramientas complementarias de nuestro modelo.

Tabla 3

Herramientas de gestión asociadas al modelo FCAPS

Categorías FCAPS	Software
Gestión de Fallos	Nagios, LightSquid, SARG
Gestión de Configuración	NetDot, Bacula, Nagios, OCS Inventory, Rancid
Gestión de Contabilidad	SQStat, FreeSA, Webalizer, Sendmail Analizer, OCS Inventory
Gestión de Rendimiento	MRTG, Cacti, FlowViewer, NFsen+NFsight+SSHCUre, SmokePing, LibreNMS, Nagios
Gestión de Seguridad	NFsen+NFsight+SSHCUre, Flow Viewer, OSSIM, Bacula, SmokePing, MRTG, Cacti

Nota. Adaptada de (Linares, Sánchez, & Marcillo, 2017)

El detalle de las características generales de las herramientas se encuentra en el ANEXO C.

3. CAPÍTULO III

SITUACION ACTUAL DE LA EMPRESA Y MODELO DE GESTIÓN DE RED

El objetivo de este capítulo es conocer la situación actual de la empresa sobre los procesos de TI, su estructura organizacional, topología de red y la descripción de los recursos físicos y lógicos que conforman la red, para comprender el entorno en el que se desarrollará el proyecto.

Mediante visita técnica se realizó una auditoría lógica y de comunicaciones para determinar las características de la Infraestructura de red, adicional a esto se realizó una encuesta que sirvió para recolectar la documentación de los procedimientos realizados en la unidad de TI, permitiendo así conocer el estado actual de la red.

Para ello, conoceremos la misión, visión y objetivos estratégicos de la empresa, teniendo en cuenta la recolección y análisis de los datos principalmente de los procesos que se llevan a cabo en el departamento de TI, los cuales se realizarán a través de una revisión de la documentación del área y entrevistas con el personal implicado.

3.1 JASSA TELECOM CIA. LTDA.

JASSA TELECOM es una empresa legalmente constituida y suscrita en la Superintendencia de Compañías en el mes de septiembre del 2015, las actividades principales giran alrededor de dos líneas estratégicas de proyectos de construcción civil y de las tecnologías de la información y comunicación a nivel nacional, con una proyección en soluciones de diseño arquitectónico.

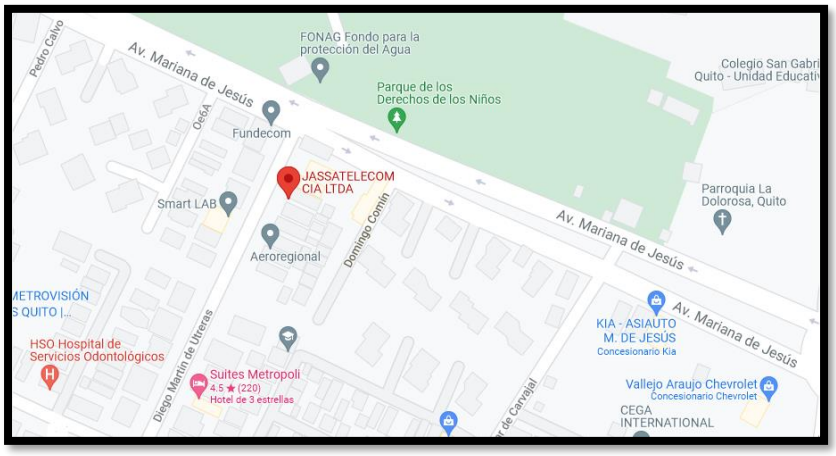
Durante este periodo la empresa ha desarrollado diferentes alianzas estratégicas con varios clientes, con los cuales mantienen relaciones comerciales, presentando como garantía su trabajo de alta calidad y eficiencia en la entrega del trabajo asignado.

3.1.1 Ubicación

La institución está alojada en la ciudad de Quito, ubicada en la calle Martín de Utreras N31-276 y Av. Mariana de Jesús, la micro y macro localización se observan en las Figuras 8 y 9.

Figura 8

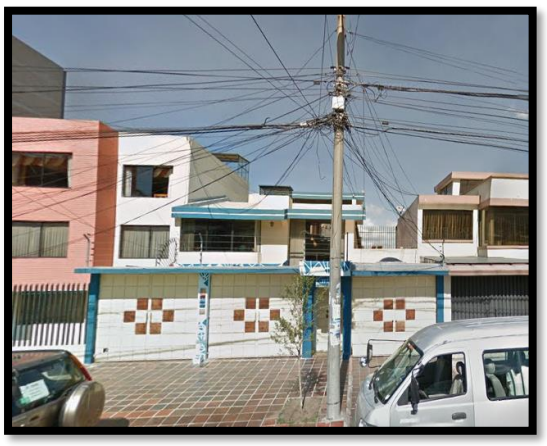
Macro localización de la empresa JASSA TELECOM



Nota: Recuperado de Google Maps.

Figura 9

Micro localización de la empresa JASSA TELECOM



Nota: Recuperado de Google Maps

3.1.2 Misión y Visión

La empresa (JASSATELECOM, 2019) tiene como misión:

“Facilitar la vida de sus clientes, con soluciones integrales garantizando calidad y continuidad de servicios en sus operaciones.

Y como Visión:

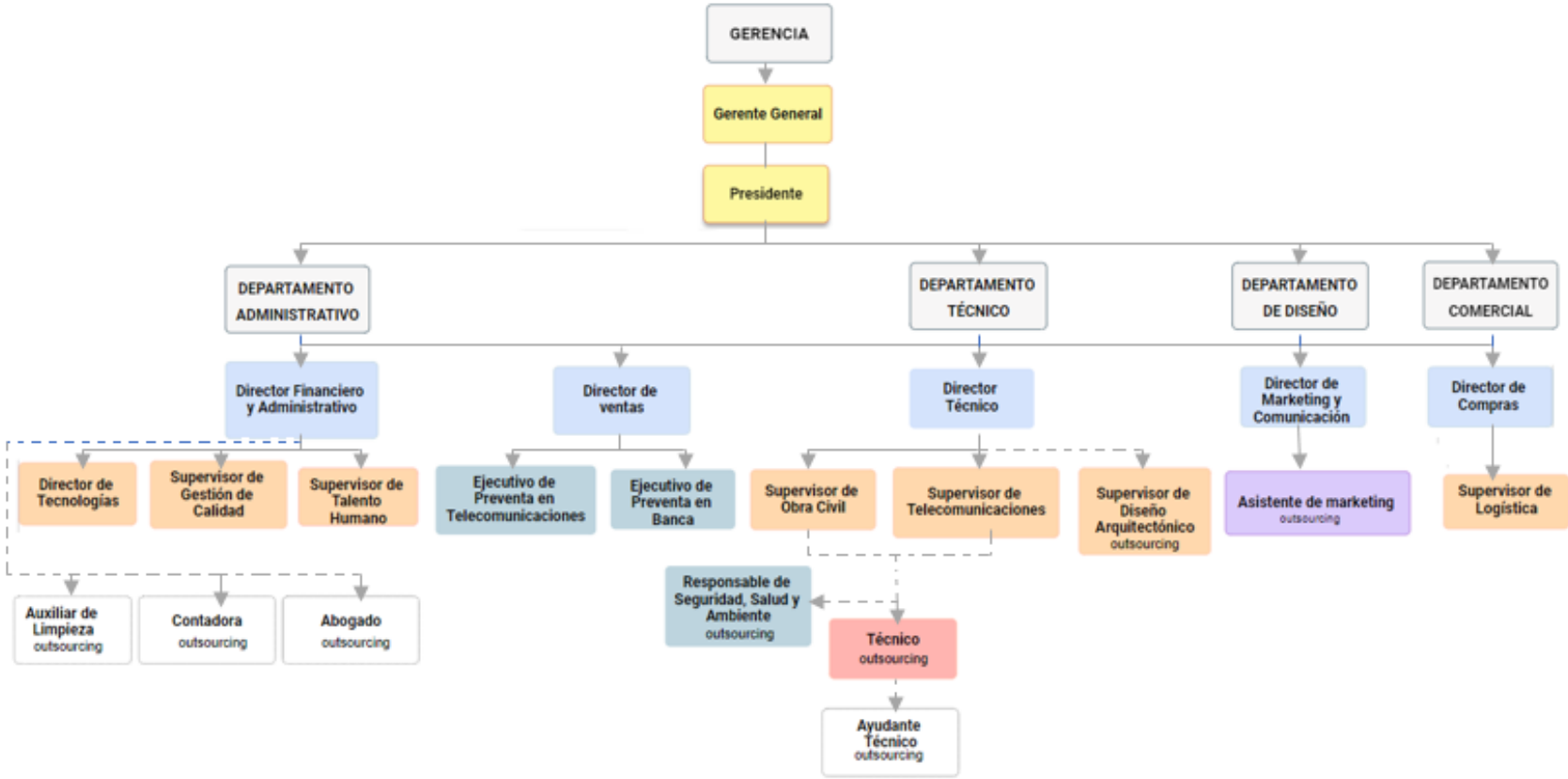
Ser una multinacional líder en el suministro, construcción e implementación de soluciones integrales de tecnologías”.

3.2 Organigrama Estructural

La empresa se encuentra conformada por diferentes áreas de trabajo como: Comercial, Marketing y Comunicación, Ingeniería TSS y demás áreas que se observan a continuación en la Figura 10 las cuales trabajan en conjunto para lograr alcanzar los objetivos y requerimientos del cliente.

Figura 10

Estructura Organizacional Empresa JASSA TELECOM



Nota: Elaboración propia basada en (JASSATELECOM, 2019)

3.2.1 Unidad de TIC (se debería incluir el nuevo organigrama de la empresa en donde conste la unidad de TIC.)

En la empresa JASSATELECOM, la Unidad de Gestión de Tecnologías de la Información y Comunicaciones (TIC), se encuentra conformado por 3 profesionales de TI, en este caso:

1 jefe de Tecnologías de Información

2 auxiliares de Tecnología de Información

El área interactúa con todas las áreas de la organización, especialmente con el área de Gerencia, área Administrativa y Financiera, ubicándose dentro de los procesos de soporte de la organización y dependiendo del Departamento Administrativo, como se muestra en el organigrama.

Las principales actividades de la Unidad de TIC son:

- Instalación y mantenimiento de infraestructura de redes y servicios de comunicaciones.
- Gestión de adquisiciones de material informático.
- Instalación y mantenimiento de pc's.
- Plan de mejora de la red y desarrollo de nuevos servicios.
- Servicio de internet a diferentes clientes y aplicaciones internos y externos.
- Administración de contratos con proveedores
- Gestión de Directorio Activo
- Gestión de seguridad de Información
- Apoyo informático a las diferentes áreas (JASSATELECOM, 2019).

3.2.1.1 Acceso a internet

La red de la empresa está conectada a Internet mediante el proveedor de servicios Claro el cual brinda un ancho de banda de 20 [Mbps]. Para el acceso a internet se emplea la interfaz de red G0/0/1 del equipo de seguridad perimetral la misma que se conecta directamente al equipo suministrado por el proveedor.

3.2.1.2 Direccionamiento IP

La asignación del direccionamiento IP para todos los equipos es dinámica (DHCP), el mismo que es provisto por el router Arris manejado por el proveedor de servicios de Internet. La dirección IP pública es manejada por el Router Arris e internamente se entregan IP privadas. Se manejan 4 Identificadores de Red (SSID) diferentes para la red inalámbrica, sin embargo, todos se encuentran en el mismo segmento y con los mismos permisos, el segmento manejado es: 192.X.X.X/24.

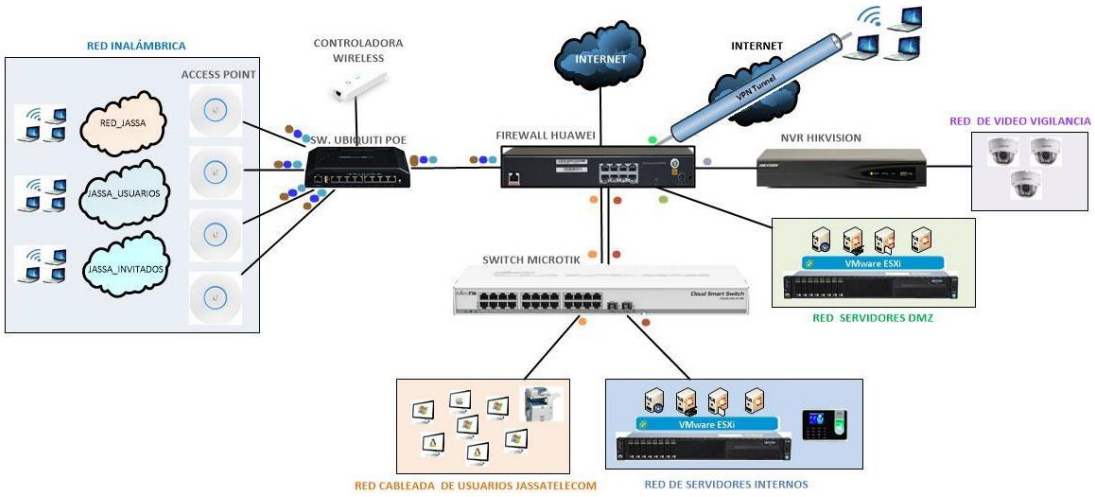
- **NOTA:** Las direcciones IP asignadas no se detallan por seguridad de la red interna de la empresa JASSA TELECOM.

3.3 Infraestructura tecnológica

Con la finalidad de mejorar el control y seguridad en el acceso a los recursos e información disponible, la empresa JASSA TELECOM cuenta con ocho segmentos de red o zonas de red controladas por el equipo de seguridad perimetral Huawei USG6320l, el mismo que permite aislar, filtrar y controlar los accesos entre los distintos segmentos de red. En la Figura 11 se describe la segmentación de red que posee JASSA TELECOM.

Figura 11

Topología Física de la empresa JASSA TELECOM



Nota: Recuperado de (JASSATELECOM, 2019)

Indicar aquí la topología de red y luego detallar cada área.

3.3.1 Red LAN Cableada

De este segmento de red forman parte todos los usuarios de JASSA TELECOM que se conectan mediante los puntos de red cableados disponibles en la empresa, los mismos que a su vez se encuentran conectados a los puertos del switch Microtik. Para este segmento de red se asignó el direccionamiento IP 192.X.X.X/24 y en el switch Microtik se creó la VLAN con identificador 51 de la cual forman parte los usuarios de JASSA TELECOM.

La distribución de los puertos en el switch Microtik para este segmento de red se detalla a continuación:

- Puertos 2 a 17 – Conexión usuarios de red cableada.
- Puerto 18 – conexión impresora de red.

- Puerto 19 – puerto de administración local.
- Puerto 20 – conexión interfaz ETH-2 Firewall.

3.3.2 Red de Servidores Internos

En este segmento de red están asociadas las máquinas virtuales que proporcionan los servicios y aplicaciones internas de JASSA TELECOM tales como ERP, Servidor de Controlador de Dominio, Servidor de archivos y Servidor FreeRadius. Para este segmento de red está asignado el direccionamiento IP 192.X.X.X/24 y en el switch Microtik se encuentra creada la VLAN con identificador 20 de la cual forman parte los servidores detallados anteriormente. La distribución de los puertos en el switch Microtik para este segmento de red se detalla a continuación:

Puertos 21- 23 conexión a red de servidores.

Puerto 24 - conexión interfaz ETH-4 Firewall.

3.3.3 Red de Servidores DMZ

En este segmento de red están asociados las máquinas virtuales que proporcionan los servicios y aplicaciones que JASSA TELECOM publica a internet, tales como servidor de aplicaciones web, servidor de correo electrónico entre otros.

3.3.4 Red de video vigilancia

En este segmento de red se encuentra incluido el NVR Hikvision y las cámaras utilizadas en el sistema de video vigilancia.

3.3.5 Red LAN Inalámbrica

En este segmento de red están los usuarios de JASSA TELECOM que mediante los Access Point Unifi UAP-AC se conectan a la red inalámbrica. Con el objetivo de aislar el

tráfico de los usuarios del departamento de gerencia o junta directiva de los demás usuarios y tener un mejor control en el acceso a la información de acuerdo a la función desempeñada dentro de la empresa, son tres segmentos de red asociados a la VLAN cuyos accesos se controlan y gestionan mediante el equipo de seguridad perimetral. Las VLAN se detallan a continuación:

- VLAN Gerencia. - De este segmento de red forman parte los usuarios del departamento de gerencia o junta directiva.
- VLAN Jassa Usuarios. - De este segmento de red forman parte los usuarios de la empresa que se conectan mediante la red inalámbrica de la empresa.
- VLAN Jassa Invitados. - Este segmento de red está destinado para el uso exclusivo de internet, empleado para los usuarios externos de la empresa (usuarios invitados) o por los dispositivos móviles.

Los Access Point Unifi se encuentran conectados al Switch POE Unifi en los puertos número 2, 3, 4 y 5. Mediante un enlace troncal (trunk) configurado en el puerto 8 desde el switch POE Unifi los Access Point se conectan al equipo de seguridad perimetral Huawei USG6320- AC el cual se encarga de controlar los accesos y establecer los permisos necesarios para las diferentes VLAN.

3.3.5.1 Virtualización

En el servidor Huawei RH2288 v3 se encuentra instalada la plataforma de virtualización VMware Vsphere ESXI versión 6.5 sobre la cual están creadas y configurados tres servidores virtuales. Adicional se encuentra creada una máquina virtual para la implementación de una solución ERP. En la figura 12 se visualiza la virtualización de equipos.

Figura 12

Virtualización de equipos

Nota: Recuperado de (JASSATELECOM, 2019)

En la tabla 4, se detallan las características de los servidores físico y virtual.

Tabla 4

Características Servidores Físico y Virtual

Servidor Físico	Sistema Operativo	Memoria RAM	Disco Duro
Huawei RH2288 V3	VMware ESXi 6.5	64 GB	8.18 TB
Servidor Virtual			
Servidor Controlador de Dominio	Ubuntu Server 18.04 LTS	4 GB	30 GB
Servidor de Archivos	Ubuntu Server 18.04 LTS	4 GB	2 TB
Servidor para Autenticación Freeradius	Debian 9.7	2 GB	30 GB
ERP	Debian 9.7	4 GB	500 GB

Nota: (JASSATELECOM, 2019)

3.4 Especificación técnica de los equipos de interconectividad.

En la tabla 5, se describen los equipos disponibles en la empresa.

Tabla 5

Especificaciones técnicas de equipos

EQUIPOS	CARACTERÍSTICAS	IMAGEN	FUNCIÓN
Huawei RH2288 v3	- 64 GB de Memoria RAM - Procesador Intel Xeon E5-2620v4 2.10 GHz - 2 Interfaces de Red - 4 discos SATA de 3 TB en arreglo RAID5 (8,18 TB de Capacidad utilizable)		- Este equipo cumple las funciones de almacenamiento y virtualización de servicios de TI.
Huawei USG6320 - AC	- Puertos de servicio obligatorios 8 × 10/100 / 1000M puertos eléctricos Ethernet con detección automática. - 1 Puerto de consola (RJ45). - 1 Puerto USB 2.0. - Rendimiento del cortafuegos IPv4. - Rendimiento del		- Cumple con la función de aislar, filtrar y controlar los accesos entre los distintos segmentos de red. Equipo de seguridad perimetral. - Se usa una interfaz Gigabit Ethernet para conectarse

	cortafuegos IPv6.		directamente al Router Arris.
Switch Microtik de 24 puertos *CRS326-24G*	- 24 Puertos 10/100/1000 Gigabit Ethernet. - 1 Puerto SFP 1.25G. 1 Puerto SFP+ 10G. 12-30 DC; PoE Pasivo.		- Equipo encargado de la gestión de LAN´s
Switch POE Unifi de 8 puertos	- 8 puertos Gigabit PoE. PoE pasivo configurable de 24V / 48V. - 150 W de potencia Interfaz de configuración de EdgeSwitch XP. - Puerto Ethernet: (1) RJ-45 10/100/1000Mbps.		- Equipo encargado de la gestión de VLAN´s
Controladora Wireless Cloud Key Unify	- Procesador: Quad-Core SoC. Memoria: 1GB DDR. Energía: 802.3af PoE o Micro-USB 5V, Mínimo 1A. - Máximo Consumo: 5W.		- Equipo encargado de la conectividad de la red inalámbrica WLAN

	- Puertos: 1 10/100/1000. - Estándar Inalámbrico:		
Access Point Ubiquiti UAP-AC-LR	802.11a/b/g/n/ac. - Frecuencia de Operación: 2.4 GHz & 5 GHz - Antenas: Triple Polaridad, Antena Dual Band de 3 dBi.		- Equipo encargado de la conexión de los usuarios a la red inalámbrica.
NVR HIKVISION	- Grabador de Vídeos en Red de 4 canales con 4 puertos PoE integrados. - Canales configurables de forma individual - 1 puerto SATA para 1 HDD con un máximo de 6 TB de capacidad - Canales de entrada de vídeo 4 canales - Máxima resolución 3840 x 2160 Pixels - Tecnología de cableado ethernet de cobre 10BASE-T,100BASE-TX Ethernet LAN, velocidad		- Cumple con la función de grabar y administrar imágenes y videos.

	de transferencia de datos 10,100 Mbit/s. - Tecnología EXIR 2.0 para visibilidad en condiciones de poca luz. - Filtro de corte IR para funcionalidad diurna y nocturna sistema de señal NTSC. - Ajuste de ángulo de tres ejes (pivote horizontal de 0 a 340°, pivote vertical de 0 a 75° y rotación de 0 a 360°) sincronización interna. - IR inteligente, brillo, nitidez, 3D-DNR y espejo.		
Hikvision TurboHD DS-2CE57D3T-VPITF			- Cumplen con la función de monitoreo, envío de imágenes y videos al NVR

Nota: Esta tabla muestra las características de los recursos físicos de la red (JASSATELECOM, 2019).

3.5 Análisis de la gestión de la infraestructura de TI

Para realizar el análisis de la gestión de la infraestructura, se realizó un diagnóstico basado en el plan estratégico de la empresa JASSA TELECOM en el área de TIC, así como entrevistas con el personal de la empresa, recolección de información mediante una encuesta.

3.5.1 Encuesta

El objetivo principal de la encuesta es identificar las debilidades y evaluar la gestión de infraestructura de TI, tomando como referencia el conjunto de buenas prácticas sobre gestión de servicios de TI (ITIL) y el modelo de gestión de red ISO (FCAPS). Las personas a las cuales se va a aplicar la encuesta son las que están relacionadas directamente con los servicios de tecnología.

Las preguntas de la encuesta están generadas en función del marco de referencia ITIL v3 y de la norma ISO FCAPS, de igual manera, se utilizó un conjunto de herramientas propuestas por ITSM para la gestión de servicios de TI (The ITIL Toolkit, 2019). En la tabla 6, se evalúan los 11 procesos que contiene ITIL para la gestión de red de infraestructura.

De acuerdo a los procesos de la ISO e ITIL se estructura la encuesta de la siguiente manera:

Tabla 6

Procesos

Procesos	Preguntas
Gestión de servicios definidos en el área de TI	3
Gestión Financiera de servicio de TI	3
Gestión del nivel del Servicio	7
Gestión de la capacidad	6
Gestión de la disponibilidad	6
Gestión de la Seguridad de la información	5
Gestión del cambio	5
Activos de Servicio y Gestión de la configuración	6

Gestión de la liberación y despliegue	7
Operación del servicio	10
Manejo de Problemas	10

Nota: Procesos seleccionados después del mapeo de FCAPS e ITIL v3

3.5.2 Muestra

Para la recopilación de información se aplica el muestreo no probabilístico, el cual es una condición en la que no se puede calcular la probabilidad de extraer una muestra determinada. Este proceso busca identificar a personas que tengan una comprensión sólida del tema en estudio y se considera que la información proporcionada por ellas es fundamental para tomar decisiones.

A continuación, en la tabla 7, se muestra al personal de la empresa que apoyó en el proceso de recopilación de información, siendo estos, los líderes de las áreas funcionales y operativas del modelo de negocio de la empresa. Se consideraron 11 personas, por lo tanto, no se utiliza ninguna técnica de muestreo y se aplica al total de la población.

Tabla 7

Personal encuestado

Nombre	Cargo en el que se desempeña	Correo
Alexander Trejo	Gerente General	alexander.trejo@jassatelecom.com
Javier Ibadando	Arquitectura	javier.ibadango@jassatelecom.com
Miguel Bravo	Product Manager	miguel.bravo@jassatelecom.com
Andrés García	Recursos Humanos	andres.garcia@jassatelecom.com
Rubén Acuña	Project Manager	ruben.acuna@jassatelecom.com
Jonathan García	Presidente	jonathan.garcia@jassatelecom.com

Jessica Trejo	Supervisión de Obra Civil	jessica.trejo@jassatelecom.com
Andrea León	Manejo de Calidad y Normativa ISO	andrea.leon@jassatelecom.com

Nota: Tomado de (JASSATELECOM, 2019)

3.5.3 Análisis de resultados

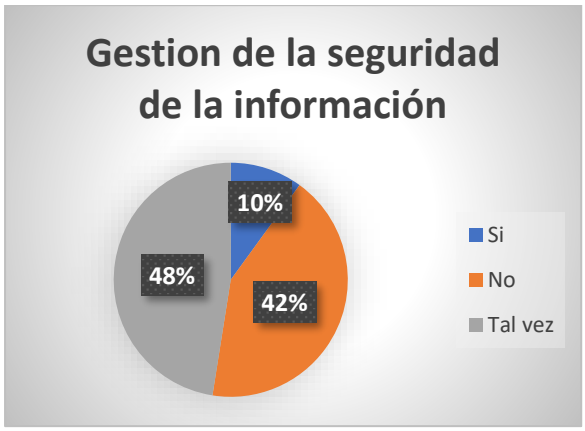
Para la presentación del análisis de resultados se ha elegido los procesos de ITIL v3 que tienen más relación con la gestión de red, el detalle de todos los procesos involucrados en la encuesta se encuentra en el Anexo B.

Proceso 1.- Gestión de la Seguridad de la Información

De los profesionales encuestados, el 48% manifiestan desconocimiento de una política de Seguridad de la Información, el 42% hace referencia a ciertos requisitos de seguridad y únicamente el 10% pueden identificar que existen definidos y conocen las políticas de seguridad existentes.

Figura 13

Conclusión preguntas (26-30)



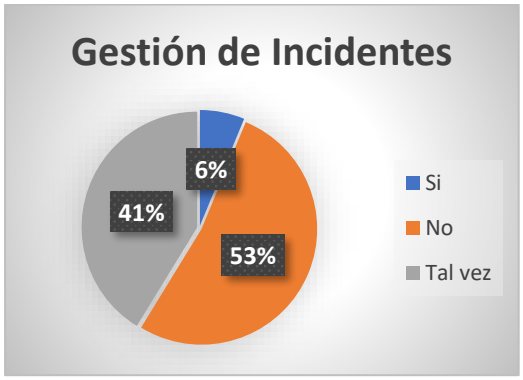
Nota: Políticas de seguridad

Proceso 2.- Gestión de Incidentes

El 53% de las respuestas desconocen de los establecimientos de políticas, diagnóstico y registros de incidencias, mientras que el 41% han escuchado de cierta priorización de incidentes y el 6% manifiesta que si se sigue un proceso para la gestión de incidentes.

Figura 14

Conclusión preguntas (49–58)



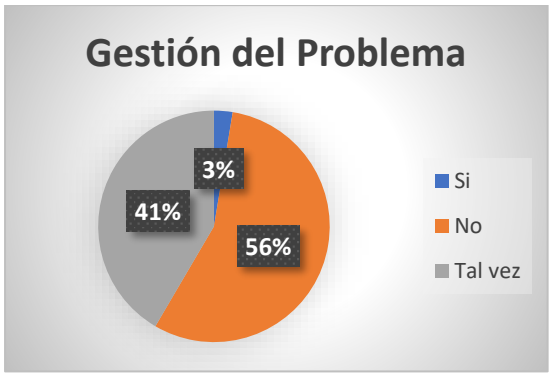
Nota: Gestión de Incidentes

Proceso 3.- Gestión de problemas

Existe el 56% que manifiesta que no existe la responsabilidad de garantizar que se lleve a cabo el análisis de la causa raíz de un problema, el 41% desconoce si se lleva un registro, resolución y cierre de problemas, el 3% afirma que se establecen y se llevan a cabo políticas, principios y conceptos básicos del manejo de problemas.

Figura 15

Conclusión preguntas (59-68)



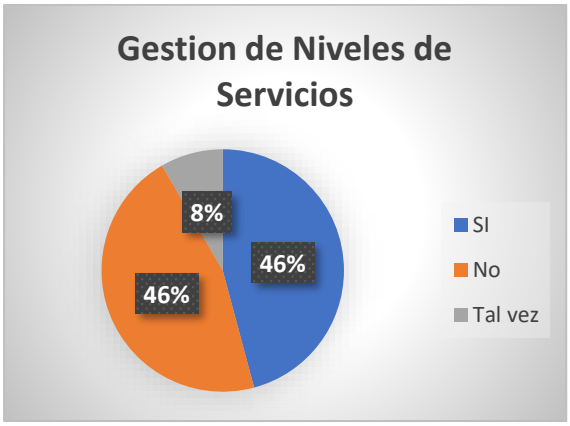
Nota: Gestión del Problema

Proceso 4.- Gestión de Niveles de Servicio

El 46% de encuestados indican que en la empresa se encuentran definidos los pasos del proceso, roles y funciones dentro de la organización, mientras que el otro 46% considera no se encuentra establecido el proceso de gestión del nivel de servicio. El 8% afirma que existe y se supervisa el rendimiento del servicio según el SLA.

Figura 16

Resumen preguntas



Nota: Gestión del nivel del Servicio

En el escenario actual, el departamento de TI de la empresa JASSA TELECOM se pudo evidenciar que no posee procesos internos definidos para la gestión del servicio, y el personal no está capacitado sobre qué prácticas seguir.

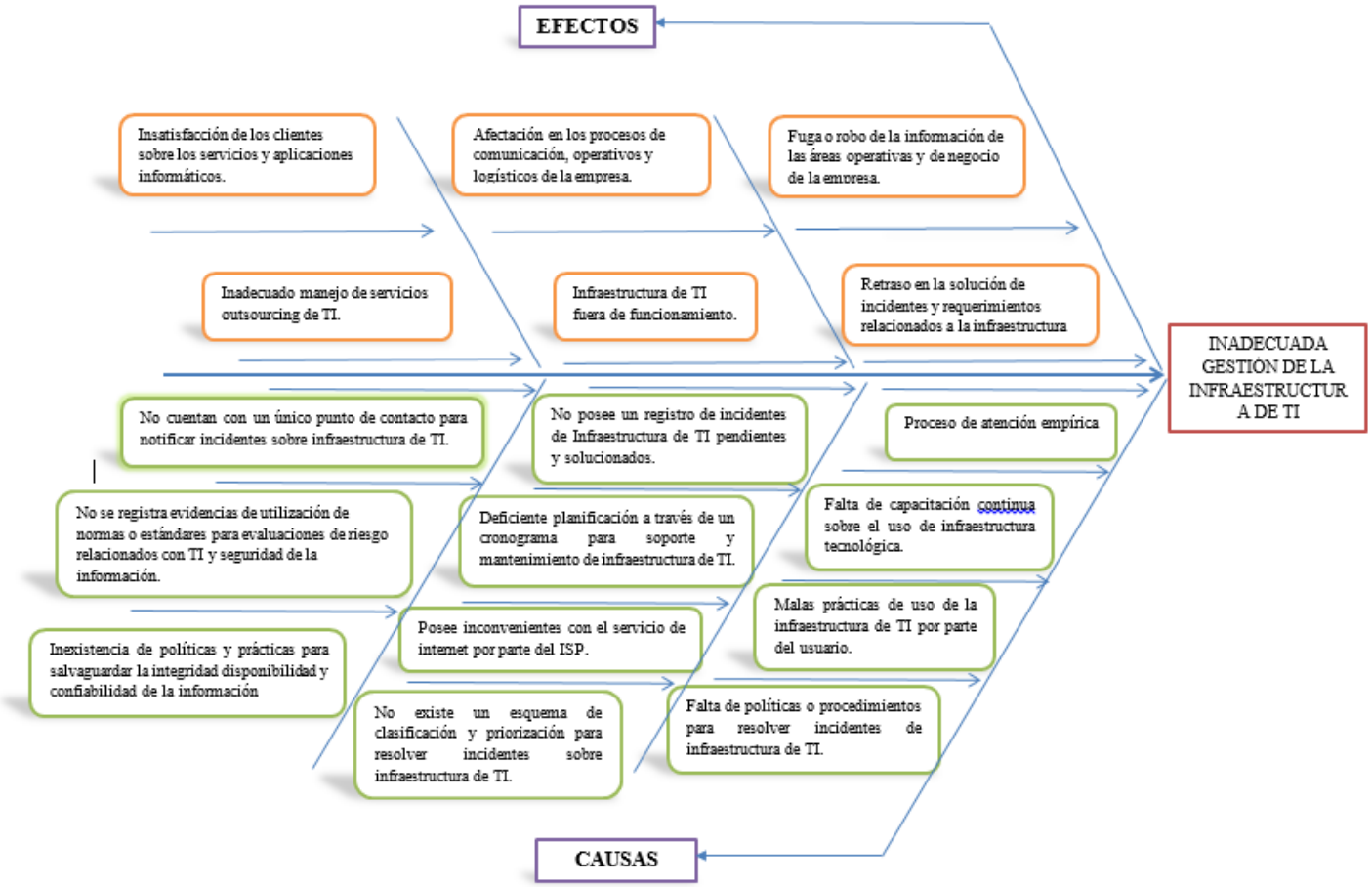
Además, se pudo divisar que las actividades de gestión de infraestructura de TI se realizan de manera manual y sin la aplicación de buenas prácticas o modelos de gestión, es decir, que el área de TI, administra y controla la red, utilizando la mayoría de veces una libreta para llevar el registro de incidentes y problemas suscitados. Así mismo establecen que no existe un manual de procesos de resolución de incidentes, problemas y un proceso de mesa de

servicio definido, es decir carecen de tiempos de entrega de servicios formalizados y acordados entre el usuario y TI.

Con estos antecedentes se elaboró un diagrama de causa - efecto (espina de pescado) como se muestra en la figura 17, en el cual se describe los problemas sobre gestión de red e infraestructura que posee la empresa JASSA TELECOM.

Figura 17

Diagrama de espina de pescado (causa y efecto)



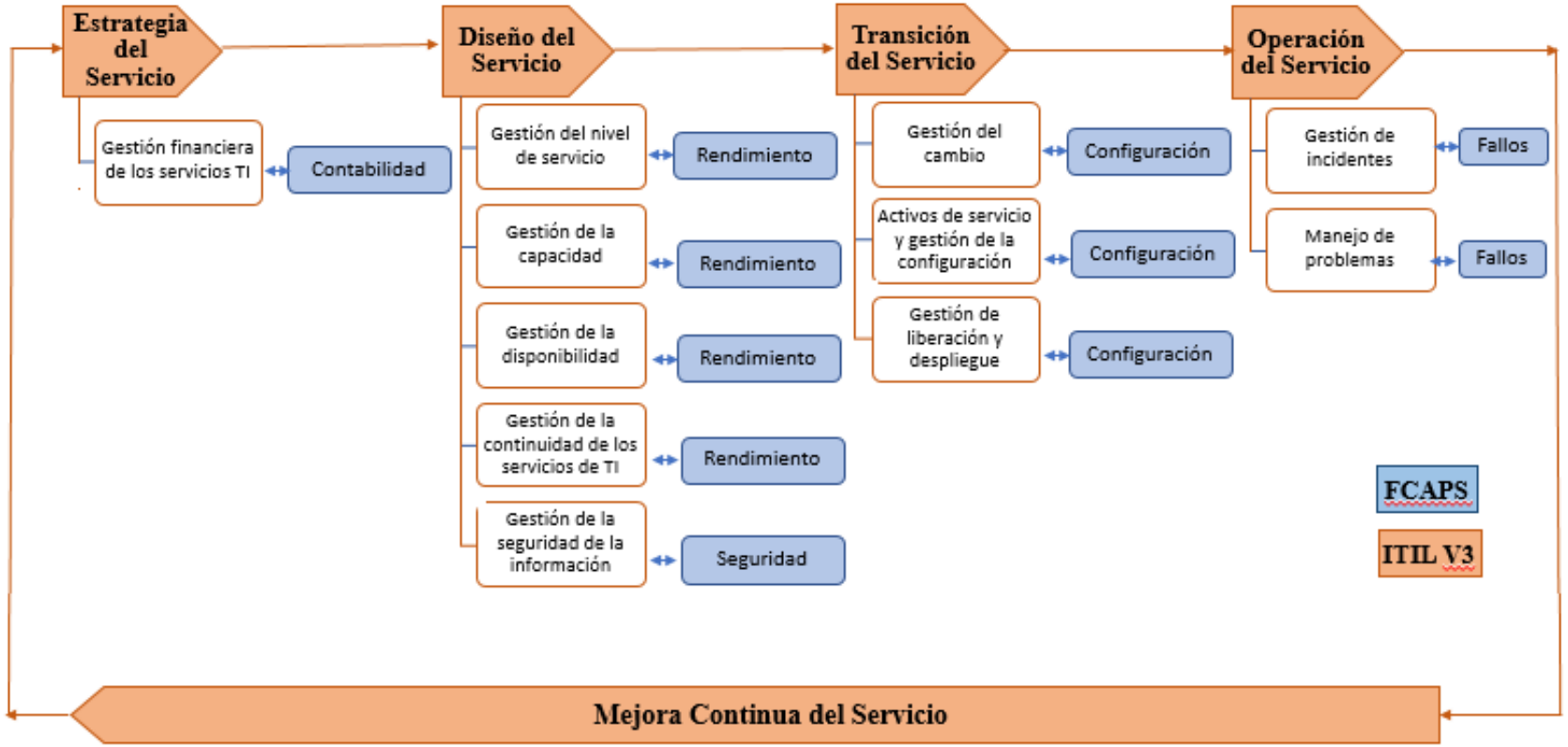
Para ayudar a resolver esta situación, se propone un modelo de gestión de red basado en el modelo de gestión FCAPS de la ISO que permita mejorar la disponibilidad y rendimiento de la red de la empresa JASSA TELECOM. A través del cual se logra identificar los procesos, prácticas para una correcta gestión de la red e infraestructura de TI, teniendo de igual manera como sugerencia la aplicación de una mesa de servicios que asista al departamento de TI con el control de incidentes, tareas, registros y así brindar la mejor asistencia posible a los usuarios de la institución. Por tanto, la mejor opción para mejorar los servicios de TI a través de una mesa de ayuda al usuario se basará en el marco de referencia ITIL.

3.6 Modelo de Gestión de red basado en la norma FCAPS de la ISO e ITIL v3

En este apartado se realiza la descripción del ciclo de vida del Modelo de gestión de red en base a las cinco áreas funcionales la norma FCAPS de la ISO e ITIL v3. Con este modelo se pretende estructurar de una manera lógica las diferentes tareas a llevar a cabo a lo largo de todo el ciclo de vida de gestión de la infraestructura de TI. En la figura 18, se muestra el modelo propuesto.

Figura 18

Modelo de Gestión FCAPS e ITIL v3



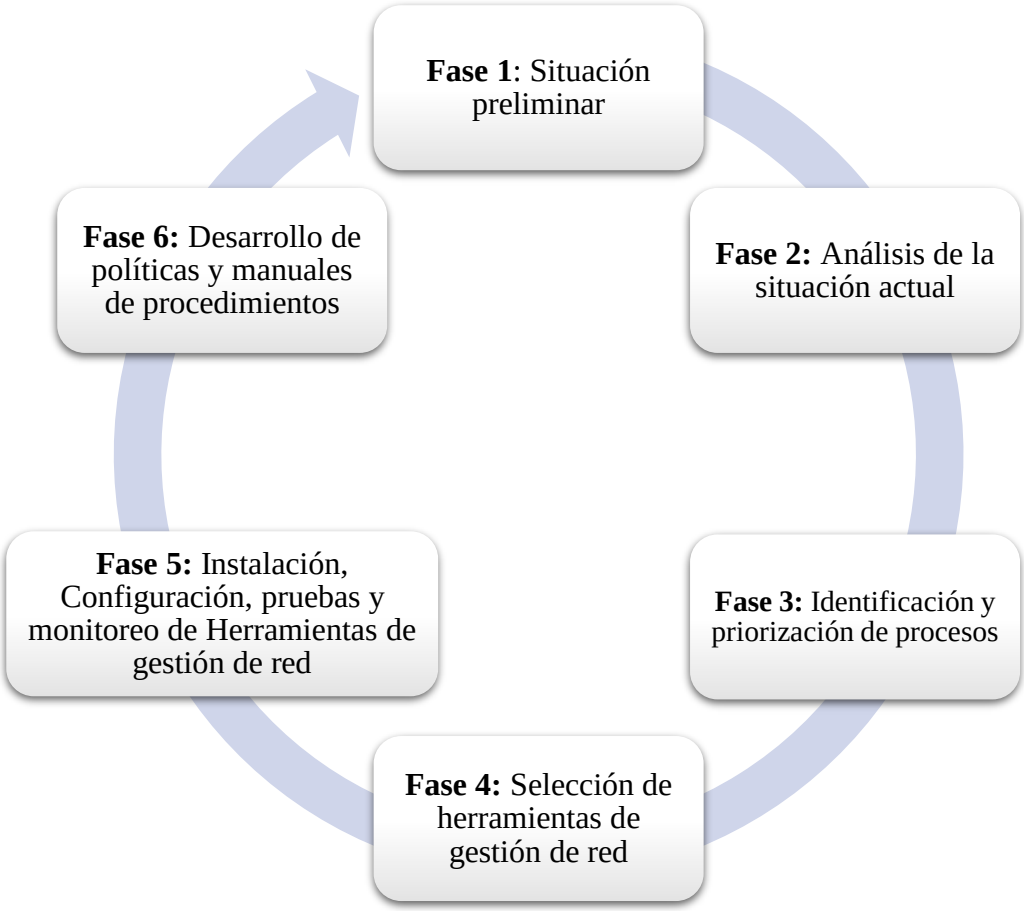
Nota. Elaboración propia. Adaptado de (ENI, 2021) (Bastidas , et al., 2011)

Modelo de aplicación para la gestión de TI de la empresa JASSA TELECOM

Posterior al planteamiento del modelo de gestión de red, se realiza una descripción de cada una de las fases del ciclo de vida a seguir para la aplicación del mismo.

Figura 19

Ciclo de vida del modelo de gestión para la empresa JASSA TELECOM



Fase 1 – Inicialmente se realiza una descripción general de la empresa JASSA TELECOM como el caso de estudio, en el cual se efectuó un levantamiento de información relevante a cerca de los procesos e infraestructura tecnológica que posee la organización, lo cual consta en el ítem 3.2.1 del presente documento.

Fase 2 – En la presente fase se aplicó una encuesta al personal de la unidad de TI y a los líderes de cada una de las áreas funcionales de la empresa JASSA TELECOM, mediante un formulario de google form, el enlace a este se encuentra en el ANEXO D, el cual permitió identificar la situación actual respecto a la gestión de red y servicios de telecomunicaciones, así como los requerimientos urgentes en el área de TI, dichos instrumentos se encuentran descritos en el ítem 3.5.1.

Fase 3 – En la siguiente fase se realiza la identificación y priorización de los procesos y áreas del modelo de gestión de red planteado, los cuales fueron identificados por el personal de JASSA TELECOM, información que se encuentra en el ANEXO D, que permitan tener una gestión de red en base al modelo propuesto. A continuación, en la tabla 8, se describe los procesos de ITIL y áreas de FCAPS que se tomaron en cuenta para el desarrollo del modelo de gestión.

Tabla 8

Procesos de ITIL v3 y áreas de FCAPS

	ITIL v3	**FCAPS**
Estrategia del Servicio	Gestión financiera	Contabilidad
	Gestión de la capacidad	
	Gestión de la continuidad	
Diseño del Servicio	Gestión la disponibilidad	Rendimiento
	Gestión de nivel de servicio	
	Gestión de seguridad de la Información	Seguridad
	Gestión de cambios	
Transición del Servicio	Gestión de la configuración y activos del servicio	Configuración

	Gestión de liberaciones e implementación	
	Gestión de incidentes	
Operación del Servicio	Gestión de problemas	Fallos
	• Función de Service Desk	

Nota: Adaptada de (Iqbal & Nieves, 2011)

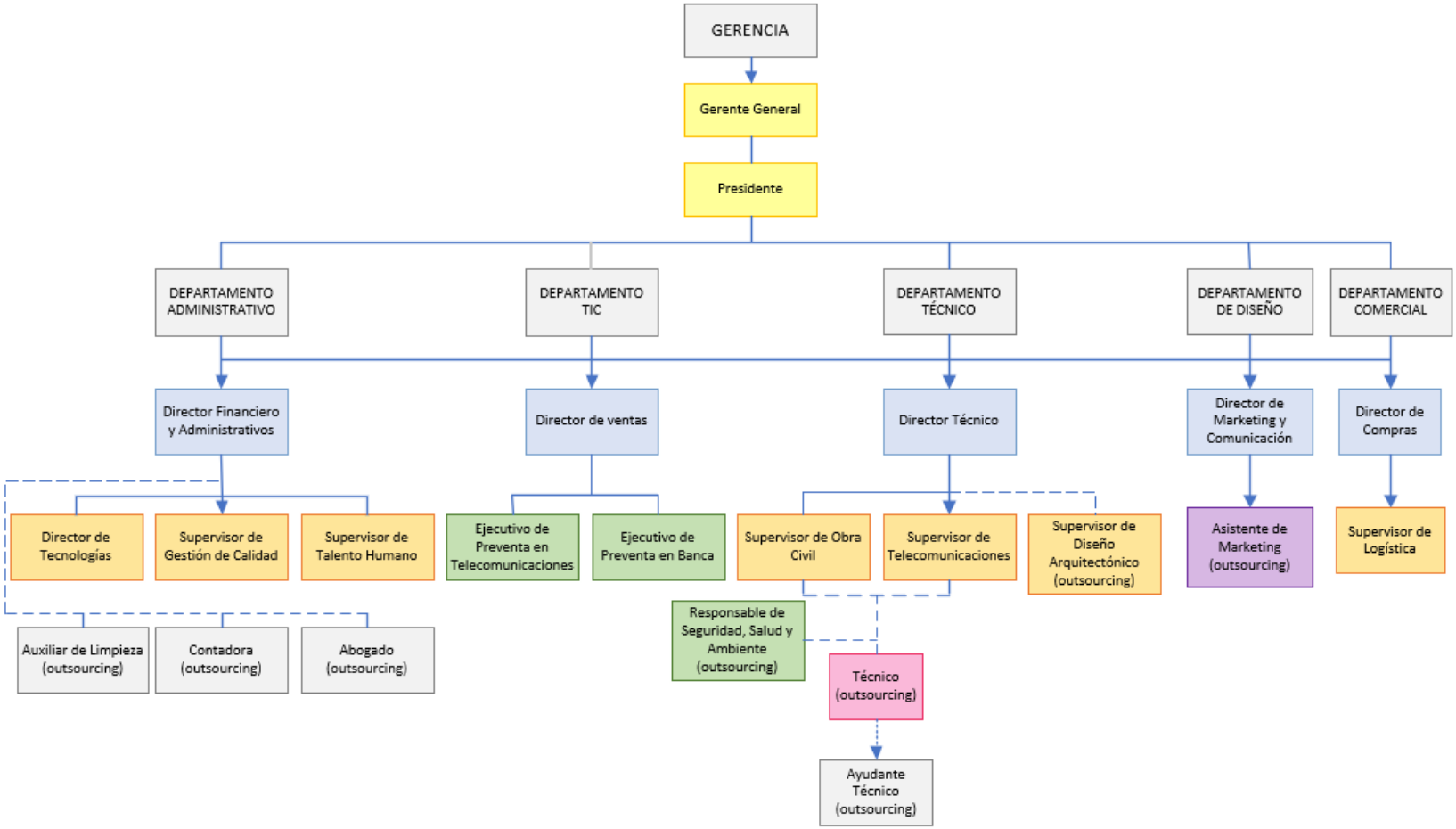
Para proporcionar una correcta gestión de red e infraestructura, se priorizan los procesos y áreas de acuerdo a los requerimientos expuestos por el Gerente y la persona encargada del departamento de TI. Los procesos prioritarios para la empresa JASSA TELECOM son:

- Incidentes
- Seguridad y la función de Service Desk.

De igual manera para una correcta implementación del modelo propuesto y acorde a las buenas prácticas de ITIL v3 se propone un organigrama para la empresa JASSA TELECOM que permita a la Unidad de Tecnología de la información apoyar los objetivos estratégicos, Figura 20, en especial al modelo de gestión planteado.

Figura 20

Organigrama propuesto para la empresa JASSA TELECOM

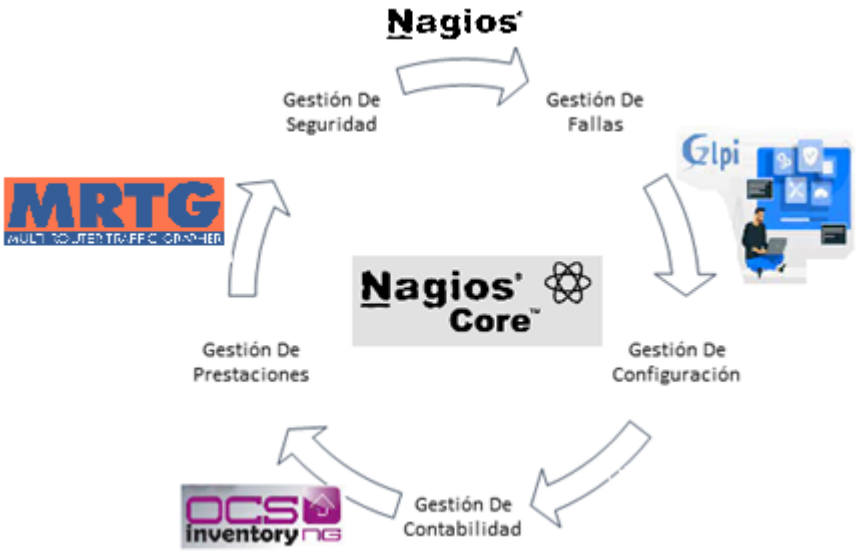


En concordancia con la gestión de servicios de TI la unidad de TI se encuentra en comunicación directa con el Gerente General de la empresa, permitiendo que los proyectos de tecnología sean comunicados directamente con el CEO y así apoyar al cumplimiento de los objetivos estratégicos de la organización.

Fase 4 – En esta fase para la operativización del modelo de gestión de red basado en la norma FCAPS de la ISO e ITIL v3, se realiza un estudio comparativo de las herramientas de gestión de red, bajo el análisis del estándar ISO/IEC/IEE 29148:2018, mediante este ejercicio se eligieron las herramienta de gestión más adecuadas para la empresa y el modelo propuesto, el cual se encuentra detallado en el ítem 4.4.1, de igual manera, se toman en cuenta varias herramientas complementarias para cubrir las demás áreas de gestión de red de la norma FCAPS de la ISO. En la figura 21, se muestran las herramientas utilizadas para la gestión de red de la empresa JASSA TELECOM.

Figura 21

Herramientas de gestión del modelo FCAPS e ITIL v3



Nota: Herramientas de Gestión interactuando en el modelo de Gestión de red

Fase 5 – En esta fase se lleva a cabo la instalación y configuración de las herramientas identificadas en la fase 4, así mismo, se realizaron procesos de monitoreo y pruebas que permitan identificar los problemas e incidentes en la red y servicios de telecomunicaciones.

Fase 6 – En este apartado se desarrolla las políticas y manuales de procedimientos que permita gestionar la red y los servicios de telecomunicaciones, acorde al modelo de gestión de red propuesto.

Nota: Las herramientas, políticas y manuales de procedimientos son planteados en base a las condiciones actuales de la infraestructura de red de la empresa JASSA TELECOM, dentro del modelo planteado se considera un proceso de mejora continua, a partir de la fase 1 en el cual se analizará nuevamente los requerimientos y necesidades de la empresa.

4. CAPÍTULO IV

APLICACIÓN DEL MODELO DE GESTIÓN DE RED BASADO EN LAS FCAPS DE LA ISO, MEDIANTE HERRAMIENTAS DE GESTIÓN, QUE PERMITA MEJORAR LA DISPONIBILIDAD Y RENDIMIENTO DE LA RED DE LA EMPRESA JASSA TELECOM

En el presente capítulo se establecen las políticas de gestión y manuales de procedimientos para la empresa JASSA TELECOM como caso de estudio, además se realiza la implementación de las herramientas de gestión, en el modelo propuesto.

4.1 Políticas de Gestión

Las políticas generales son un conjunto de reglas sencillas que gobiernan la gestión de los recursos de la red. Estas políticas tienen que ser congruentes con los objetivos de la institución y permitir el acceso a la información de una forma coherente, simple y segura.

No existe un estándar específico que identifique un proceso preciso o único para determinar las políticas de gestión, por lo que las políticas de gestión se definen como un conjunto de reglas que establecen procedimientos para controlar, monitorear y administrar la red en general, en función de las necesidades de la red.

4.2 Establecimiento de políticas de gestión de red

Las políticas de gestión de red son creadas en base a las cinco áreas funcionales la norma FCAPS de la ISO e ITIL v3 descritas en el apartado 3.6. A continuación, se presenta un manual que contiene cada una de las políticas de gestión de red para la empresa JASSA TELECOM, cuya función es la de definir las reglas pertinentes para asegurar el buen uso del sistema de gestión de red, que se ajustan a las necesidades de la institución, destinadas al administrador, personal encargado de la administración de red y usuarios.

El establecimiento de las políticas de gestión se respalda al obtener los resultados de la auditoría de la red y el análisis de las áreas funcionales que determina el modelo de gestión FCAPS de la ISO e ITIL v3, además tomando en cuenta las necesidades que posee la administración de la red para brindar los servicios adecuados a los usuarios internos. El objetivo principal es regular los procesos que se realizan en la institución guiándose de políticas establecidas mediante las cuales mantenga la red en correcto funcionamiento y aprovechando los recursos existentes para brindar los servicios de una manera eficiente. Es importante recalcar que las políticas de gestión son una guía sugerida orientada al personal de administración de la red, para el manejo, manipulación, control y resolución inmediata de problemas e incidentes, basada en el cumplimiento de las mismas mediante la utilización de un sistema de gestión con el apoyo del software de gestión elegido acorde a las necesidades de la empresa, que permite la administración de la red de manera amigable cubriendo las áreas funcionales del modelo, presentando a la institución un sistema de gestión completo, centralizado, eficiente de bajo costo relativo.

EMPRESA JASSA TELECOM		
POLÍTICAS DE GESTIÓN PARA LA RED DE DATOS		
	Versión:	1.0
	Revisado por:	Msc. Alexander Trejo
	Aprobado por:	
	Elaborado por:	Lila Hermosa Msc. Fabián Cuzme
	Fecha de elaboración:	Junio 2022

I. PROPÓSITO

El objetivo principal de este documento es brindar políticas de gestión de red que deben ser cumplidas por el personal encargado de la administración de red, para asegurar el buen funcionamiento de la red y la prestación eficiente de servicios a los usuarios.

II. CONCEPTOS PRELIMINARES

- **Gestión de red**

La gestión de la red es el proceso que permite controlar y realizar un seguimiento de sus recursos con el fin de evitar que esta llegue a funcionar incorrectamente degradando su funcionamiento.

- **Políticas de gestión de red**

Una política es un objetivo claro o método de acción que guía al administrador de la red y determina el presente y futuras decisiones que puedan presentarse en la red.

Políticas como un conjunto de reglas para administrar, gestionar, y controlar acceso a los recursos de red.

III. NIVELES ORGANIZACIONALES

a) **Presidente. -** El presidente tiene autoridad inmediata y es responsable de organizar, planificar, coordinar y supervisar los procesos productivos de la empresa, así como de

desempeñar funciones administrativas y técnicas, ejecutar programas y cumplir con las normas legales de la empresa.

b) Gerente General. - El gerente es la persona que controla, dirige y coordina una determinada organización

c) Director de Tecnologías. - Profesional responsable de diseñar y/o desarrollar sistemas tecnológicos que faciliten la gestión y los procesos en la organización. Dirige el departamento de tecnología o ingeniería, desarrolla políticas y procedimientos y utiliza la tecnología para mejorar los productos y servicios que se centran en los usuarios.

d) Supervisor de Telecomunicaciones. - Responsable de mantener el buen funcionamiento del software y hardware de la red.

e) Administrador de Red.-. Persona responsable de mantener la red informática actualizada y en continuo funcionamiento sin que existan problemas y, en caso de que los haya, poder solucionarlos de la forma más rápida y eficaz posible

f) Usuario. - Persona que utiliza una computadora o un servicio de red.

IV. GENERALIDADES

a. El objetivo de desarrollar políticas de gestión es ahorrar tiempo y reducir errores. Uno de los beneficios más importantes es la capacidad de crear plantillas para tareas específicas, lo que permite actualizaciones y / o cambios simultáneos en la red.

b. La persona a cargo de la gestión de la red de datos se comprometerá a cumplir todas las políticas descritas en este documento.

c. Las políticas descritas en este documento sirven de guía y pueden ser actualizadas si es necesario, identificando al personal autorizado para realizarlo y marcando las condiciones de su registro, siempre y cuando se integren a los objetivos de gestión.

V. VIGENCIA

El documento de administración de la red actual será admitido después de que las autoridades correspondientes lo aprueben como documento técnico para la administración de la

red. Estas políticas deben ser analizadas y actualizadas de acuerdo con las necesidades de esta dependencia, o si se requieren cambios fundamentales en la infraestructura tecnológica de la red.

VI. REFERENCIA

Debido a que actualmente no existe un estándar definido para el establecimiento de políticas de gestión de red, se ha utilizado como referencia las tesis realizadas en el GAD de Ibarra por Myriam Ipiales, en el año 2015, en la UTN por Jésica Báez, en el año 2017 y en base al modelo generado del modelo FCAPS e ITIL v3.

VII. ESTRUCTURA DE LAS POLÍTICAS DE GESTIÓN

1. **Políticas de gestión de red**
   - 1.1. Objetivo de las Políticas de Gestión de Red
   - 1.2. Compromiso de las Autoridades
2. **Gestión de Fallos**
   - 2.1. Manejo de fallos
   - 2.2. Manejo de Incidentes
   - 2.3. Documentación de fallos e Incidentes
   - 2.4. Mesa de servicio
3. **Gestión de Configuración**
   - 3.1. Ingreso de equipos a la red
   - 3.2. Configuración de equipos
4. **Gestión de Contabilidad**
   - 4.1. Inventario de equipos gestionados
5. **Gestión de Prestación**
   - 5.1. Informe de rendimiento
6. **Gestión de Seguridad**
   - 6.1. Acceso al sistema de gestión de red

6.2. Acceso a los dispositivos gestionados

VIII. TÉRMINOS Y DEFINICIONES

Administrador de red: Persona designada en una organización cuya responsabilidad incluye el mantenimiento de las infraestructuras informáticas con énfasis en las redes.

Red de datos: Sistema de interconexión de computadoras que permite a sus usuarios compartir recursos, aplicaciones, datos, voz, imágenes y transmisiones de video.

Dispositivo de red: Es el hardware que permite la comunicación entre las computadoras que hay en una red.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio que causa o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.

Problema: ITIL define un problema como la causa desconocida de uno o más incidentes.

SNMP: (Simple Network Management Protocol), es un protocolo de la capa de aplicación que intercambia información de administración entre dispositivos de red.

Mesa de Servicio: La mesa de servicio es el principal y único punto de contacto entre un equipo de TI y los diferentes tipos de usuarios de una empresa. Registra y monitorea todas las actividades con el objetivo de solucionarlas y evitar que se repitan.

GLPI: Es una solución libre de gestión de servicios de tecnología de la información (ITSM), un sistema de seguimiento de incidencias y de solución Service Desk.

Ticket: Documento que se entrega a la persona interesada en el que se garantiza que esta ha realizado una entrega o pago por una compra o por un servicio.

SLA: (Service Level Agreement), es un contrato firmado entre las partes involucradas en una negociación que determina cuáles son las responsabilidades de cada uno en relación a los servicios contratados.

KEDB: Base de datos que contiene todos los registros de errores conocidos. Proporciona información valiosa a los técnicos de soporte que se encargan de resolver las incidencias

reportadas por los usuarios.

4.3 Desarrollo de políticas de gestión de red para la empresa JASSA TELECOM

EMPRESA JASSA TELECOM		
	**Dominio**	1. Políticas de gestión de red
	Control	1.1. Objetivo de las políticas de gestión de red
	Delegado	Administrador de red

Art. 1. Exponer la información necesaria al administrador de la red y al personal a cargo de la administración de la red sobre los pasos que se deben tomar para mantener el correcto funcionamiento de la red y el uso de los recursos disponibles para la resolución inmediata de problemas.

Art. 2. Dar a conocer la información necesaria a los nuevos usuarios que acceden a los servicios de la red por primera vez para su correcta utilización.

EMPRESA JASSA TELECOM		
	**Dominio**	1. Políticas de gestión de red
	Control	1.2. Compromiso de las Autoridades
	Delegado	Administrador de red

Art. 3. El administrador de la red, como persona a cargo de desarrollar las políticas de gestión de la red para la empresa JASSA TELECOM, acepta la responsabilidad de revisar y

difundir las políticas descritas en este documento.

4.3.1 Políticas de gestión de Fallos

EMPRESA JASSA TELECOM		
	**Dominio**	2. Gestión de fallos
	Control	2.1. Manejo de Fallos
	Delegado	Administrador de red

Art. 4. Cuando existen fallos en el entorno de la red, el administrador o responsable de administración debe identificar el fallo sucedido en la red, mediante la herramienta de gestión, llamada telefónica, correo electrónico o mensaje, realizar la selección adecuada del problema, para luego aislar y corregir el fallo, asegurando la continuidad del servicio. Todo esto siguiendo el manual de gestión de fallos.

Art. 5. Se deberá notificar el fallo, ya que permite informar al personal de soporte técnico de cualquier problema.

Art. 6. Los problemas deben resolverse dentro de la red en el menor tiempo posible.

Art. 7. Al momento de ocurrir una nueva falla que no se encuentre en la guía y la solución requiera el uso de nuevos y diferentes mecanismos, se deberá documentar la falla y su procedimiento de resolución.

EMPRESA JASSA TELECOM		
	**Dominio**	2. Gestión de fallos
	Control	2.2. Manejo de Incidentes
	Delegado	Administrador de red

Art. 8. El proceso de gestión de incidentes inicia con un usuario final que comunica un problema y concluye con un profesional del equipo de la mesa de servicio que resuelve dicho problema.

Art. 9. Cumplir con el proceso de ciclo de vida de la gestión de incidentes: reporte, asignación, tratamiento, respuesta y cierre.

Art. 10. Categorizar y priorizar los incidentes, de esta manera son asignados a los técnicos calificados en el tema para su resolución. La priorización se determina en función de su impacto y urgencia.

- **Prioridad 1 (Crítico):** Esto se refiere a una interrupción a gran escala que afecta a un gran número de personas. El equipo está fuera de servicio, inoperable o experimenta interrupciones frecuentes durante cortos períodos de tiempo. Para que el servicio se restablezca a las condiciones regulares de operación, el administrador debe actuar de inmediato.
- **Prioridad 2 (Alto):** Es posible utilizar un sistema o aplicación, pero con importantes limitaciones. La calidad del servicio se ha deteriorado. Siempre y cuando no existan alertas prioritarias, el administrador de la red debe actuar de inmediato.
- **Prioridad 3 (Medio):** No requiere atención inmediata por parte del administrador de la red. Notificación de cualquier tipo de impacto en el servicio como resultado de actividades planificadas como mantenimiento, actualizaciones y adición de equipos.
- **Prioridad 4 (Notificación, Información):** Información referente al servicio.

  No genera ningún impacto sobre el servicio y la productividad del usuario no se ve afectada directamente.

Tipo de Fallo	Prioridad	Tiempo de solución
Caída total del servicio	Critico	Solución del problema de 0 a 1 hora.
Alerta de un dispositivo desconocido	Alto	Solución del problema de 2 a 4 horas.
Alerta del Servicio parcialmente caído	Medio	Solución del problema dentro de 24 horas.
Dispositivo funcionando	Notificación, Información	Solución del problema dentro de 48 horas

EMPRESA JASSA TELECOM		
	**Dominio**	2. Gestión de fallos
	Control	2.3. Documentación de fallos e Incidentes
	Delegado	Administrador de red

Art. 11. Documentar las conclusiones de un incidente después de que se haya resuelto, esto ayuda a preparar mejor a los equipos para futuros incidentes y crea un proceso de gestión de incidentes más eficiente.

Art. 12. Los fallos que ocurrieron, así como las soluciones a esos fallos, deben documentarse para que la próxima vez que sucedan y exista un proceso, permita una resolución más rápida.

Luego de la verificación del cumplimiento de la política descrita en este documento, el director puede tomar las medidas que considere necesarias para asegurar el cumplimiento.

EMPRESA JASSA TELECOM		
	**Dominio**	2. Gestión de fallos
	Control	2.4. Mesa de Servicio
	Delegado	Administrador de red

Art. 13. El servicio al cliente requiere prontitud. La mesa de ayuda debe estar respaldada por herramientas tecnológicas que faciliten la interacción entre el cliente y la empresa proveedora. Generalmente utilizan:

- Vía telefónica
- Correo electrónico
- Reporte automático

Art. 14. Será el único punto de contacto entre los usuarios y la gestión de servicios TI. Sin este contacto se pasarían por alto las limitaciones de estructura o la priorización de incidencias.

Art. 15. Proporcionará información correcta y en el tiempo adecuado a los diferentes actores del proceso.

Art. 16 Antes de realizar la visita en sitio, los técnicos de la mesa de ayuda deben intentar atender y resolver las incidencias de forma remota.

Art 17. Los casos que quedan fuera del alcance del primer nivel de servicio no deben ser resueltos por los agentes de la mesa de ayuda.

Art. 18. Todos los casos deben ser cerrados por el personal de la mesa de ayuda previo a la validación con el usuario.

Art 19. Todas las novedades que afecten al caso del usuario deberán serle comunicadas.

Art 20. Los indicadores, análisis y sugerencias de mejora deben incluirse en los informes de evaluación mensuales.

4.3.2 Políticas de gestión de Configuración

EMPRESA JASSA TELECOM		
	Dominio	3. Gestión de configuración
	Control	3.1. Ingreso de equipos a la red.
	Delegado	Administrador de red

Art. 21. El departamento de TI debe mantener un inventario de propiedad de los equipos de red, al agregar un nuevo equipo se deberá documentar la información relevante

Art. 22. Para el ingreso de equipos en la base de datos se utilizará la nomenclatura establecida por la unidad de TI de la empresa. JASSA TELECOM.

EMPRESA JASSA TELECOM		
	Dominio	3. Gestión de configuración
	Control	3.2. Configuración de equipos.
	Delegado	Administrador de red

Art. 23. El departamento de TI debe mantener un inventario de propiedad de los equipos de red, al agregar un nuevo equipo o reconfigurar uno de ellos se deberá documentar la información relevante

Art. 24. El administrador de la red y quienes estén previamente autorizados podrán realizar configuraciones sobre los dispositivos de red.

Art. 25. Los equipos a integrarse en la red deben ser configurados con los lineamientos básicos de la empresa.

Art. 26. Todo cambio realizado en la configuración de los equipos deberá ser documentado, para tener un registro de los cambios.

4.3.3 Políticas de gestión de Contabilidad

<table>
<tr><td colspan="3">EMPRESA JASSA TELECOM</td></tr>
<tr><td rowspan="3"></td><td>Dominio</td><td>4. Gestión de Contabilidad</td></tr>
<tr><td>Control</td><td>4.1. Inventario de equipos gestionados</td></tr>
<tr><td>Delegado</td><td>Administrador de red</td></tr>
<tr><td colspan="3">Art. 27. La herramienta de gestión de la red se utilizará para generar informes sobre el uso de los recursos:
• Dispositivos Monitoreados
• Estadísticas de protocolos
• Estadísticas de interfaces
Art. 28. El administrador de la red tendrá la facilidad de obtener informes sobre el uso de los recursos de la red, mediante la herramienta de gestión, según sea necesario.</td></tr>
</table>

4.3.4 Políticas de gestión de Prestación

<table>
<tr><td colspan="3">EMPRESA JASSA TELECOM</td></tr>
<tr><td rowspan="3"></td><td>Dominio</td><td>5. Gestión de Prestación</td></tr>
<tr><td>Control</td><td>5.1. Informe de rendimiento</td></tr>
<tr><td>Delegado</td><td>Administrador de red</td></tr>
<tr><td colspan="3">Art. 29. Se generarán los reportes de acuerdo a la información requerida por el administrador de la red y las solicitudes de la institución.
Art. 30. Los informes deberán analizarse al término de cada mes para garantizar que los equipos y servicios estén siempre disponibles.</td></tr>
</table>

Art. 31. Se establecerán límites de aceptación, bajo los cuales los equipos de la red trabajarán correctamente.

4.3.5 Políticas de gestión de Seguridad

EMPRESA JASSA TELECOM		
	**Dominio**	6. Gestión de Seguridad
	Control	6.1. Acceso al sistema de gestión de red
	Delegado	Administrador de red

Art. 32. El administrador de la red será el encargado de crear nuevas cuentas de los usuarios para acceder al sistema de gestión con los privilegios que estime oportunos.

Art. 33. En caso de retiro del funcionario, el administrador deberá anular y cancelar todos los permisos otorgados

Art. 34. El acceso a la configuración de los dispositivos activos de la red deberá estar restringido por contraseñas y tendrá un impacto significativo en la gestión de red.

Art. 35. Las notificaciones vía correo electrónico serán dirigidas exclusivamente al administrador de la red.

Art. 36. Todas las credenciales de inicio de sesión para los sistemas y recursos de tecnología de la información son únicas e intransferibles, durante la vigencia de los derechos de uso.

Art. 37. Las cuentas de ingreso a los sistemas y recursos de cómputo serán administradas directamente por la Unidad de TI en coordinación con las distintas gerencias y jefaturas, y serán utilizadas únicamente para actividades propias de la institucion.

Art. 38. El administrador de la red podrá realizar las configuraciones que estime necesarias en el sistema de gestión.

Art. 39. El administrador de la red debe auditar periódicamente el entorno de monitoreo (al menos dos veces al año), para determinar posibles vulnerabilidades a los sistemas de red.

Art. 40. El administrador de la red un análisis de riesgo

EMPRESA JASSA TELECOM		
	**Dominio**	6. Gestión de Seguridad
	Control	6.2. Acceso a los dispositivos gestionados
	Delegado	Administrador de red

Art. 39. Para realizar operaciones de configuración o actualización en dispositivos de red, el acceso está restringido por el administrador; de no ser así, se requerirá autorización administrativa para el respectivo cambio o actualización.

Art. 40. Solo los usuarios autorizados tendrán acceso a las claves para el ingreso a los dispositivos administrados.

Art. 41. Cuando se detecte el uso no autorizado de la red, se bloqueará temporal o permanentemente el acceso del usuario o de la red, y se notificará a las autoridades correspondientes. La conexión se hará a solicitud del jefe de área respectivo.

Art. 42. Durante la configuración de un servidor, los jefes del departamento de TI deben establecer lineamientos para el uso de los recursos del sistema y de la red, particularmente las restricciones de directorios, permisos y programas que pueden ejecutar los usuarios.

Art. 43. Durante la configuración de un servidor, los jefes del departamento de TI deben establecer lineamientos para el uso de los recursos del sistema y de la red, particularmente las restricciones de directorios, permisos y programas que pueden ejecutar los usuarios.

NOTA: Nadie puede copiar, editar, destruir o divulgar información almacenada en sistemas informáticos o servidores a menos que tenga la debida autorización.

4.4 Manuales de procedimientos

Dentro del proceso de gestión, es fundamental contar con guías donde se puedan encontrar soluciones inmediatas, así como procesos que puedan ayudar a resolver una anomalía en la red de gestión de la empresa JASSA TELECOM, en este apartado se describen los manuales de procedimientos, que no es más que una guía amplia que explica cuándo y cómo utilizar las herramientas que se han implementado, no pretende ser un estatuto, sino un apoyo de acceso rápido para ayudar al administrador a resolver problemas e incidencias sin causar interrupciones dentro de la red.

El presente manual de procedimientos está estructurado en base al modelo propuesto del estándar de gestión red ISO/OSI y las buenas prácticas ITIL v3, el cual deberá ser utilizado por el personal encargado de la administración de red para diagnosticar y corregir problemas de manera oportuna.

4.4.1 Manual de procedimientos para la Gestión de fallos

EMPRESA JASSA TELECOM		
Manual de procedimientos para la gestión de Fallos		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-001
	Procedimiento:	Manejo de Fallos
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Presentar el proceso a seguir para la identificación, control del fallo y control de errores, que se ocasionen dentro de la red, con el fin de mejorar el tiempo de respuesta a este tipo de eventos sin causar molestias a los usuarios finales.

Alcance. - Este manual ha sido creado para ser aplicado a todos los dispositivos gestionados, incluidas las áreas estratégicas; este procedimiento se aplica a fallos generales de la red.

En caso de producirse un fallo, se documentará junto con su solución para que en caso de que vuelva a ocurrir se conozca el procedimiento para resolverlo de forma eficaz.

Descripción del procedimiento

N.º	**Actividad**	**Descripción**	**Responsable**
1	Identificación del fallo	a) Identificar el fallo. b) Registrar el fallo en una herramienta de gestión de problemas.	Director de Tecnología
2	Control del fallo	a) Priorizar el fallo b) Investigar el fallo c) Analizar los fallos registrados.	
3	Control de errores	a) Gestionar los errores conocidos de la KEDB periódicamente. b) Analizar el problema c) Documentar como un error conocido, volviendo a evaluar periódicamente para tener en cuenta el impacto que crean y	

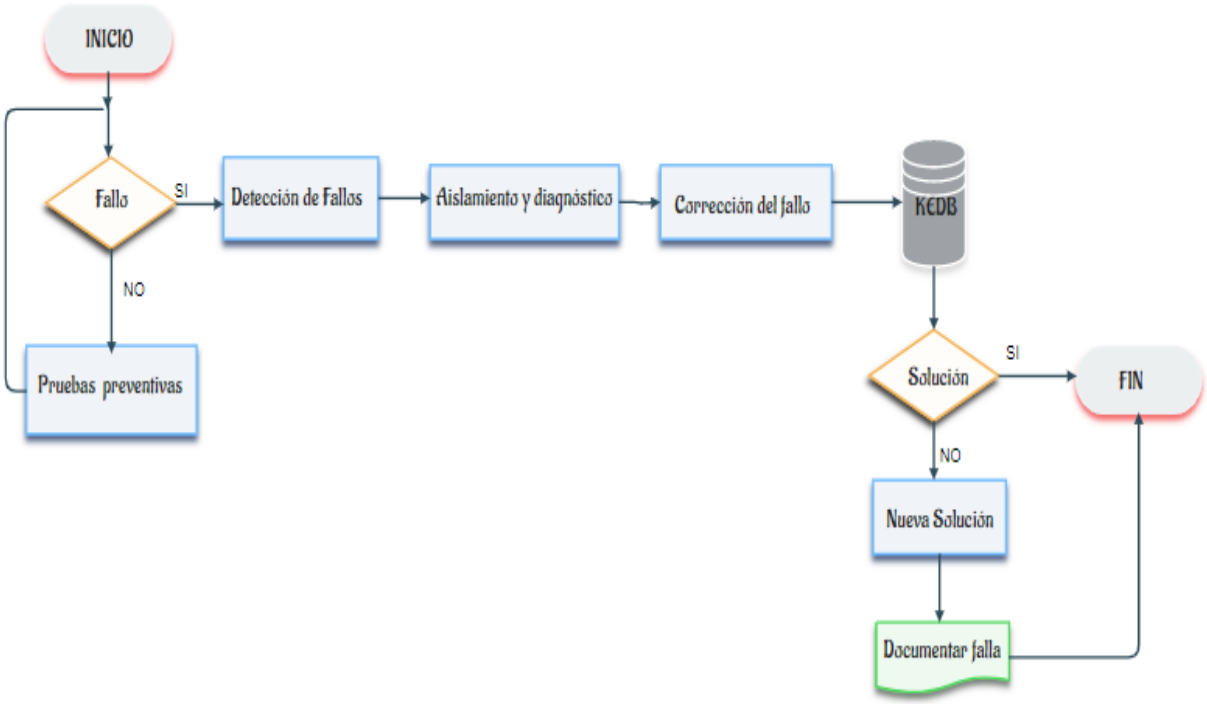
		probar la eficacia de las soluciones.	

Diagrama de flujo

PROCEDIMIENTO: MANUAL PARA GESTIÓN DE FALLOS

RED DE DATOS – EMPRESA JASSA TELECOM

ADMINISTRADOR DE RED



4.4.1.1 Manual de procedimientos para la Gestión de Incidentes

EMPRESA JASSA TELECOM		
Manual de procedimientos para la Gestión de Incidentes		
	Elaborado por:	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-002
	Procedimiento:	Manejo de Incidentes
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Presentar el proceso a seguir para la identificación, prevención y solución de incidentes que se ocasionen dentro de la red, con el fin de mejorar el tiempo de respuesta a este tipo de eventos sin causar molestias a los usuarios finales.

Alcance. - Este manual ha sido creado para ser aplicado a todos los dispositivos gestionados, incluidas las áreas estratégicas; este procedimiento se aplica a incidentes generales de la red.

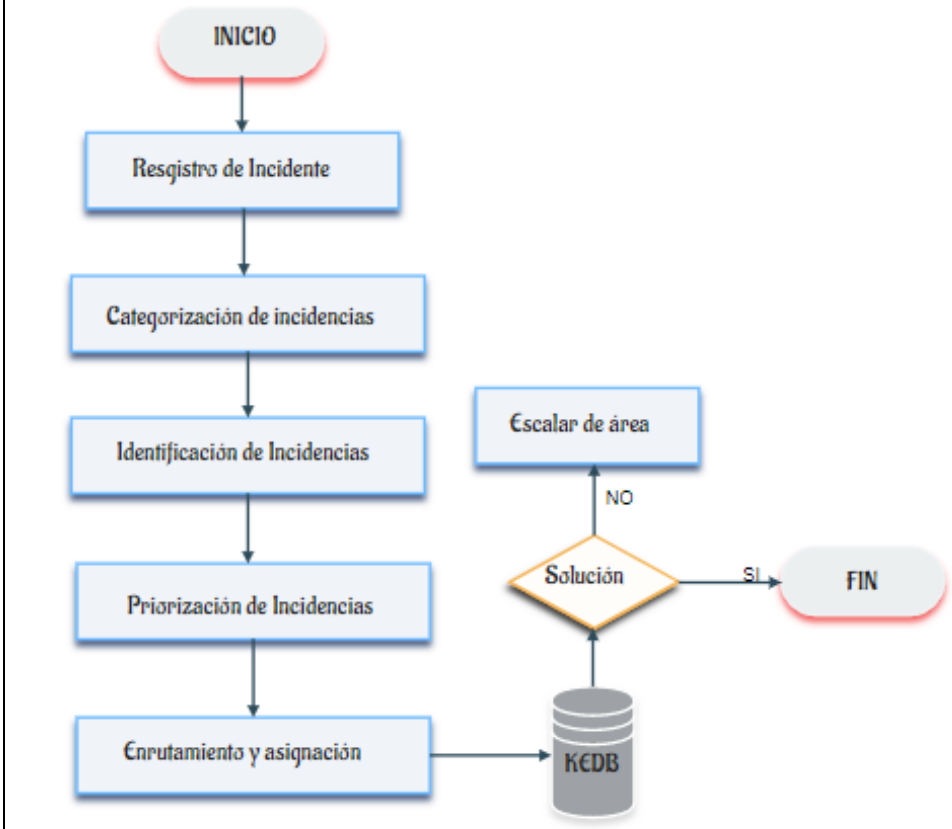
Descripción del procedimiento

N.º	Actividad	Descripción	Responsable
1	Registro del incidente	a) Registro de incidente mediante llamada telefónica, correo electrónico, sms.	

2	Categorizar el incidente	b)	Se pueden clasificar y subcategorizar en función del área de TI o negocio en la que el incidente causa una interrupción, como la red, el hardware, etc.	
3	Priorizar el incidente	c)	Priorizar según su impacto y urgencia utilizando una matriz de prioridad.	Director de Tecnología
4	Enrutamiento y asignación de incidentes	d)	Una vez clasificado y priorizado el incidente, se asigna automáticamente a un técnico con la experiencia relevante.	
5	Creación y gestión de tareas	e)	Según la complejidad del incidente, se puede desglosar en subactividades o tareas	
6	Gestión y escalamiento del SLA	f)	Mientras se procesa el incidente, el técnico debe asegurarse de no infringir el SLA.	
7	Resolución del incidente	g)	Se considera resuelto un incidente cuando el técnico ha encontrado una solución permanente para el problema.	Director de Tecnología
8	Cierre del incidente	h)	Un incidente se puede cerrar	

		una vez que se resuelve el problema y el usuario acepta la resolución y está satisfecho.	
9	Revisión posterior al incidente	i) Luego de que se haya cerrado un incidente, se recomienda documentar todas las conclusiones de ese incidente.	

Diagrama de flujo

PROCEDIMIENTO: MANUAL PARA GESTIÓN DE INCIDENTES	
RED DE DATOS – EMPRESA JASSA TELECOM	
ADMINISTRADOR DE RED	

4.4.1.2 Manual de procedimientos para la Mesa de Servicios

EMPRESA JASSA TELECOM		
Manual de procedimientos para la Mesa de Servicio		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-002
	Procedimiento:	Mesa de Servicio
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Atender, supervisar y solucionar todas las solicitudes e incidentes de TI mediante el uso de una mesa de servicio y prestar el apoyo necesario en la operación y / o resolución de problemas e incidentes, logrando incrementar la productividad y efectividad del proceso de gestión de red.

Alcance. - Este manual de procedimientos se aplica a todo el personal de la organización. Todos los casos de hardware y software informados por el usuario se registrarán en la mesa de ayuda.

Definiciones

Usuario. - Es la persona que solicita soporte por algún problema. Puede ser telefónico o por la aplicación de mesa de ayuda.

GPLI. - Es un software de código abierto distribuida bajo la GPL (Licencia Pública General), que simplifica la gestión de recursos informáticos. GLPI es una aplicación basada en Web escrita en PHP, que permite a los usuarios registrar y gestionar inventarios de hardware y software, agilizando el trabajo de los técnicos gracias a la información registrada y almacenada en la herramienta. Cuenta con un sistema de seguimiento de tareas con notificaciones por correo electrónico del inicio, avance y cierre de las solicitudes.

ITIL. - Es un marco estratégico orientado al ciclo de vida del servicio. A través de procesos de mejora continua de la efectividad y eficiencia de procedimientos operacionales, permiten resolver fallos, arreglar problemas y llevar a cabo operaciones rutinarias de manera coordinada.

Mesa de ayuda. - Es una función de Operación que provee a los usuarios de TI, un punto único de contacto.

Incidente. - Es la alteración a cualquier ítem de configuración, que afecta el normal funcionamiento de un servicio TI. Ocasionando la interrupción no planeada del mismo

Fallo. - Es la causa de uno o más incidentes.

Soporte Técnico. - Encargado de revisar la mesa de ayuda, realizar visitas para dar el diagnóstico y la correcta solución al problema registrado. Para luego documentar y finalizar el soporte

Descripción del procedimiento

N.º	Actividad	Descripción	Responsable
1	Reporte de incidente	a) El usuario informará o registrará el incidente presentado por teléfono o mesa	

		de ayuda para que pueda ser gestionado y abordado de esta manera.	
2	Asignación de incidente	b) El técnico a cargo revisa, identifica y valida el tipo de requerimiento. c) Vía telefónica: El técnico designado informará al usuario de manera clara y remota sobre la disponibilidad del servicio y una solución a su solicitud. d) Mesa de ayuda: A través de este medio se notificará al usuario el número de ticket asignado, el estado de su ticket y el técnico asignado.	Director de Tecnología
3	Analizar y asignar mesa de ayuda	e) Se realiza el análisis y se asigna el nivel f) El incidente está dentro de la base de datos g) SI: Realizar diagnósticos NO: Se rechaza, se realiza el cierre en el sistema. FIN: El procedimiento ha concluido.	Director de Tecnología
4	Diagnosticar	h) Para atender la solicitud el	

		técnico a cargo, deberá trasladarse al sitio del usuario para brindar el diagnóstico y la solución de acuerdo con el tipo de incidente.	
5	Solución del Incidente	i) El técnico asignado soluciona el incidente.	
6	Reasignar a otro nivel	j) Este segundo nivel de soporte proporciona una asistencia más especializada. k) El técnico a cargo que está manejando el caso escala la solicitud al tercer nivel de servicio y registra el motivo del escalamiento, informando al usuario del estado actual del ticket.	
7	Revisar requerimiento	l) ¿Está resuelta la solicitud? SI: Continúe con la Actividad 6 NO: El procedimiento ha finalizado.	
8	Verificar y realizar prueba del equipo	m) Después de asegurarse de que el equipo funciona correctamente, se realiza una prueba. ¿Está trabajando el equipo?	Director de Tecnología

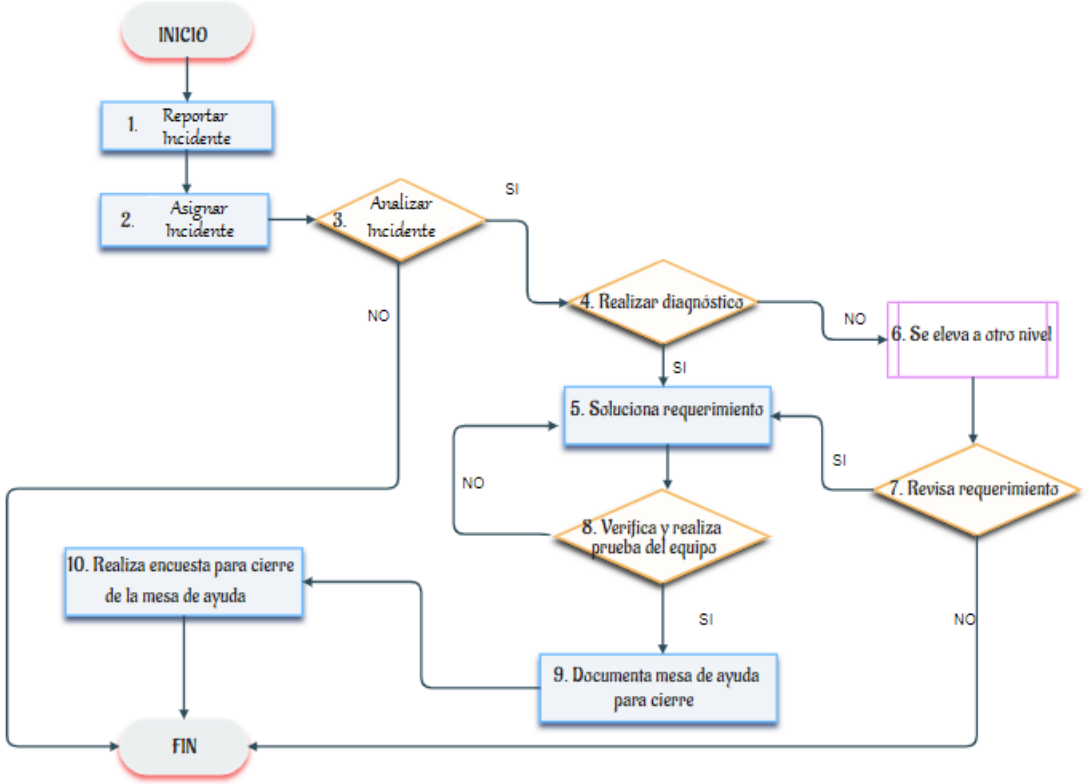
		SI: Continúe con la Actividad 10 NO: Regrese a la Actividad 6	
9	Documentar en la mesa de ayuda	n) La persona que está respondiendo a la solicitud informará el estado del ticket en el repositorio designado, cerrando la gestión, con el consentimiento del usuario.	
10	Realizar encuesta para cierre de la mesa de ayuda	o) El usuario realiza la calificación de la mesa de ayuda y realiza el cierre. Si el usuario no cierra el incidente, esté quedará en la lista de espera.	
11	Reporte de Estadísticas	a) Obtención de un análisis estadístico de incidentes atendidos b) Estadística de los casos atendidos	

Diagrama de flujo

PROCEDIMIENTO: MANUAL PARA MESA DE SERVICIO

RED DE DATOS – EMPRESA JASSA TELECOM

ADMINISTRADOR DE RED



4.4.2 Manual de procedimientos para la Gestión de Configuración

EMPRESA JASSA TELECOM		
Manual de procedimientos para la gestión de Configuración		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-001
	Procedimiento:	Manejo de Gestión de Configuración
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Presentar el procedimiento a seguir al incorporar un nuevo dispositivo a la red y realizar sus respectivas configuraciones para que pase a formar parte de la administración y realice la función que le ha sido asignada.

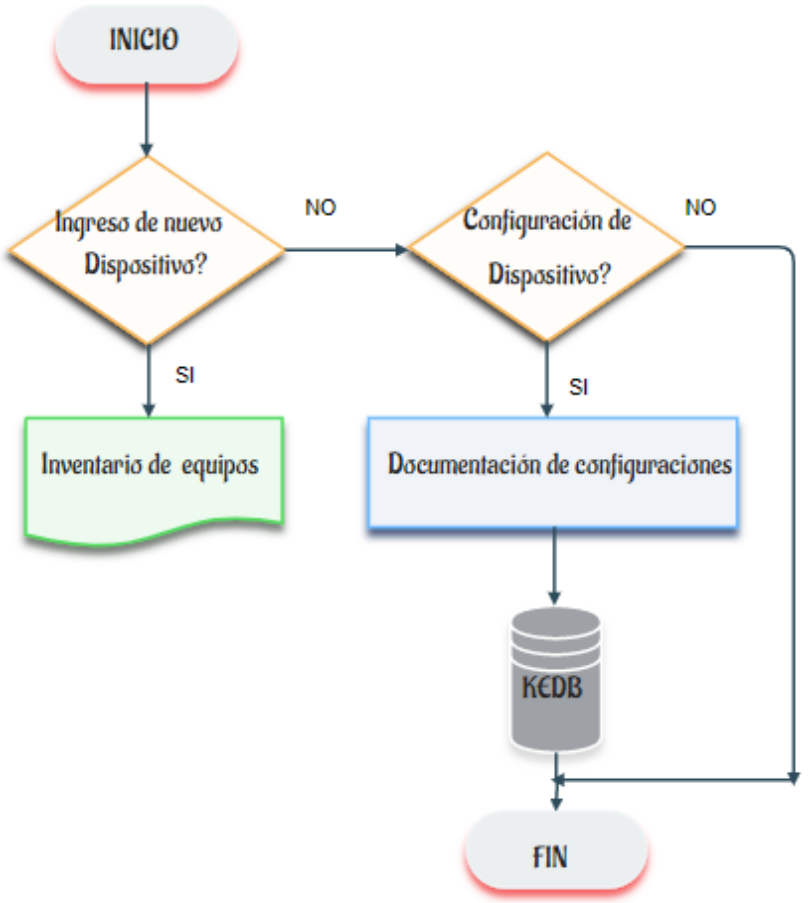
Alcance. - Este manual explica cómo agregar nuevos dispositivos a la red de la empresa; el procedimiento se aplica a cualquier dispositivo que se incremente. También explica los formatos para documentar los datos de los dispositivos recién agregados, así como los pasos a seguir para obtener una copia de seguridad del sistema de administración y los dispositivos

Descripción del procedimiento

N.º	Actividad	Descripción	Responsable
1	Proceso de ingreso de dispositivos	a) La institución cuenta con un sistema de compra de dispositivos, que consiste en presentar una solicitud admitida con las características necesarias al departamento que se encargará de financiarla.	Director de Tecnología
2	Compra del dispositivo	a) Al comprar un dispositivo, el personal de TIC debe justificar el uso del dispositivo para completar la compra.	
3	Implementación del dispositivo	d) Una vez que haya comprado el dispositivo, siga los procedimientos descritos en este manual para configurar el dispositivo.	
4	Nomenclatura para dispositivos de red	e) La Unidad de IT, determina la nomenclatura con el objetivo de identificar rápidamente los dispositivos de red.	
5	Recolección	f) La información del dispositivo se recopila para identificar el dispositivo y su configuración.	
6	Proceso de	g) Realizar la configuración del	

	Configuración de red	equipo, incluyendo: Configuraciones básicas de seguridad. h) Configuraciones de red basadas en la función del dispositivo.	

Diagrama de flujo

PROCEDIMIENTO: MANUAL PARA GESTIÓN DE CONFIGURACIÓN	
RED DE DATOS – EMPRESA JASSA TELECOM	
ADMINISTRADOR DE RED	

4.4.3 Manual de procedimientos para la Gestión de Contabilidad

EMPRESA JASSA TELECOM		
Manual de procedimientos para la gestión de Contabilidad		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-001
	Procedimiento:	Manejo de Gestión de Contabilidad
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

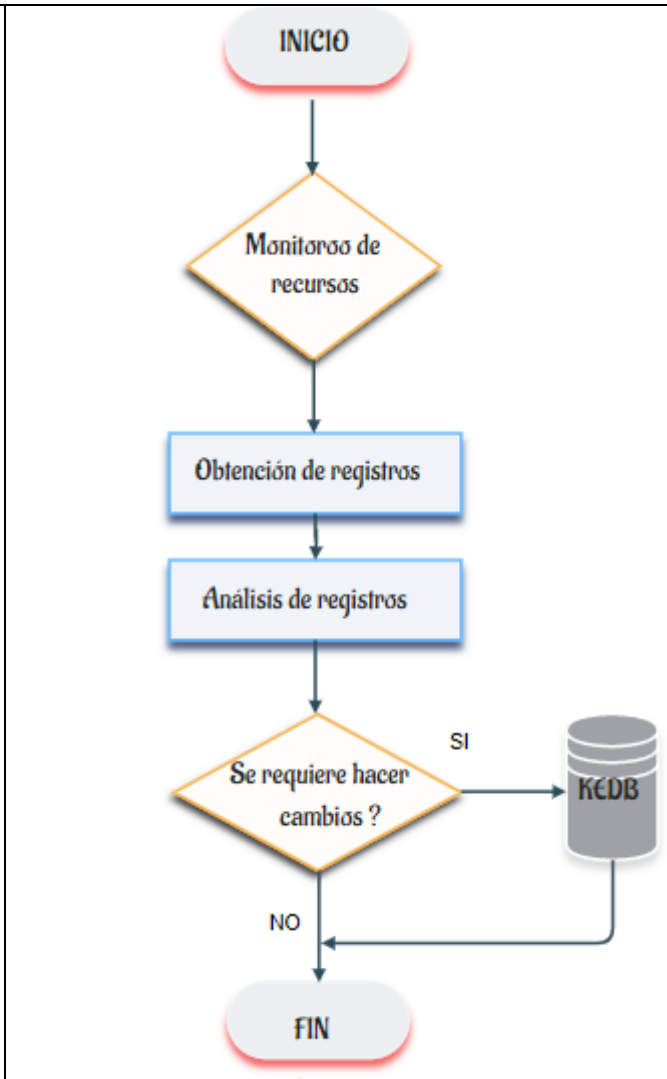
Objetivo. - Presentar el procedimiento a seguir para la configuración y seguimiento de los recursos y servicios que muestran el estado de los dispositivos de la red.

Alcance. - Este manual describe los pasos a seguir para evaluar el uso de los recursos de la red y generar informes sobre los dispositivos. El procedimiento se aplica a todos los recursos y servicios, lo que permite obtener información sobre el estado actual de la red.

Descripción del procedimiento

N.º	Actividad	Descripción	Responsable
1	Proceso de obtención de reportes	a) Supervisión de los recursos de la red: • Memoria • CPU • Estadísticas de tráfico en las interfaces b) Determinar el reporte o historial en base al tiempo de operación, ya sea semanal o mensual. c) Crear los informes en formatos pdf. d) Análisis de reportes. e) En caso de requerir cambios, continuar con el proceso de administración de la configuración	Director de Tecnología

Diagrama de flujo

<table>
<tr><td colspan="2">PROCEDIMIENTO: MANUAL PARA GESTIÓN DE CONTABILIDAD</td></tr>
<tr><td colspan="2">RED DE DATOS – EMPRESA JASSA TELECOM</td></tr>
<tr><td>DMINISTRADOR DE RED</td><td> 
</td></tr>
</table>

4.4.4 Manual de procedimientos para la Gestión de Prestaciones

EMPRESA JASSA TELECOM		
Manual de procedimientos para la gestión de Prestaciones		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-001
	Procedimiento:	Manejo de Gestión de Prestaciones
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Recopilación y análisis de información sobre el rendimiento de los recursos de los dispositivos gestionados

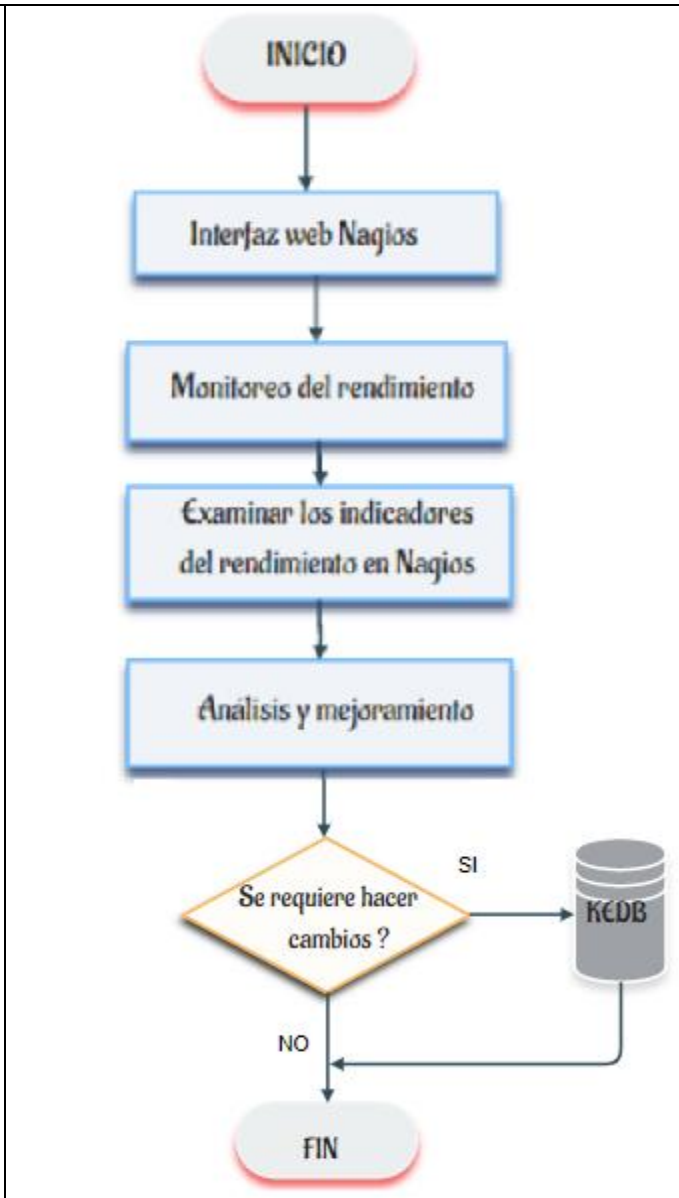
Alcance. - Esta gestión está ligada a la gestión de fallos, por lo que determina el comportamiento en varios aspectos, ya sea en un intervalo de tiempo concreto o en tiempo real. Esto le permitirá tomar decisiones adecuadas en función de los resultados del comportamiento de los dispositivos administrados. Al mismo tiempo, es necesario asegurarse constantemente de que los límites de los umbrales establecidos se cumplan dentro de los parámetros establecidos para su medición.

Descripción del procedimiento

N.º	Actividad	Descripción	Responsable

1	Monitoreo del rendimiento	a) Uso de la interfaz del software de gestión para representar gráficamente el rendimiento de los dispositivos de red. Se tendrán en cuenta los siguientes indicadores: • Tráfico de interfaz • Tiempos de respuesta • Disponibilidad periódica. b) Establecer límites para un rendimiento aceptable de la red.	Director de Tecnología
2	Examinar los indicadores	c) Los reportes generados deben ser evaluados para su posterior pronóstico. d) La planificación de la capacidad y las instalaciones se realizará de acuerdo con la previsión. e) Si se determina que se requiere un cambio, proceder al proceso de gestión de configuración.	

Diagrama de flujo

<table>
<tr><td colspan="2">PROCEDIMIENTO: MANUAL PARA GESTIÓN DE PRESTACIONES</td></tr>
<tr><td colspan="2">RED DE DATOS – EMPRESA JASSA TELECOM</td></tr>
<tr><td>ADMINISTRADOR DE RED</td><td> 
</td></tr>
</table>

4.4.5 Manual de procedimientos para la Gestión de Seguridad

EMPRESA JASSA TELECOM		
Manual de procedimientos para la gestión de Seguridad		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-001
	Procedimiento:	Manejo de Gestión de Seguridad
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Presentar los pasos a seguir para obtener acceso a los dispositivos de red, el sistema de gestión y todas sus herramientas.

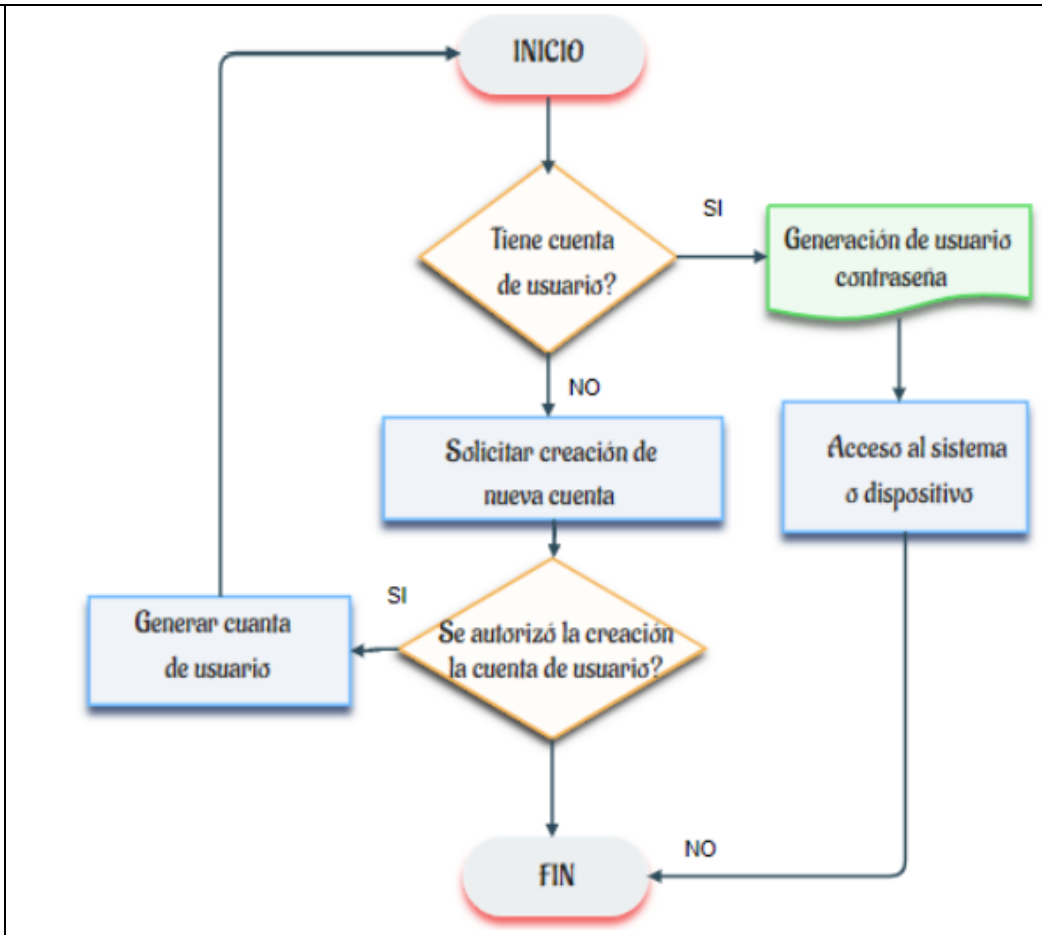
Alcance. - Este manual es la guía de procedimientos para obtener acceso a los sistemas y dispositivos de gestión. El procedimiento se aplica al sistema de gestión, es decir, la aplicación y los dispositivos que forman parte de la red de la empresa.

Descripción del procedimiento

N.º	Actividad	Descripción	Responsable
1	Acceso al software de gestión	a) El administrador de la red creará nuevas cuentas de usuario si se solicita, sujeto a la	Director de Tecnología

		aprobación del Director de DDTI. b) El nombre de usuario se generará usando la inicial del primer nombre y apellido completo. c) Solo los usuarios con cuentas de usuario podrán acceder al sistema de gestión de red	
2	Acceso a los dispositivos gestionados	d) El administrador de la red podrá acceder a los dispositivos administrados utilizando las contraseñas que están actualmente en uso en los dispositivos.	

Diagrama de flujo

PROCEDIMIENTO: MANUAL PARA GESTIÓN DE SEGURIDAD	
RED DE DATOS – EMPRESA JASSA TELECOM	
ADMINISTRADOR DE RED	

EMPRESA JASSA TELECOM		
Manual de procedimientos para la gestión de Seguridad		
	**Elaborado por:**	Lila Hermosa MSc. Fabián Cuzme
	Revisado por:	Msc. Alexander Trejo Gerente General
	Destinatario:	Administrador de red
	Código:	PRO-001
	Procedimiento:	Auditoría
	Aprobado por:	
	Fecha de elaboración:	Junio 2022

Objetivo. - Presentar los pasos a seguir para obtener una guía de gestión de riesgos basada en la identificación de los activos, de sus amenazas y vulnerabilidades.

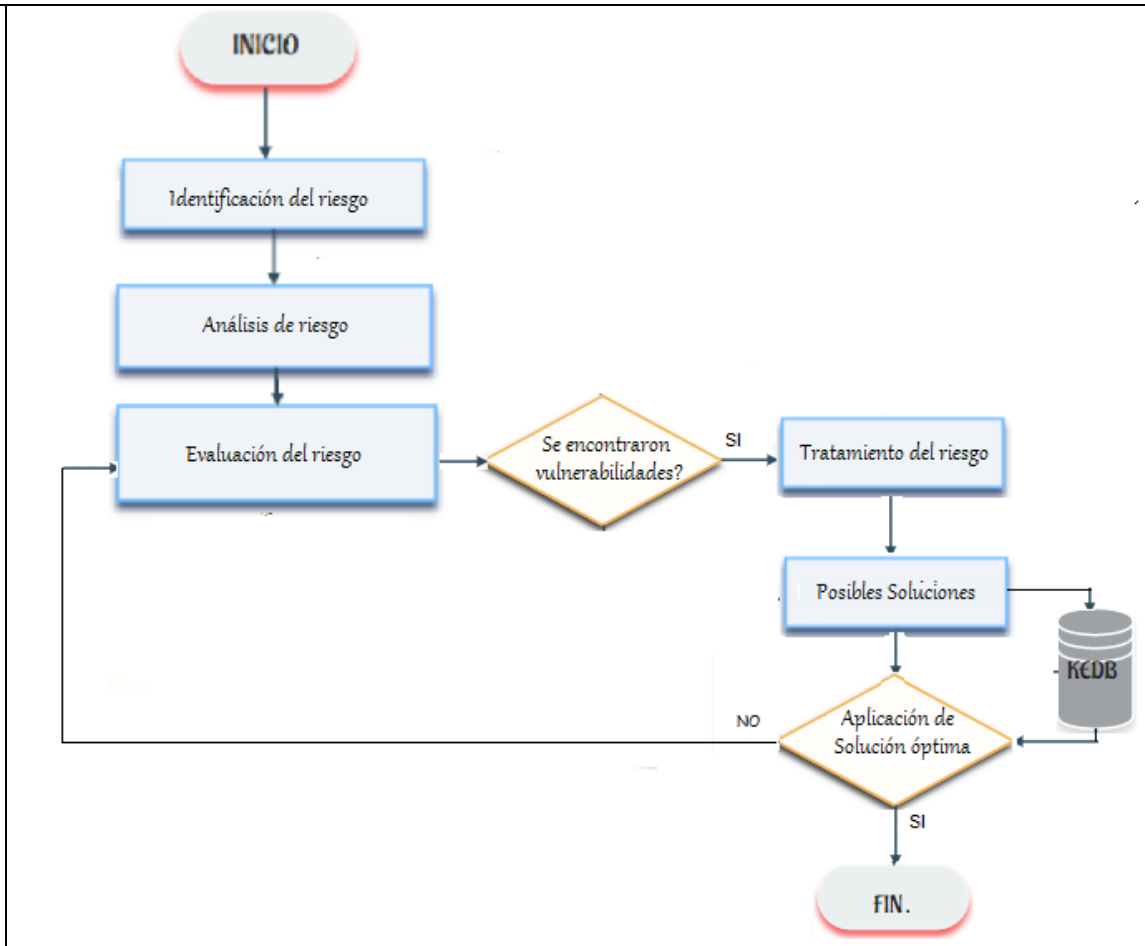
Alcance. - El proceso de gestión de riesgos está vinculado a la gestión de seguridad y consiste en definir el enfoque organizacional para la evaluación de riesgos y la posterior gestión de riesgos. Para mitigar el impacto de las amenazas, es fundamental comprender los riesgos a los que están expuestas las actividades, realizar un análisis y emplear enfoques estadísticos.

Descripción del procedimiento

N.º	Actividad	Descripción	Responsable
1	Identificación del riesgo	a) Definición del alcance. b) Identificación de activos. c) Identificación de	Director de Tecnología

		vulnerabilidades.	
2	Análisis de riesgos	d) Determinar probabilidad. e) Determinar consecuencias. f) Determinar nivel de riesgos.	
3	Evaluación del riesgo	g) Identificar controles para el riesgo. h) Verificar la efectividad de los controles. i) Establecer tratamiento	
4	Tratamiento del riesgo	j) Identificación de nuevos controles de seguridad. k) Implementación y reducción del riesgo.	
5	Posibles Soluciones	a) Aceptación del riesgo b) Si se determina que se requiere un cambio, proceder al proceso de gestión de configuración.	

Diagrama de flujo

PROCEDIMIENTO: MANUAL PARA GESTIÓN DE SEGURIDAD	
RED DE DATOS – EMPRESA JASSA TELECOM	
ADMINISTRADOR DE RED	

4.5 Selección e implementación de las herramientas en el modelo propuesto para la empresa JASSA TELECOM.

En este apartado se describe el desarrollo para llevar a cabo la implementación del modelo, con un enfoque en las áreas críticas de la red local de datos, teniendo en cuenta las cinco áreas funcionales del modelo de gestión de red y su interacción en el proceso.

4.5.1 Selección de herramientas de gestión.

Para iniciar el proceso de implementación en esta área de gestión, se requiere un análisis comparativo de las funcionalidades y mejores características de software de gestión libre y software de gestión comercial, como se puede ver a detalle en el apartado 2.13. El software de gestión fue elegido en base al estándar ISO / IEC / IEEE 29148: 2018, el cual proporciona normas para la creación de Especificación de Requisitos de Software (SRS), que están organizados en torno al paradigma de gestión de FCAPS y las necesidades de la organización. A continuación, en la Tabla 9 se realiza una comparación de las herramientas antes expuestas.

Tabla 9

Cuadro comparativo de Herramientas de monitoreo

			Herramientas de Gestión						
Requisitos	**Código**	**Descripción**	Hp OpenView	SolarWinds	IBM Tivoli	Nagios	Cacti	Zabbix	Zenoss
Requisitos Funcionales	RQ01	Monitorización y control	Si	Si	Si	Si	No	Si	Si
	RQ02	Notificaciones y alertas	Si	Si	Si	Si	Si	Si	Si
	RQ03	Generación de reportes	Si	Si	Si	Si	No	Si	Si
	RQ04	Soporte de envío de correo electrónico	Si	Si	Si	Si	Si	Si	Si
	RQ06	Visualización en forma gráfica	Si	Si	Si	Si	Si	Si	Si
	RQ07	Soporte SNMP	Si	Si	Si	Si	Si	Si	Si
	RQ08	Documentación suficiente	Si	Si	Si	Si	Si	Si	Si
Requisitos de usabilidad	RQ09	Fácil instalación, configuración y uso	Si	Si	Si	Si	Si	Si	Si
Requisito de rendimiento	RQ10	Performance	Si	Si	Si	No	No	No	No
Atributos del Sistema	RQ11	Seguridad	Si	Si	Si	Si	Si	Si	Si
	RQ12	Disponibilidad	Si	Si	Si	Si	Si	Si	Si
	RQ13	Escalabilidad	Si	Si	Si	Si	Si	Si	Si

Para la selección de las herramientas a utilizar, se establecen cuatro requisitos específicos, los cuales deben cumplir el software que se elija, conforme a los requerimientos indicados por el responsable de tecnologías de la empresa:

- ✓ Herramientas basadas Software libre y código abierto.
- ✓ Todas las aplicaciones deberían tener una Interface Web.
- ✓ Preferencia por software diseñado para sistemas operativos de tipo Linux.
- ✓ El software seleccionado debería contar con un amplio respaldo bibliográfico, con extensa experiencia en su utilización y aplicación.

El objetivo del software es ayudar a los administradores de red a realizar un seguimiento de los eventos que ocurren en la red y detectar problemas antes de que afecten a los usuarios. Además, el análisis tiene en cuenta los requisitos de la organización, uno de los cuales es el costo de adquisición e implementación, que debe ser bajo; como resultado, debe tener una licencia de software libre que garantiza actualizaciones y soporte.

Tras evaluar cada uno de los requisitos de las herramientas, se puede observar que la similitud entre ellas es relativa, lo que implica que todas las propuestas de software de gestión consideradas reúnen un número no despreciable de características y funcionalidades relevantes para los requisitos del proyecto. Sin embargo, en términos de reconocimiento y capacidad, Nagios es líder en el mercado, además de contar con una gran biblioteca de soporte y una amplia experiencia en su uso y aplicación,

Por ello, la herramienta escogida es Nagios porque cumple con los requisitos para el modelo de gestión propuesto, ventajas significativas de Nagios es que tiene un sistema robusto de dependencia de hardware y software con otros sistemas de hardware y software, presenta una gestión centralizada, permite el monitoreo remoto de varios sistemas operativos, establece umbrales que generan alertas cuando llegan a su límite máximo de funcionamiento

y envían notificaciones de correo electrónico o SMS al administrador de la red, brinda diversas opciones para la generación de reportes y datos estadísticos a partir de la información recolectada, y también soporta su instalación en un ambiente virtualizado, lo cual es fundamental para el desarrollo de la implementación. Existen herramientas complementarias que ayudan a las tareas de Nagios y la convierten en una herramienta más robusta e integrada.

- **MRTG.** (Multi Router Traffic Grapher) es una herramienta escrita en C y Perl por Tobias Oetiker y Dave Rand que se utiliza para monitorear la carga de tráfico en las interfaces de red. MRTG genera un informe HTML con gráficos que proporcionan una representación visual de la evolución del tráfico a lo largo del tiempo. La herramienta utiliza el protocolo SNMP para recopilar información sobre el tráfico del dispositivo (normalmente, enrutadores). Este protocolo proporciona datos en bruto sobre el número de bytes que han pasado por ellos, distinguiendo entre entrada y salida. Esta cantidad sin procesar debe manejarse adecuadamente para generar informes (Oetiker T. , 2017).
- **OCS Inventory. -** Es una solución de gestión de activos, útil en la gestión de registros y contabilidad, que permite la creación de inventarios de las actividades de TI, mediante la recopilación de información sobre el hardware y el software de los programas OCS del cliente existentes en la red, y luego visualiza la información recopilada a través de un interfaz web (FACTORFX SOLUTIONS OPEN SOURCE, 2021) .

- **GLPI. -** Es un software de código abierto para administrar servicios de tecnología de la información (ITSM), cuenta con un centro de soporte que permite a las organizaciones mejorar su infraestructura de TI, optimiza la productividad de los

empleados y reducir costos. GLPI proporciona una interfaz basada en web que permite a los usuarios crear su propia base de datos: asistencia multiusuario, uso de múltiples ubicaciones, gestión multilingüe, etc. Sus funciones principales son:

- Proporcionan la base de conocimientos
- Inventario (manual o automático)
- Gestión de problemas, incidentes, solicitudes, cambios, liberaciones y actividades (GLPI-PROJECT.ORG, 2021).

ITIL brinda asistencia en el diseño e implementación de procesos, así como evaluaciones para determinar cuan cerca está la organización de las actividades de las mejores prácticas y recomendar posibles mejoras. Estas áreas de ITIL están cubiertas por Nagios:

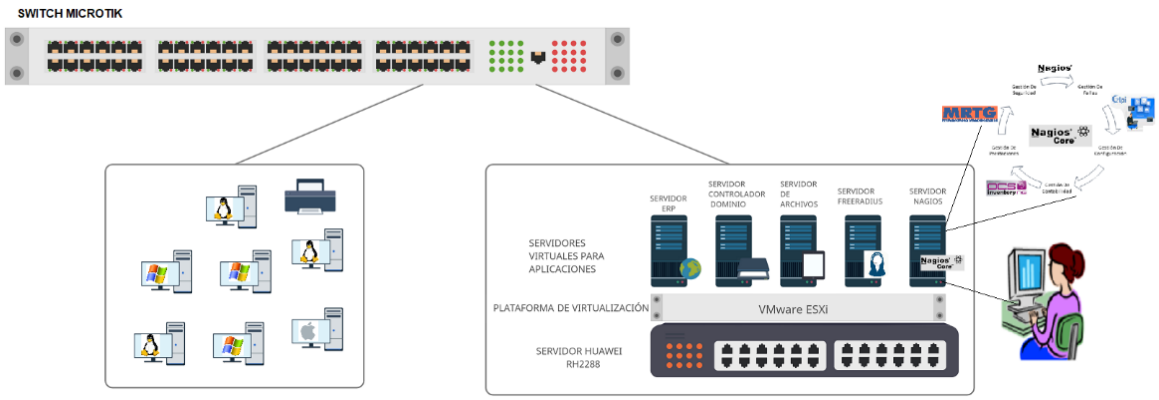
- Service Desk
- Incident Management
- Service Level Management
- Capacity Management
- IT Service Continuity Management
- Availability Management
- ICT infrastructure Management

4.5.2 Implementación del modelo de gestión de red

Se describe en detalle la implementación del modelo de gestión de red, compuesto por el administrador, los agentes, así como un protocolo de gestión, se está trabajando en base a cada una de las áreas funcionales del sistema de gestión de red FCAPS de la ISO. La figura 22 muestra el diseño del sistema de gestión de red implementado en la empresa JASSA TELECOM.

Figura 22

Diseño del sistema de gestión de red



Para realizar la configuración fueron asignadas 2 direcciones IP descritas en la tabla 10, que corresponden:

Tabla 10

Direcciones IP asignadas para configuración

Dirección IP del Servidor	192.X.X.X
Dirección IP del Agente	192.X.X.X

- Configuración del Gestor

La institución dispone de un servidor Huawei RH2288 V3 con las siguientes características, tabla 11, que es apropiado para la implementación del modelo de gestión.

Tabla 11

Especificaciones técnicas de Huawei RH2288 V3

Procesadores	Procesadores de la serie Intel® Xeon® E5-2600 v3/v4
Memoria	24 DDR4 RDIMMs/LRDIMMs Configuraciones de disco duro: 8 HDD o SSD frontales SAS/SATA de 2,5 pulgadas. 10 discos duros SATA frontales de 3,5 pulgadas. 12 HDD SAS/SATA frontales de 3,5 pulgadas (4 SSD NVMe compatibles con el modelo NVMe) y 2 módulos de disco duro traseros, cada módulo proporciona 2 HDD o SSD.
Almacenamiento interno	SAS/SATA de 2,5 pulgadas, o 2 SAS de 3,5 pulgadas /HDD SATA. 25 HDD o SSD SAS/SATA frontales de 2,5 pulgadas y 2 o 3 HDD o SSD SAS/SATA traseros de 2,5 pulgadas Memoria flash incorporada: 2 tarjetas mini-SSD (SATADOMs) 2 tarjetas SD
Puertos de red LOM	2 puertos GE o 4 GE, o 2 puertos 10 GE, o 2 puertos FDR InfiniBand de 56 Gbit/s
Expansión PCIe	Hasta 9 ranuras PCIe 3.0
Módulos de ventilador	Módulos de ventilador intercambiables en caliente en modo de redundancia N+1
Unidades de fuente de	2 fuentes de alimentación intercambiables en caliente en

alimentación	modo de redundancia 1+1
Administración	Utiliza el chip de gestión Huawei Hi1710 y puertos independientes Admite interfaces de administración estándar, como SNMP e IPMI; proporciona GUI, KVM remoto, medios virtuales, SOL, análisis predictivo de fallas (PFA), fuente de alimentación inteligente, control remoto y monitoreo de hardware Incorpora un panel LCD de pantalla táctil para el diagnóstico de fallas Admite el software de gestión Huawei eSight y la integración con sistemas de gestión de terceros, como VMware vCenter, Microsoft System Center y Nagios

Nota: Tomado de (HUAWEI, 2022)

4.5.2.1 Implementación dentro de la Gestión de la Configuración

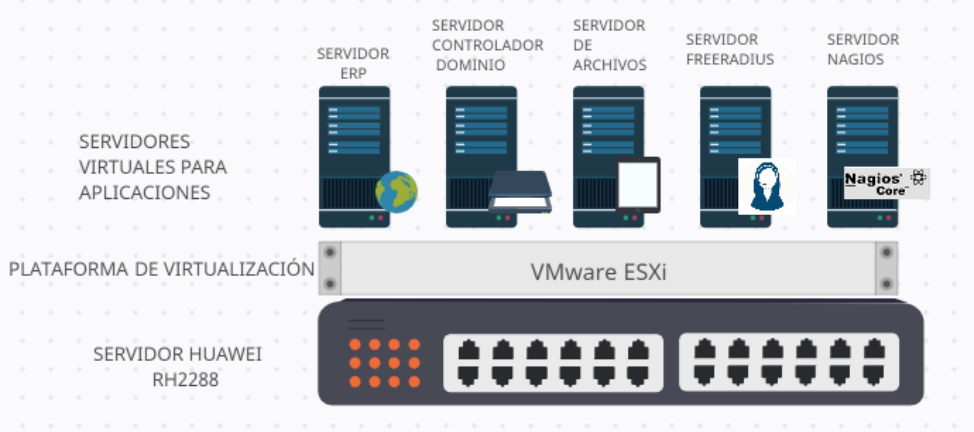
Una vez determinado el software de gestión a utilizar y los requerimientos de hardware que necesita para su funcionamiento se procedió a realizar el diseño del sistema de gestión de red como se indica anteriormente, en donde se observa que el servidor de administración Nagios se encuentra instalado en el servidor físico Huawei RH2288 v3 mediante un entorno virtualizado en VMware ESXi, el mismo que está conectado al switch de Core Microtik, donde se encuentra conectada toda la red local de datos de la entidad y a la vez este, está conectado con el firewall Huawei como el equipo de borde para conexión con la red del ISP.

Nagios fue instalado en el sistema operativo Centos 7 debido a que los servidores actualmente se encuentran dentro de un entorno de virtualización, Figura 23 y utilizando esta

versión de software libre, puesto que para los administradores de la red esta versión de Linux es una de las más utilizadas gracias a su fácil adaptación.

Figura 23

Servidores virtualizados en equipo Huawei RH2288

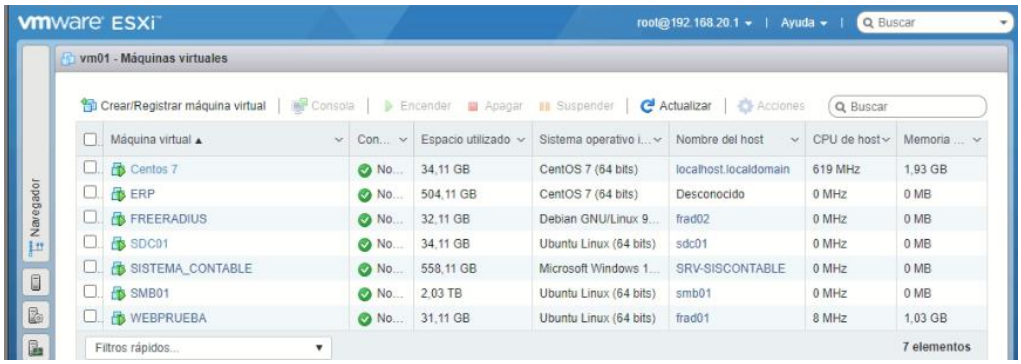


Nota: Servidores virtualizados para aplicaciones de la empresa JASSA TELECOM

En la Figura 24 podemos observar la página principal del entorno de virtualización en VMware ESXi con los servidores de la empresa JASSA TELECOM

Figura 24

Página principal VMware ESXi



Previamente a la configuración del servidor Nagios se debe instalar ciertos requerimientos de software que se puntualizan a continuación:

- Servidor web Apache.

- PHP: intérprete de lenguaje de script PHP, para algunos plugins que lo requieran.
- Perl: intérprete de lenguaje de script Perl, para algunos plugins que lo requieran.
- GCC: librerías de desarrollo y compilación.
- Net: paquete SNMP para comunicarse con los dispositivos a través del protocolo SNMP.

Utilizaremos una máquina que actúa como servidor, que se monitorizará a sí misma y a las máquinas remotas que configuremos, donde instalaremos:

- Nagios Core.
- Los plugins de Nagios.
- El plugin NRPE.

Y por otro lado tendremos una máquina que monitorizaremos remotamente y en la que instalaremos:

- Los plugins de Nagios.
- El servicio Nagios NRPE.

Para monitorear los servicios se debe instalar un agente de gestión, quien se encarga de recolectar los datos y enviarlos a la estación de gestión.

Proceso de monitoreo final de Nagios

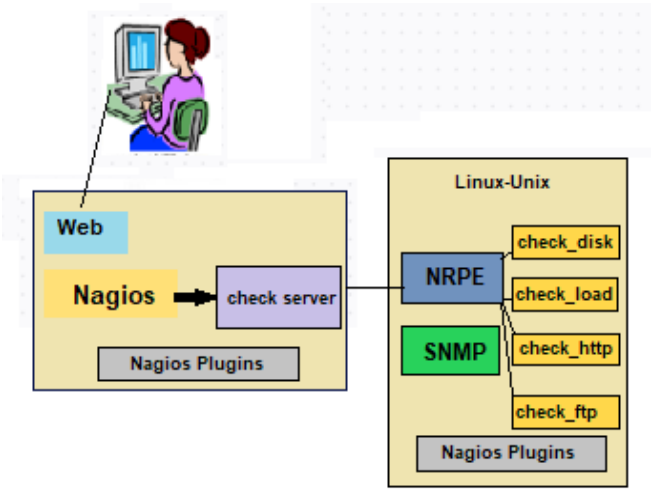
- El gestor de monitoreo de Nagios indica que servicios detectar, ejecutando el complemento check_nrpe.
- El gestor de monitoreo de Nagios se conecta al NRPE en la máquina monitoreada remotamente usando el protocolo SSL y verifica nrpe.

- El agente supervisado por NRPE ejecuta varios suplementos locales para detectar servicios y estados locales (carga del procesador, comprobar uso de discos, ping, etc.), en varios sistemas operativos.
- Finalmente, NRPE envía el resultado de la prueba al complemento check_nrpe de la terminal del gestor de Nagios, y check_nrpe agrega el resultado a la columna de estado de Nagios.
- Nagios lee la información en cola por turnos y luego muestra los resultados en la web.

En la figura 25, se muestra la descripción de la Implementación de Nagios en la empresa JASSA, de igual manera el procedimiento de configuración de Nagios y sus Plugins se presenta a detalle en el Anexo F con todos sus requerimientos para su eficaz funcionamiento.

Figura 25

Agentes en los servidores

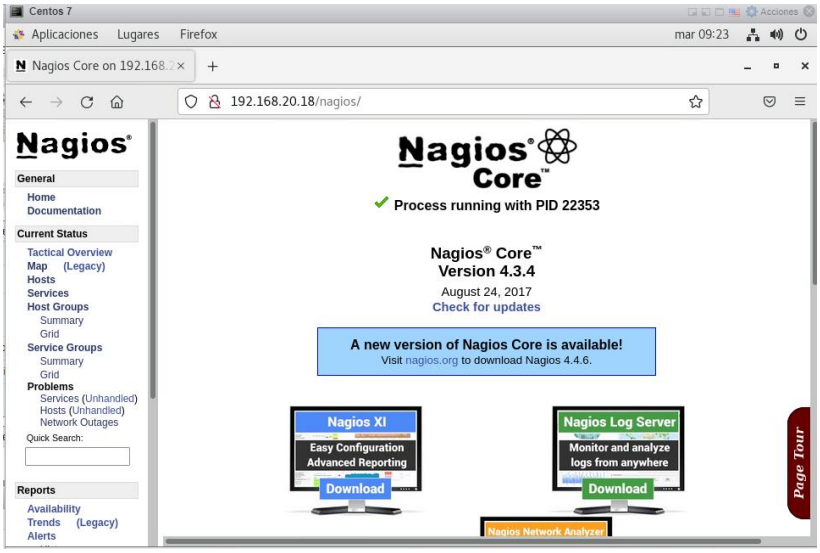


Nagios es una herramienta que facilita el inventario de equipos; al agregar un nuevo dispositivo al sistema de administración de red, se debe ingresar toda la información conocida del dispositivo. Como resultado, el dispositivo quedará registrado en el sistema, como se

muestra en la Figura 26, y el acceso a esa información estará disponible en cualquier momento.

Figura 26

Página principal de Nagios



Una vez instalado el servidor se podrá controlar todo lo que ocurre en el equipo final, gracias a la monitorización, previniendo cualquier fallo o determinando el origen de los mismos.

Para la gestión de inventario y de incidencias presentadas con los equipos y servicios inventariados se realiza la configuración e instalación del software GLPI y sus complementos el cual permitirá solventar los incidentes de gestión de red.

Implementación de la Mesa de Servicio GLPI

La mesa de servicio GLPI proporciona al administrador una base de conocimiento, que le permite llevar inventarios (manual o automático), gestionar los problemas, solicitudes, incidentes de una manera ordenada y atender los requerimientos de los usuarios oportunamente.

En la figura 27, se muestra la herramienta GLPI implementada en la empresa JASSA, de igual manera el procedimiento de instalación y configuración se presenta a detalle en el Anexo G con todos sus requerimientos para su eficaz funcionamiento.

Figura 27

Página principal de Nagios

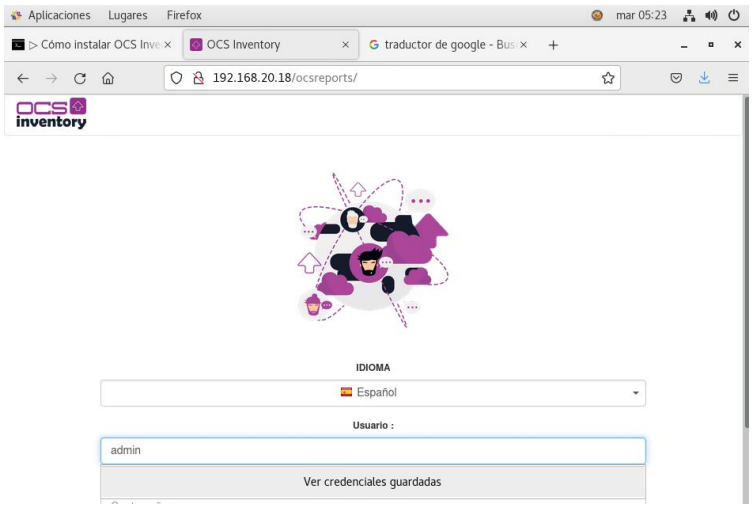
Además, se integró al sistema de inventario la herramienta OCS-Inventory, que se complementa con el Software GLPI.

Implementación de OCS Inventory

OCS Inventory recopila información sobre el uso de la red para luego obtener registros sobre los recursos utilizados, mejorando la eficiencia de los inventarios de hardware y software. Los agentes OCS envían composiciones de software y hardware al servidor a intervalos regulares, también consulta la red para descubrir elementos activos que no pueden ser atendidos por un agente y pueden integrarse en la funcionalidad de escaneo SNMP. En la figura 28, se muestra la herramienta OCS Inventory implementada en la empresa JASSA.

Figura 28

Página principal OCS Inventory



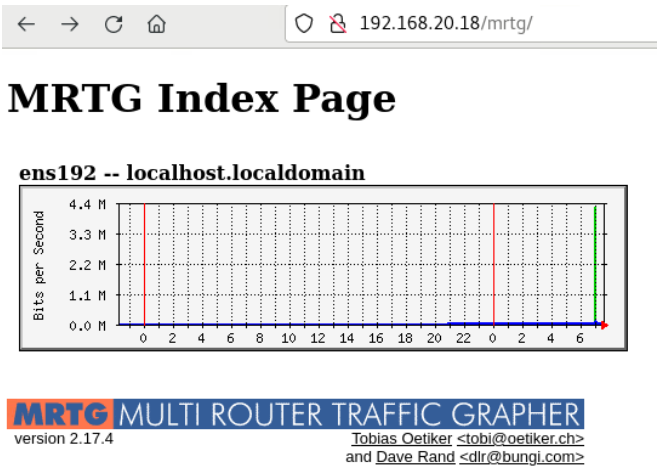
La implementación de esta herramienta se encuentra en el Anexo H.

Implementación MRTG

Es fundamental contar con un monitor de tráfico dentro de la red, este ayuda a medir el uso de la red para prever posibles fallas y tomar medidas. La herramienta MRTG lee los datos de los agentes SNMP instalados en el servidor Centos 7, con dirección 192.168.20.18, estos se representan gráficamente en un entorno amigable para el usuario y se utilizan para evaluar el rendimiento del equipo. En la figura 29 se visualiza la página inicial de MRTG instalada en el servidor.

Figura 29

Página HTML de MRTG



4.5.2.2 Implementación dentro de la Gestión de Fallos.

La implementación de la gestión de fallos comprende en realizar el proceso de localizar, diagnosticar y corregir problemas antes de que sucedan y una vez que han sucedido en los componentes hardware de los dispositivos de red gestionados. Esta gestión está interrelacionada con las otras gestiones del modelo. El objetivo principal de la gestión de fallos, es encontrar la mejor solución frente a cualquier incidente que ocurra, en el menor tiempo posible.

Todos los datos recuperados son procesados en tiempo real y visualizados en una pantalla amigable con el usuario, con el objetivo de brindar herramientas que faciliten el monitoreo y, a su vez, una toma de decisiones más eficiente sobre la administración de la red de la empresa, con el objetivo de cumplir con las tareas descritas. en el modelo FCAPS dentro de la administración. Los resultados y las pantallas se muestran a continuación

Nagios

La función principal de Nagios es un servidor de monitoreo que, ya sea distribuido central o geográficamente, prueba y planifica repetidamente los elementos de la red para determinar

su estado actual y detectar anomalías, este sistema se conoce como monitoreo activo (polling). Además, existe el monitoreo pasivo, en el que los dispositivos de la red tienen un módulo de software específico (agente) que notifica al servidor de monitoreo de ciertos eventos.

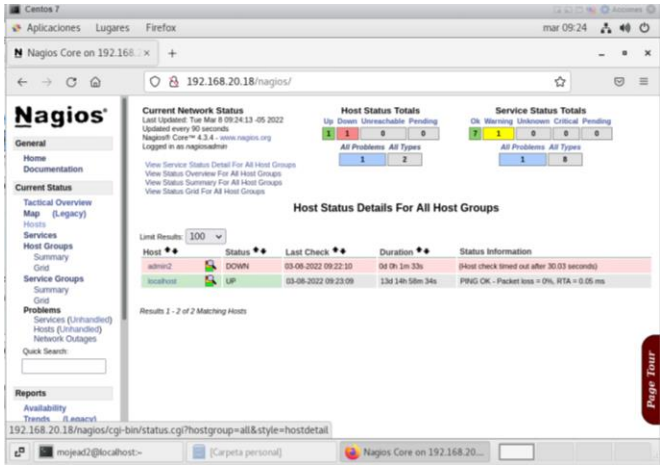
Los fallos son detectados de acuerdo alertas que genera el software de gestión Nagios, estas pueden ser visuales, que el administrador de la red genera para el seguimiento de un problema dentro de los dispositivos gestionados.

En la Figura 30 se observa como la herramienta Nagios, permite al equipo administrador supervisar el estado de los equipos remotos y así detectar fácilmente un fallo. Para el monitoreo la empresa JASSA TELECOM, ha proporcionado una máquina de pruebas identificado como admin2, que se encuentra dentro de su segmento de red con la dirección IP 192.168.X.X,

Nagios puede interactuar con una variedad de complementos para ampliar su funcionalidad, que puede definir gráficos de análisis de rendimiento de host improvisados, alarmas, registro automático y monitoreo redundante.

Figura 30

Hosts monitoreados



- **Comprobación de monitoreo en Nagios**

Cuando la estación de gestión genera una alerta esta debe ser detectada aproximadamente en el mismo instante de haber sido emitida, en este caso las notificaciones serán enviadas a los 90 segundos de haberse dado el fallo, para que el administrador de la red pueda actuar de forma inmediata. En la figura 31, se muestra las alarmas visuales que presenta la interfaz web del software Nagios.

Figura 31

Monitoreo de servicios en Nagios

Nota: Alarmas Visuales, Software Nagios

En la Tabla 12, según la cola de alertas, se explica cuando aislar un fallo en función del estado que produzcan los dispositivos gestionados. De esta manera, se espera que otros equipos no se vean afectados por el mismo problema y que se pueda encontrar la mejor solución, permitiendo que el resto de los componentes de la red sigan funcionando.

Tabla 12

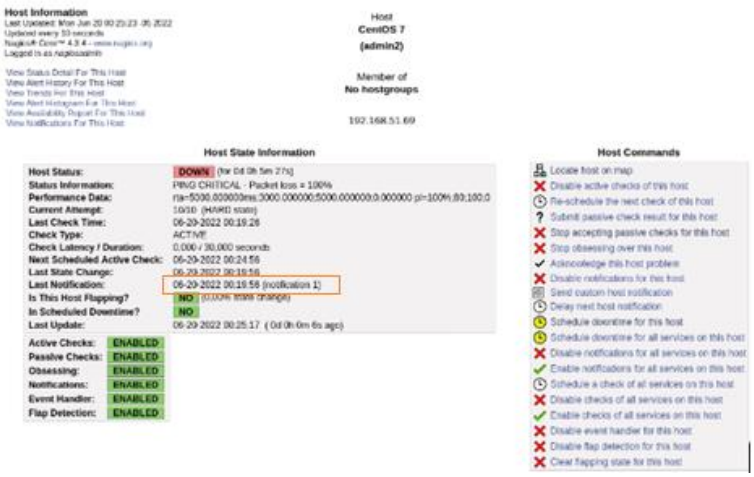
Jerarquía de alertas que genera Nagios

Estado	Representación	Descripción
Recovery/Recuperado		Un host está en UP y/o un servicio está en OK en la última comprobación del estado.
Warning/Advertencia		Se ha detectado problemas en la última comprobación en un host o servicio, antes de volverse crítico.
Down/Abajo Únreacheable/Inalcanzable Critical/Critico		En la última comprobación de estado ha ocurrido un fallo, un host está en Down/Abajo o Unreacheable/Inalcanzable, cuando un servicio esté en estado Critical/Crítico porque presentan problemas que sobrepasan de los umbrales normales de funcionamiento.
Unknown/Desconocido		Un servicio no está bien definido presenta este estado Desconocido
Pending/Pendiente		Está reconociendo una nueva configuración

Nagios al detectar que el Host está en estado down (crítico), permanentemente envía peticiones hasta que el host vuelva a estar activo (up), si no está activo genera una alerta que se envía vía e-mail, indicando que el servicio está caído. En la figura 32 muestra el estado y la notificación generada del Host agente.

Figura 32

Cambio de estado en Nagios



Nota: Notificación de Nagios

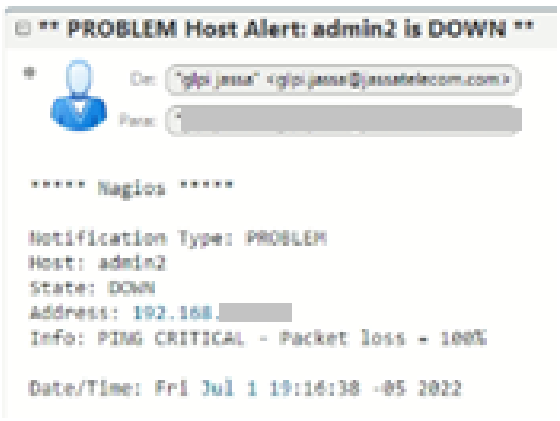
También se puede observar el próximo chequeo activo programado, el último cambio de estado y la última notificación enviada.

- **Notificación por correo electrónico**

Como sistema de alerta, se encuentra habilitado el envío de correos electrónicos. Nagios hace posible recibir actualizaciones por correo electrónico sobre el estado de varios recursos, lo que permite ser notificado de cualquier incidencia en tiempo real. En cuanto a las notificaciones, se debe tener en cuenta que Nagios permite configurar el envío de alertas al contacto adecuado, admitiendo realizar reconexiones o esperar un cierto tiempo antes de informar al administrador.

Figura 33

Notificación por correo



En la figura 33, se observa el correo de la notificación generada por Nagios, del dispositivo que presenta el problema, en este se detalla, el tipo de notificación, el host, el estado, la dirección IP y la información del estado del host.

Mesa de Servicio GLPI

La Mesa de Servicio es un elemento vital del área de TI en una organización, razón por la cual será el único contacto entre los usuarios, servicios de TI, con el fin de canalizar todas las observaciones, reclamos, inquietudes, necesidades y cambios relacionados con TI en el día a día. (Ariza Zambrano y Ramírez Cuero, 2012,31).

Para que exista un adecuado desarrollo del funcionamiento de la mesa se servicio, es importante, que los usuarios conozcan sobre las funcionalidades de dicho servicio, como, por ejemplo:

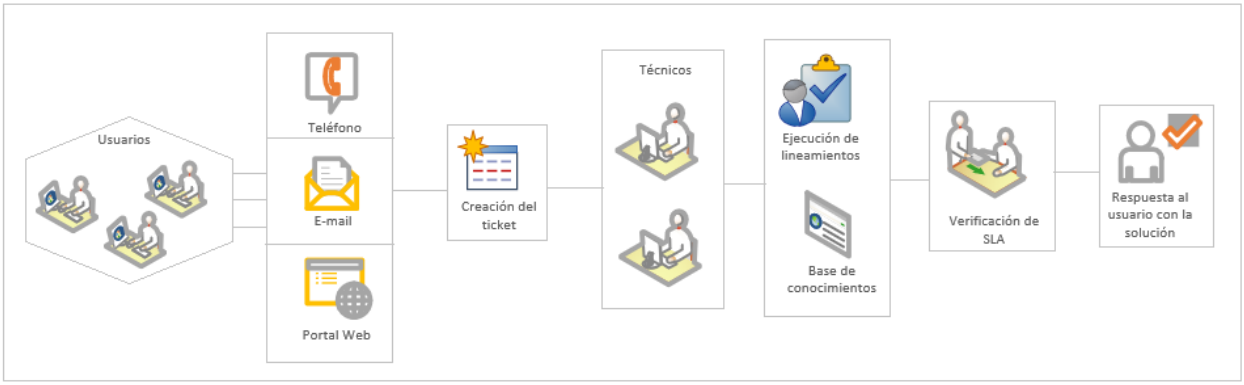
- Respuestas rápidas y acertadas a las incidencias y peticiones de servicio.
- Información pertinente del cumplimiento de los acuerdos de servicio (SLA’s).
- Registro y monitoreo de incidencias.

- Proveer soluciones transitorias, a errores identificados en colaboración con gestión de problemas.

En la figura 34, se observa el funcionamiento de la mesa de servicio.

Figura 34

Funcionamiento de la mesa de Servicio



Cuando ocurre un incidente existen diferentes formas para hacer la notificación a la mesa de servicio, puede ser por llamada telefónica, por correo electrónico o personalmente. Posterior a la notificación, se registra el incidente y se solventa el fallo mediante el uso de manuales o procedimientos establecidos, esto implica restaurar los servicios lo más rápido posible y cumplir con los acuerdos de nivel de servicio. El escalamiento de un incidente a un problema, requiere de procesos adicionales involucrados en la gestión de servicios de TI (gestión de problemas, gestión de cambios, etc.).

Tiempo de resolución de un incidente

El uso de Nagios reduce significativamente el tiempo que lleva identificar un problema.

- Su objetivo es asegurarse de que el administrador identifique el problema antes que los usuarios.

- Para reducir el tiempo de resolución, la supervisión y el análisis efectivos de todos los servicios críticos, así como la notificación oportuna, son esenciales.
- Los informes de incidentes y rendimiento ayudarán a resolver problemas y determinar la necesidad de crecimiento.
- Mejora de la gestión de la capacidad al estar directamente agnado al proceso ITIL.

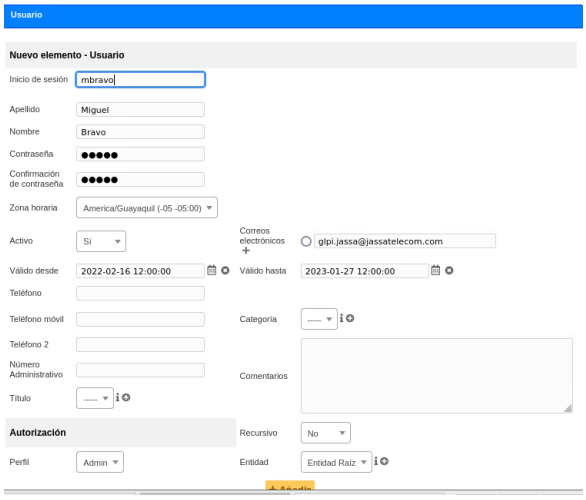
Las siguientes actividades se llevan a cabo dentro de GLPI.

- Registro de usuarios.
- Registro de activación del servicio (inventario TI).
- Registro de incidencias.
- Seguimiento automático por correo electrónico.
- Monitoreo mediante el uso del GLPI.
- Notificaciones por correo electrónico.
- Generación de tickets a través de la mesa de servicio.

Al ingresar a la aplicación, a primera vista se observa el amplio menú que ofrece, para comenzar a trabajar en la base de datos de GLPI, se debe alimentar el sistema, con la información de la empresa, se añaden usuarios con los permisos adecuados, equipos hardware y software de la infraestructura de TI, entre otros. En la figura 35 se observa la plantilla que genera GLPI para la creación de usuarios.

Figura 35

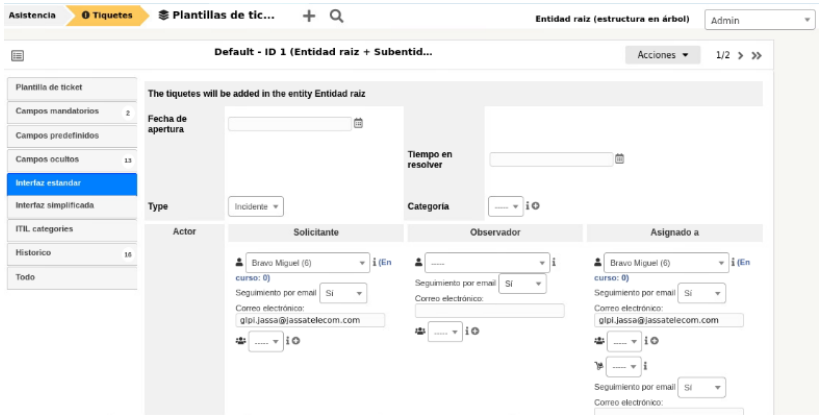
Generación de usuario administrador



Teniendo los principales requerimientos en el sistema GLPI se procede a generar el registro de incidentes por el usuario administrador. En la figura 36 se muestra la plantilla para generar un ticket.

Figura 36

Plantilla de GLPI para generar ticket



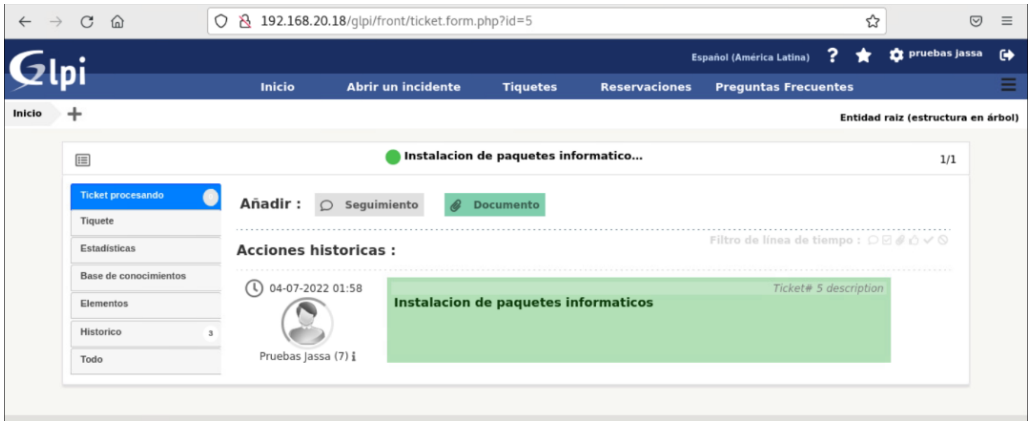
Generación de ticket

Para generar un ticket el usuario puede ingresar a la plataforma GLPI con el ID y contraseña proporcionada por el administrador, de acuerdo al requerimiento y a los accesos el

usuario puede generar su petición, la figura 37 presenta la notificación que llega al correo de GLPI administrador y se procede a dar inicio a la solución del incidente.

Figura 37

Ticket GLPI

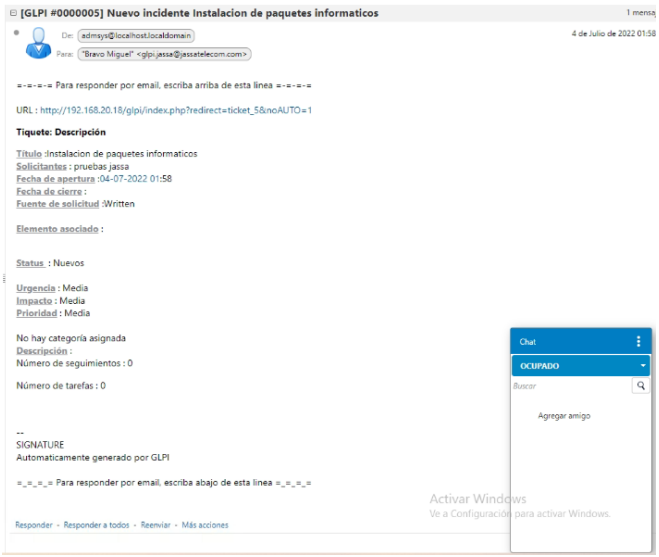


- **Generación de ticket por el usuario en la plataforma GLPI**

El ticket que es generado por el usuario llega al correo del administrador dando notificación para su respectiva atención, en la figura 38 se observa la notificación por correo electrónico al administrador.

Figura 38

Notificación de incidente vía correo electrónico

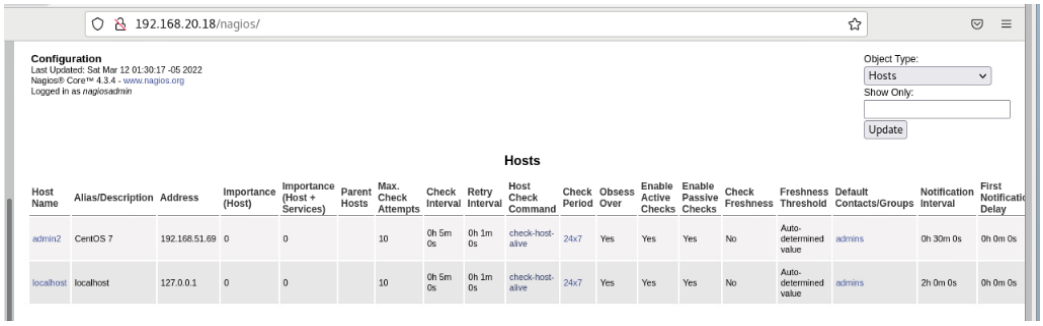


4.5.2.3 Implementación dentro de la Gestión de Contabilidad

Esta área se encarga de recopilar información sobre los equipos que hacen uso de la red, para que posteriormente se puedan obtener registros sobre los recursos utilizados. De igual manera, la herramienta Nagios da la facilidad de realizar inventarios de los recursos informáticos y de todo el software existente en la empresa, al añadir un nuevo dispositivo al sistema de gestión de red se debe ingresar manualmente la información conocida del dispositivo. De esta manera el dispositivo quedará registrado en el sistema, la Figura 39 muestra las configuraciones de los chequeos de cada uno de los dispositivos que se encuentra en la base de datos de Nagios y se puede acceder a dicha información en cualquier momento.

Figura 39

Inventario de Nagios



OCS INVENTORY da la posibilidad de hacer un inventario con más características de los activos de hardware y software totalmente actualizado y automático, realiza seguimiento de todo lo que se tenga inventariado en el sistema, en la figura 40, se observa la plantilla generada por esta aplicación.

Principio de Operación

- El servidor OCS recibe los inventarios enviados por los agentes en formato XML, así como los datos almacenados en la base de datos MySQL.

- Los agentes se ponen en contacto con el servidor.
- Durante este proceso, el servidor solo escucha.
- Las interacciones entre agentes y servidores se realizan a través de http y/o https.
- Las implementaciones de software y los escaneos SNMP solo se realizan a través de https.

Figura 40

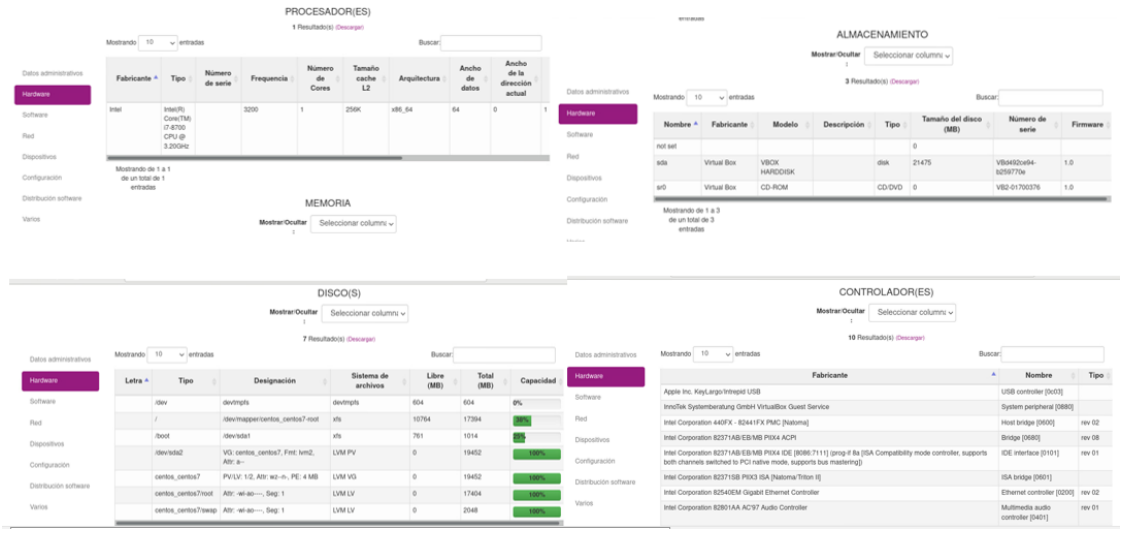
Inventario en OCS Inventory

La información que nos muestra es detallada del equipo monitoreado como el sistema operativo, versión Kernel y su descripción, dominio, memoria RAM entre otros.

AL ingresar a la opción Hardware se despliega toda la información correspondiente acerca del procesador del equipo, almacenamiento, partición de discos, controladores, etc. En la figura 41 se puede observar con más detalles estos datos.

Figura 41

Información de Hardware en equipo remoto



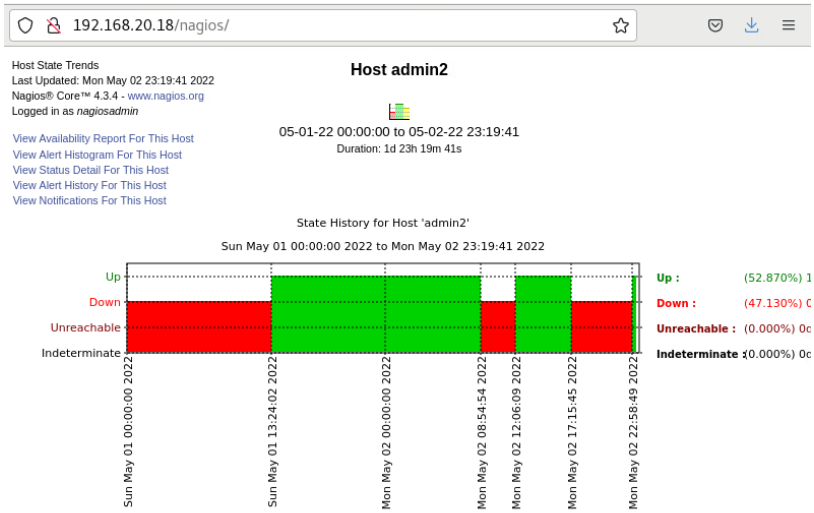
4.5.2.4 Implementación dentro de la Gestión de Prestaciones

En esta área, el desempeño de los recursos de la red se mide a través del monitoreo continuo de los equipos. Para un mejor monitoreo, Nagios separa los servicios o elementos del host. Adicionalmente, se distribuye al administrador de la red el manual del administrador, y contiene todas las configuraciones realizadas para asegurar el correcto funcionamiento del servicio Nagios.

NRPE ejecuta el comando en el cliente y proporciona la información para que Nagios la procese. En la figura 42 se observa el monitoreo del servicio SSH del cliente (admin2).

Figura 42

Monitoreo del servicio SSH del cliente



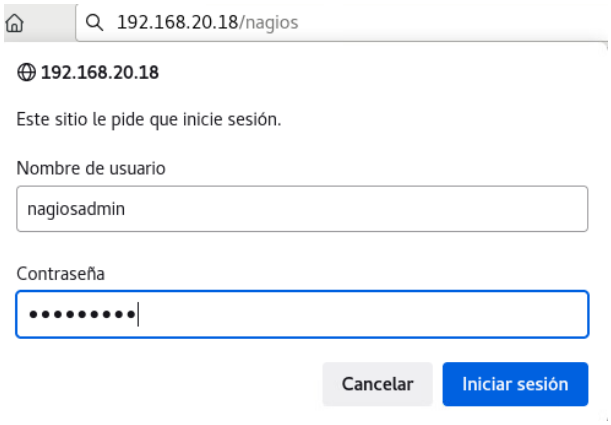
Nagios

4.5.2.5 Implementación dentro de la Gestión de Seguridad

Se ocupa principalmente del acceso a la red autenticado y autorizado, así como del cifrado de datos, es decir, controlar todos los accesos y protege todos los datos, administra los permisos de los usuarios. En este caso el Administrador de red da el acceso y los permisos necesarios a los usuarios de acuerdo a sus funciones.

Figura 43

Inicio de sesión en Nagios

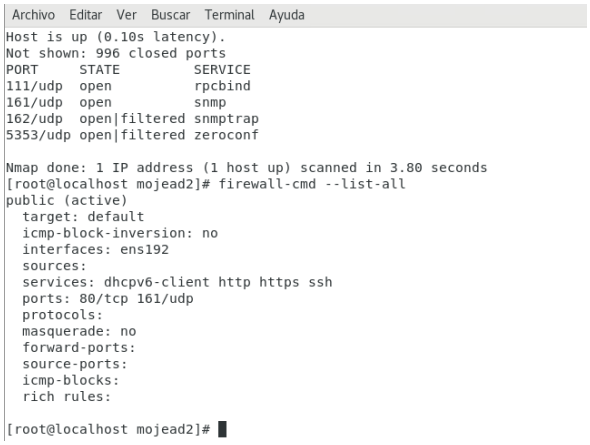


En la figura 43 se observa el acceso a la plataforma Nagios del administrador, es el único usuario permitido para realizar cambios.

De igual manera, para la gestión de seguridad la herramienta Nagios mediante su configuración establecida permite la gestión de puertos abiertos y cerrados dentro del servidor de administración, figura 44, permitiendo disminuir las vulnerabilidades y riesgos.

Figura 44

Gestión de puertos



Nota: Puertos abiertos Nagios

Una vez que hemos descubierto que el host está online, se puede realizar un escaneo rápido de puertos y comprobar si tiene un firewall filtrando todos los paquetes, o bien tenemos un puerto abierto para poder explotar alguna vulnerabilidad.

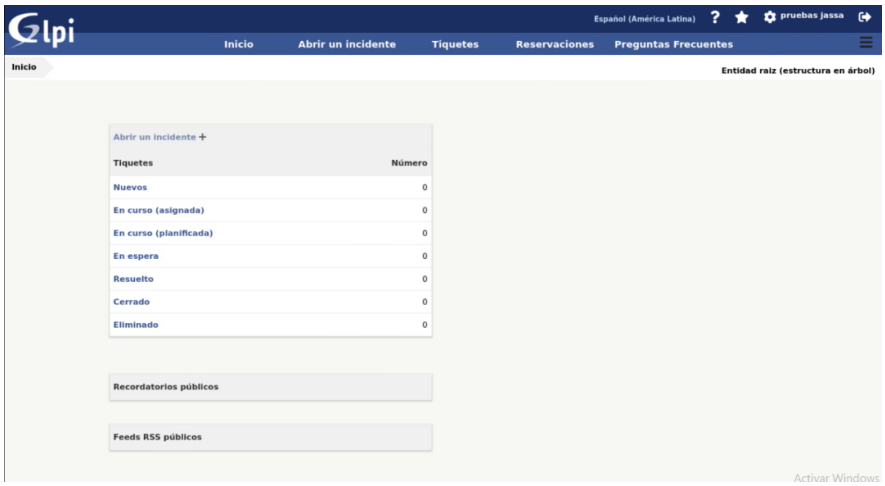
- **Prevención**

Acceso selectivo a recursos GLPI

El administrador es el encargado de generar los usuarios y permitir los accesos a la plataforma, proporcionando los privilegios necesarios para el manejo de esta. En el caso de GLPI, el usuario tiene privilegios únicamente para la generación de incidentes, figura 45.

Figura 45

Acceso de usuario interno a la plataforma GLPI



4.6 Resultados obtenidos

A continuación, en la tabla 13 se presenta una comparativa de los problemas de la empresa al iniciar el proyecto y después de la implementación del modelo de gestión.

Tabla 13

Tabla Comparativa de Resultados

Inicio	Actual
No cuenta con un sistema de monitoreo de red.	El departamento TIC cuenta ahora con un sistema de gestión de red gracias a la implementación de las herramientas, lo que ha mejorado la calidad del servicio y aumentado el rendimiento.
El personal y usuarios no tiene conocimiento del software para generación de incidentes.	Una vez realizada la capacitación del software al personal y con la ayuda del manual de la herramienta GLPI, ahora es de conocimiento del departamento de TI. El software GLPI es

	amigable con el usuario y su fácil acceso para la generación de incidentes, reducen la cantidad de tiempo necesario para encontrar una solución.
No existe un procedimiento de resolución de los incidentes de manera inmediata.	Se ha mejorado el tiempo de respuesta y atención, cada usuario tiene roles y formatos que le son asignados una vez que son registrados en la plataforma.
No se realiza un correcto registro de los problemas e incidentes suscitados en el día, en ocasiones se los realiza de manera manual y en ciertas ocasiones no se registran.	Actualmente se registra cada uno de los incidentes, mediante la mesa de servicio, sea vía telefónica o generando cada usuario en la plataforma GLPI.
EL personal de la institución no cuenta con un procedimiento a seguir para el tratamiento de procesos internos.	La contribución de las políticas y procedimientos facilitaron al personal del área de TICS al desarrollo de procesos que permiten el control, planificación y monitoreo de los recursos físicos y lógicos de la red.
No se generan reportes de los procesos de la empresa para la toma de decisiones.	Con la herramienta de gestión se encuentra disponible toda la información necesaria de los activos de la red, que sirven para la elaboración de informes y la toma de decisiones.
El personal de TI desconoce de las buenas prácticas ITIL v3	Con la información brindada, el personal tiene conocimiento de las mejores prácticas ITIL v3 para llevar a cabo una guía adecuada, garantizando la preparación operativa, la gestión eficaz de los recursos y la satisfacción

	del cliente interno.
El sistema no cuenta con alarmas visuales para corregir errores oportunos.	Al ingresar un equipo a la red, se establecen parámetros de configuración, en los que se habilitan las notificaciones de las alarmas visuales para el administrador de la red, con ello se disminuye el tiempo de solución de incidentes.

4.7 Análisis costo-beneficio

Los proyectos deben someterse a un análisis económico que determine su factibilidad y viabilidad y evitar gastos innecesarios o una mala inversión de recursos. En este subcapítulo se realizó el análisis de viabilidad económica a través de la relación costo-beneficio, que provee la implementación de herramientas de monitoreo y control de gestión de red, así como también, de una Mesa de Servicios mediante el software GLPI, para administrar la red y servicios de telecomunicaciones de la empresa JASSA TELECOM.

La inversión que propone este proyecto se fundamenta en el análisis de viabilidad de las herramientas de gestión utilizadas, la mesa de servicio, los beneficios operativos para el departamento de TI y sus usuarios.

4.7.1 Costo Infraestructura de Red

Los precios detallados a continuación se fijan en el mercado nacional al precio del año en curso. Es importante señalar que las cotizaciones incluyen el impuesto IVA, tanto por costos de infraestructura de red como por costos de instalación y configuración de equipos.

4.7.1.1 Software

El costo del software se determina tomando en cuenta las cuatro herramientas implementadas, con Nagios sirviendo como software principal de gestión de red y GLPI, OCS Inventory y MRTG como software complementario para la gestión de incidentes, contabilidad y la gestión de seguridad, respectivamente. La tabla 14 describe el total de costos de licencias de mantenimiento y soporte, cada licencia se otorga por un período de doce meses.

Tabla 14

Costos de software

Número	Ítem	Costo de mercado	Costo del proyecto
1	Licencia Nagios	$1,995.00	$0.00
1	Licencia GLPI	$3,456.00	$0.00
1	Licencia OCS Inventory	$2,536.00	$0.00
1	Licencia MRTG	$2,316.00	$0.00
1	Capacitación Software Libre	$260.00	$0.00
	Total	$10,563.00	$0.00

(NAGIOS , 2022) (GLPI, 2022) (OCS INVENTORY, 2022) (MRTG, 2017) (EUROINNOVA, 2022)

4.7.1.2 Hardware

Para el costo del hardware se toma en cuenta las proporcionadas por la empresa, ya que son equipos altamente eficaces para realizar la implementación, en la tabla 15 se encuentran definidos los valores de hardware.

Tabla 15

Costo Hardware

N.º	Ítem	Costo de Mercado	Costo de Proyecto
1	Servidor Huawei RH2288 V3	$24,168.00	$0.00
1	PC de Escritorio	$504.86	$0.00
Total		$24,672.86	$0.00

(ITPRICE, 2022) (AMAZON, 2022)

La tabla 16 describe la carga horaria para las actividades de implementación del proyecto de gestión de red.

Tabla 16

Descripción de labores por hora

ACTIVIDAD	**N.º HORAS**
Estudio de las condiciones de la red	40
Instalación y configuración de dispositivos de red	62
Puesta en marcha del sistema de gestión y pruebas de funcionamiento	30
Documentación guías y manuales de procedimiento	25
Capacitación al personal	3
Total, horas	**160**

La tabla 17 muestra los valores totales por realización del proyecto.

Tabla 17

Costos totales por horas de trabajo

Ítem	Detalle	Precio Unitario (USD)	Subtotal
480	Horas de trabajo	$2.70 x hora	$1.296.00
140	Recursos tecnológicos	$0.60 x hora	$84.00
15	Transporte	$8.00	$120.00
15	Alimentación	$5.00	$75.00
	Total		**$1,575.00**

Nota: Valores proporcionales a hora de trabajo, tiempo estimado tres meses. (MINISTERIO DEL TRABAJO, 2021)

4.7.2 Presupuesto total

Luego de analizar todos los parámetros de instalación, se determina el presupuesto total para la implementación de este proyecto tomando en cuenta los costos totales de hardware, software y la distribución de horas de trabajo detallados en las secciones anteriores. La tabla 18 denota el costo referencial de implementación del proyecto.

Tabla 18

Presupuesto total

Descripción	Costo de Mercado	Costo de proyecto
Costo de software	$10,563.00	$0.00
Costo de Hardware	$24,672.86	$0.00
Costos totales por hora de trabajo	$1,575.00	$0.00
Total	**$36,810.86**	**$0.00**

Factibilidad Económica. - El proyecto no registra gastos en este lapso de tiempo, ya que se utilizó herramientas de software libre para la implementación. En caso de ejecutarse el proyecto para una institución, se usará el presupuesto referencial planteado para la implementación de los equipos necesarios para soportar el proyecto. Los costos de licencias son exclusivamente para el soporte de software libre referenciados.

4.8 Beneficiarios

La implementación del proyecto Titulado "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 JASA TELECOM" y de las herramientas utilizadas para cubrir con las áreas funcionales del modelo de gestión FCAPS, es un proyecto que beneficia a la empresa JASSA TELECOM como entidad privada, al personal técnico encargado de la administración de la red y a sus usuarios internos, quienes acceden a una red constantemente monitoreada y disponible.

Beneficios para usuarios internos:

Los beneficiarios directos del proyecto propuesto son los usuarios internos, quienes se favorecen de una red más estable y disponible, ya que los problemas se resuelven en tiempos más reducidos, aumentando la productividad y permitiendo un acceso más fácil a los recursos y servicios de la red.

Beneficios para el administrador:

La unidad de TIC es uno de los beneficiarios importantes en el proyecto ya que ahora cuenta con un sistema de detección de fallas con mayor rapidez, una mejor gestión de inventario y la capacidad de obtener informes de rendimiento de la red casi en tiempo real, lo

que le permite prever y planificar futuras configuraciones mejorando la disponibilidad del sistema

Beneficios para la empresa

La implementación de este proyecto utilizando herramientas de código abierto brinda un beneficio significativo a la red de datos de la empresa JASSA TELECOM, ya que cuenta con una red en la que es posible realizar el mantenimiento y resolución de problemas de manera centralizada e inmediata a través de procesos, la detección temprana de incidentes mediante un sistema de alertas automatizado, mejorando significativamente la gestión de la red y, en consecuencia, la optimización de los recursos.

CONCLUSIONES

Con la implementación del modelo de gestión de red, “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 JASATELECOM”, se logró una gestión integral que abarca el monitoreo de la red, la gestión de incidentes de manera más efectiva y rápida, permitiendo disminuir el tiempo de respuesta y el tiempo en OFF de la infraestructura tecnológica.

A partir de la información recopilada del estado actual de la red, se establecieron las políticas de gestión que abarcan las cinco áreas funcionales del modelo FCAPS, con las cuales el personal de TI puede proceder de una forma adecuada, asegurando así el correcto funcionamiento de la red.

Se realizaron las pruebas funcionales en cada una de las áreas del Modelo FCAPS, y se demostró que el proyecto implementado contribuyó a la mejora de la red, al brindar un sistema de notificaciones mediante correo electrónico, lo cual permite al administrador conocer de manera oportuna los fallos suscitados en la red optimizando la resolución de los mismos, consiguiendo trabajar sin interrupciones y con alta disponibilidad.

El caso de estudio permitió evidenciar que el modelo es aplicable y cumplió con los objetivos de implementación de herramientas, levantamiento de información, implementación de manuales de procedimientos, documentación de información, y la formalización de procesos cumpliendo con los objetivos planteados inicialmente.

Anteriormente la resolución de incidentes no tenía mayor importancia y no se llevaba un registro, con el modelo de gestión implantado en cuanto a la gestión de incidentes se lleva un registro adecuado, ordenado y la resolución se efectúa de manera inmediata y no sobrepasa

las 24 horas de solución y si fuera el caso, el usuario se mantiene informado por medio de la plataforma el estado del incidente.

El modelo de gestión de red propuesto permite tener un proceso de mejora continua en las actividades de la unidad de TI, mediante el uso de las FCAPS de la ISO y el conjunto de buenas prácticas ITIL.

Mediante el proceso de gestión de prestaciones se cubre las necesidades del departamento de TI, ya que provee información del funcionamiento de la red en tiempo real, recolectando y analizando el rendimiento de la misma.

Con la instalación de las herramientas de gestión se alcanzaron resultados favorables para la empresa, en cuanto a monitoreo, orden y gestión de incidencias, logrando atender los requerimientos en tiempos más eficientes, alcanzando la satisfacción del usuario interno.

En cuanto al análisis de factibilidad técnica económica, se evaluó el hardware, software y el recurso humano de la empresa, determinando así que la implementación del proyecto es fundamental para una adecuada gestión de la red, asegurando la disponibilidad de la misma en situaciones críticas.

RECOMENDACIONES

La implementación del modelo de gestión debe ser vista como un proyecto a largo plazo. Es un proceso en evolución a medida que el personal de TI adquiere experiencia, este proceso debe ser apoyado por los líderes de la empresa, respaldado por técnicos y usuarios, y sustentado en capacitación permanente.

A futuro se recomienda realizar un proceso de mejora continua, que permita identificar nuevas herramientas y establecer procesos de actualización de manuales y procedimientos establecidos en el presente trabajo de titulación, para mejora de la gestión de red.

Se recomienda que el departamento de TI se concentre en los puntos críticos identificados y analizados por el FCAPS, para que el modelo de gestión propuesto pueda ser mejorado a futuro.

Se recomienda seguir los lineamientos de los manuales de procedimiento propuesto por el modelo de gestión, ya que son una referencia para resolución de improvistos que se presenten en la red, esto mantendrá el orden en la ejecución de procesos.

Para mantener un inventario actualizado y organizado, se recomienda que cada dispositivo conectado a la red de datos esté registrado en el sistema.

GLOSARIO

AppleTalk: Conjunto de protocolos desarrollados por Apple Inc. para la interconexión de redes locales

BML: Business Management Layer (Capa de Gestión de Negocios)

CAB: Evaluación de cambios por el consejo de asesores de cambios

CEO: Chief Executive Officer (Director Ejecutivo)

CLNS: Connection Less Network Protocol **(**Servicio No Orientado a Conexión); servicio que establece la comunicación entre entidades sin necesidad de establecer una conexión entre ellas.

CMIP: Common Management Information Protocol (Protocolo de administración de información común)

CMIS: Common Management Information Service (Servicio de información de gestión común)

CSI: Continual Service Improvement (Mejora Continua del Servicio)

DDP: Datagram Delivery Protocol **(**Protocolo de entrega de datagramas**)**

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host); Servidor de Red el cual permite una asignación automática de direcciones IP

Disponibilidad: estado operacional de una red de ordenadores y su capacidad para establecer conexiones, procesar el tráfico y responder a las solicitudes de los usuarios de forma rápida

DMZ: zona desmilitarizada es una porción de una red empresarial situada tras un cortafuegos, pero fuera de la red interna o segmentada de ella

EML: Element Management Layer; gestionar un subconjunto de elementos de red, desarrollando tareas de configuración, gestión de alarmas, registros de actividad, para ello, empleará el protocolo de gestión CMIP del ISO

Error conocido. - Problema que tiene un origen documentado y una solución alternativa

Escalamiento. - El acto de transferir la propiedad de un ticket de acuerdo con una necesidad funcional o jerárquica.

Evento. - Un suceso que es importante para la gestión de un servicio o activo.

FCAPS: Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad) que son las categorías en las cuales el modelo ISO define las tareas de gestión de redes.

Fiabilidad: La fiabilidad de un sistema es la probabilidad de que ese sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período de tiempo determinado (definición según IEEE)

Framework: Conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia.

Heterogénea: Red de conexión de ordenadores y otros dispositivos con diferentes sistemas operativos y/o protocolos

IAB: Internet Architecture Board (Comité de Actividades Internet); es el comité responsable del monitoreo y desarrollo de Internet designado por la Internet Society (ISOC).

ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información); Conjunto de conceptos y mejores prácticas referentes a la gestión de servicios TI

IMMPC: Instituto Mexicano De Mejores Prácticas Corporativas, es una organización multidisciplinaria, encargada de identificar, estudiar, promover y divulgar las mejores prácticas corporativas, así como la relación coherente, congruente y efectiva que existe entre ellas.

Impacto: Medida de la gravedad de un incidente.

ITSCM: IT Service Continuity Management (Gestión de la Continuidad del Servicio de TI); Representa una parte del Ciclo de vida del Diseño de Servicios de ITIL. Este proceso; recopila políticas y procedimientos orientados a ayudar a la organización a responder de forma efectiva ante fallas del sistema.

ITSM. – Information Technology Service Management (Administración de servicios de TI); es un enfoque estratégico para aportar valor al negocio mediante soluciones TI combinando de forma adecuada Personas, Procesos y Tecnología.

LightSquid: Aplicación vía web, que a partir de los logs generados por Squid, nos genera informes detallados de consumo y acceso a la red de los equipos

MIB: Management Information Base (Base de Información Gestionada); es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los parámetros gestionables en cada dispositivo gestionado de una red de comunicaciones.

NEL: Network Element Layer (Capa Elemento de red).

NML: Network Management Layer (Capa de gestión de red.).

NMS: Network Management Station (Estación de gestión de red); Servidor que ejecuta una aplicación de gestión de red.

NRPE: Nagios Remote Plugin Executor () se ejecutará como servicio o demonio en las máquinas a monitorizar y estará escuchando para que, desde Nagios, con el comando 'check_nrpe', le hagamos peticiones**.**

OID: Object identifier (Identificador de Objeto); es una secuencia de números que se asignan jerárquicamente y que permite identificar objetos en la red, siendo usados con gran cantidad de protocolos.

Plugin: Son complementos que añaden funcionalidades extra o mejoras a los programas. Funcionan como añadidos, pero no por sí mismos

Polling: Sondeo; Método de control de terminales en una red multipunto, consistente en que cada terminal es interrogado por el Host, por turno, para conocer su disposición a transmitir o recibir.

SARG: Squid Analysis Report Generator (Generador de Reportes de Análisis de Tráfico); Es una aplicación que genera estadísticas en formato html usando como datos los logs de Squid

Service Desk: Sistema diseñado para ser el punto principal de contacto entre los trabajadores TI y los usuarios.

Servicio: Es un medio para entregar valor a los clientes, facilitando los resultados que los clientes quieren lograr y sin que éstos tengan que asumir los costes y riesgos asociados a la consecución de dichos resultados

SGSI.: Information Security Management System (Sistema de gestión de la seguridad de la información).

SLA: Conjunto de políticas de administración de la información

SML: Service Management Layer; Es responsabilidad de este nivel la prestación de servicios a clientes, es por ello necesario tener una visión global de los recursos (servicios) disponibles en la red

SNMP: Simple Network Management Protocol (Protocolo simple de Gestión de Red); protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SSID: Service Set Identifier (Identificador de red); Nombre público de una red de área local inalámbrica (WLAN) que sirve para diferenciarla de otras redes inalámbricas en la zona

SSL: Secure Sockets Layer (Capa de Puertos Seguros); Protocolo para navegadores web y servidores que permite la autenticación, encriptación y desencriptación de datos enviados a través de Internet.

TIC: Information technologies and communication **(**Tecnologías de la información y la comunicación)

Escalamiento: servicio esperado y el tiempo de entrega esperado.

Urgencia: Una medida de la velocidad con la que se debe resolver un incidente.

REFERENCIA

© Universidad “Dr. Rafael Belloso Chacín” . (2010). *Planificación y Gestión de red.* Maracaibo: © Universidad “Dr. Rafael Belloso Chacín” .

Agencia de Regulación y Control de las Telecomunicaciones . (2016, Marzo 05). *Arcotel.* Arcotel: https://www.arcotel.gob.ec/wp-content/uploads/2015/06/RESOLUCI%c3%93N-05-03-ARCOTEL-2016-pdf-1.pdf

Amazon. (2021). *ROUTER ARRIS TG862*. Retrieved from https://www.amazon.com/-/es/Dg860a-Docsis-Wireless-Router-Gateway/dp/B00MJUF8TW: https://www.amazon.com/-/es/Dg860a-Docsis-Wireless-Router-Gateway/dp/B00MJUF8TW

Bacula.org. (2016, 12 22). *Bacula Documentation*. Bacula DokuWiki. http://blog.bacula.org/doku.php

Barba Martí, A. (1999). *Gestión de Red.* Editorial Universidad Politécnica de Cataluña.

Bartesaghi, M., Bernardo, F., & Zubía, F. (2004). *Gestión de Inventario de Red.*

Bastidas , J., Contreras, Y., Galito, Y., Ochoa, A., Pulido, Y., & Romero, R. (2011, Marzo). *FCAPS MODELO DE GESTIÓN.* https://es.slideshare.net/JhenniferBastidas/fcaps-7220464

BAUD, J.-L. (2016). *ITIL® V3 - Entender el enfoque y adoptar las buenas prácticas.* Barcelona: ENI.

Beal, V. (2021, Mayo 24). *Software de red*. Webopedia: https://www.webopedia.com/definitions/network-software/

Berthier, R., Cukier, M., Hiltunen, M., Kormann, D., & Gregg Vesonder, D. S. (2010). *Nfsight: NetFlow-based Network Awareness Tool.* AT&T Labs https://www.usenix.org/legacy/event/lisa10/tech/full_papers/Berthier.pdf

Calvo, Á. (2016). *Gestión de redes Telemáticas(UF1880).* IC. https://elibro.net/es/ereader/utnorte/44150

Cano-Pita, G. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones.

https://dialnet.unirioja.es/descarga/articulo/6313252.pdf

Circutor. (2021, 06 01).Gestion eficiente en sistemas de Telecomunicaciones.

http://circutor.com/es/documentacion-es/articulos/2864-gestion-eficiente-en-sistemas-de-telecomunicaciones

Contributors, EcuRed. (2016, Junio 15). *EcuRed*. Nagios.

https://www.ecured.cu/index.php?title=Nagios&oldid=2664517educaedu. (2021). Retrieved from Seminario Software Libre: www.educaedu.com.ec

electrónica, T. S. (2021). *UBIQUITI UCCK.*

https://tvc.mx/products/8770: https://tvc.mx/products/8770

ENI, B. b. (2021, 06). *ITIL® V3 - Preparación para la certificación ITIL®Foundation V3*.2da edición.Belearn by ENI.

https://www.ediciones-eni.com/open/mediabook.aspx?idR=7fd346770908671b13346

cac20d84b06

Enose, N. (2012, Febrero 06). A Unified management system for Smart Grid. *Institute of Electrical and Electronics Engineers IEEE*. doi:10.1109/ISET-India.2011.6145400

Estrada, C., Romero, J., & Vera, J. (2014, Junio 11). *FCAPS y SolarWinds.* Retrieved from

https://es.slideshare.net/jesus_vt91/art-35758987

FACTORFX SOLUTIONS OPEN SOURCE. (2021, Septiembre 12). *Acerca del Inventario OCS*. OCS Inventory.

https://ocsinventory-ng.org/?lang=en

Felicio, C., Alexandre, M., & Jacomo, B. (2014). *ITIL Information Technology Infrastructure Library*. REDCEDIA.

GLPI-PROJECT.ORG. (2021). *GLPI*. Retrieved from Gestión del Servicio de TI: https://glpi-project.org/es/

Guerrero, C. (2011). *EVALUACIÓN DE SISTEMAS DE GESTIÓN DE REDES BAJO SOFTWARE LIBRE DE LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO"[Tesis de Ingeniería, Universidad Politécnica Salesiana].* Repositorio Institucional.

Guzmán, E. (2018). *Impacto de la implementación del software de gestión para la fase de análisis de requerimientos funcionales en la Cooperativa Financiera Atuntaqui[Tesis de Maestría,Universidad Técnica del Norte]*. Repositorio Institucional UTN. Retrieved from http://repositorio.utn.edu.ec/bitstream/123456789/8223/1/PG%20647%20TESIS.pdf

Haag, P. (s/f). *User Documentation nfdump & NfSen versión PDF*. Retrieved from SOURCEFORGE.

https://www.first.org/resources/papers/conference2006/haag-peter-papers.pdf

Hegering, Abeck, & Neumair. (1998). *Integrated Management of Networked System.* Morgan Kaufmann.

Herrera Pérez, E. (2004). *Introducción a olas Telecomunicaciones Modernas.* (NORIEGA, Ed.) México: LIMUSA. S.A. DE C.V.

Humbrial, L. (2014, noviembre 19). *Elementos y procesos de la gestión*. Retrieved from El Maravilloso Mundo De Las Redes.

https://leandrojhumbrial.wordpress.com/2014/11/19/administracion-de-redes-2/

IBM. (2013). *IBM Tivoli Monitoring*. IBM.

https://www.ibm.com/docs/es/tivoli-monitoring/6.3.0?topic=63-quick-start-guide

IMMPC. (2021, 06 01). Retrieved from Instituto Mexicano De Mejores Prácticas Corporativas. https://www.immpc.org.mx/que-son-mejores-practicas

Iqbal, M., & Nieves, M. (2011). *ITIL Version 3 Service Strategy*. Best Management Practice Product.

https://www.kornev-online.net/ITIL/OGC%20-%20ITIL%20v3%20-%20Service%20Strategy.pdf

ISO, IEC, & IEEE. (2011). *International Standard ISO/IEC/IEEE 29148.*

ITU-T. (1996). *Recommendation M.3010*. Retrieved from Principles for a Telecommunications Management Network (TMN): https://www.T-REC-M.3010-200002-I!!PDF-E.pdf

JASSATELECOM. (2019). *JASSA TELECOM*.

http://jassatelecom.com/

Jiménez, J. (2015). *UF1875: Gestión de recursos, servicios y de la red de comunicaciones.* ELEARNING S.L.

Kaiser, A. (2011, Julio 2). *Abhinav PMP*.

http://abhinavpmp.com/2011/07/02/itil-2011-on-29-jul-2011/

Lago, N. & Sánchez, N. (2018). Presencia de la metodología ITIL en América Latina. *Congreso Internacional de Información*.

http://www.congreso-info.cu/index.php/info/info2018/paper/viewFile/596/516.

Linares, M., Sánchez, L., & Marcillo, K. (2017). Implementación de los sistemas de gestión de la red en dos universidades. *SINAPSIS, 2*(11), 6-15.

Liu, D., & Deters, R. (2008). Managemente of service-oriented systems. *Springer-Velarg London* , 52-62, DOI:10.1007/s11761-008-0028-1.

Lorge, F., Ricci, S., & Iglesias, A. (2020, s/f). *Introducción a la Gestión de Redes.* Universidad Nacional de Lujan. http://www.labredes.unlu.edu.ar/sites/www.labredes.unlu.edu.ar/files/site/data/aygr/AyG_Redes_2020_02_Intro_Gestion-Redes.pdf

Lubis, M. (2019, Julio 7). Optimization performance management with FCAPS and ITILV3: opportunities and obstacles. *Indonesian Journal of Electrical Engineering and Computer Science, 17(1)*. Indonesia. https://www.researchgate.net/publication/336144889_Optimization_performance_management_with_FCAPS_and_ITILv3_opportunities_and_obstacles

Mega , D., & Nurul, A. (2019). ANALYSIS OF NETWORK PERFORMANCE MANAGEMENT DASHBOARD. *International Journal of Mechanical Engineering and Technology (IJMET), 10*, 3-5.

Millán Tejedor , R. (1999). Consultoría Estratégica en Tecnologías de la Información y la Comunicación.

http://www. ramonmillan. com/tutoriales/gestionred. php.

Millán Tejedor, R. J. (2003;2015). *Consultoría Estratégica en Tecnologías de la Información y Comunicaciones*.

http://www.ramonmillan.com/tutoriales/snmpv3.php

Molina Robles, F. J. (2010). *Planificación y administración de redes.* Madrid: Madrid [España] : RA-MA Editorial.

Montoya, Y., Duarte, G., & Lobo, R. (2011). *SISTEMA DE GESTIÓN DE REDES Y SERVICIOS DE TELECOMUNICACIONES.* Mérida- Yucatán, México.

Muharman, L. (2020, Enero). Optimization performance management with FCAPS and ITILv3: opportunities and obstacles. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(1), 281-290. doi:10.11591/ijeecs

Oetiker, T. (2017, Mayo). *MRTG*. Retrieved from Tobi Oetiker's MRTG - The Multi Router Traffic Grapher.

https://oss.oetiker.ch/mrtg/

Oetiker, T. (2017, Marzo 05). *Oetiker's*. MRTG: https://oss.oetiker.ch/mrtg/doc/index.en.html

Orozco, P. (2010, 02 22). *Gestión de red*. Paco Orozco.

https://es.slideshare.net/pakus/gestion-de-red

Pandora FMS team. (2021, Noviembre 12). *Las 16 mejores herramientas de monitoreo de Redes*. PANDORAFMS.

https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

PandoraFMS. (2021, Octubre 19). *Alternativas a HP OPen View*. PANDORAFMS. https://pandorafms.com/blog/es/alternativas-a-hp-open-view/

Planificación y Gestión de Red. (2010). Maracaibo.

http://gssi.det.uvigo.es/users/mramos/public_html/gprsi/gprsi4.pdf

Quispe, L., & Ramírez, F. (2017). *ISSU*. Arquitectura TMN: https://issuu.com/onzdenaz/docs/arquitectura_20tmn

Robles, F. (2014). *Redes Locales.* RA-MA, S.A.

Router-Switch.com. (2021). *USG6320-AC Datasheet*.

https://www.router-switch.com/pdf/usg6320-ac-datasheet.pdf:https://www.router-switch.com/usg6320-ac-p-21485.html

sincables. (2021). *UAP-AC-LR UniFi AP Dual Band Long Range 2.4/5GHz*.

https://sincables.com.ec/product/unifi-uap-ac-lr-ant-3dbi-dualband/

sincables.ec. (2021). *Router Switch de 24 puertos Gigabit*.

https://sincables.com.ec/product/crs326-24g-2srm-cloud-router-switch-24p-gigabit-2xsfp/: https://sincables.com.ec/product/crs326-24g-2srm-cloud-router-switch-24p-gigabit-2xsfp/

Solís, C. (2014). *Implementación de NOC para el monitoreo de Servicios e Infraestructura de Redes para el Banco de Loja, basado en Software Libre.* UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA.

http://dspace.utpl.edu.ec/bitstream/123456789/9187/1/SOLIS%20ALVAREZ%20CAMILO%20JAVIER%2028-03-2014.pdf/

STEG. (2021). *STEG Electronics AG* .

https://www.steg-electronics.ch/de/merkliste

Subramanian, M. (2000). *Network Management: Principles and practice*. Feedipedia.

https://pdfslide.net/documents/telecommunication-management-network-tmn-mani-subramanian-network-management-principles-and-practice-addison-wesley-2000.html

The Cacti Group. (n.d.). *About Cacti*. Cacti.

https://www.cacti.net/

The ITIL Toolkit. (2019). *News and Information for ITIL The IT Infrastructure Library*. ITIL.

https://itsm.fwtk.org/Toolkit.htm

The Use of FCAPS and Itl in Managing the Network of a Medium to Large Public Sector Organisation. (n.d.).

URBE. (2010). *Planificación y Gestión de Red.* Maracaibo: URBE.

Varela, C. (2003). Gestión integrada de telecomunicaciones y TMN de la ITU. *XDOC.MX*, 29.

Von, J. B. (2010). *Fundamentos de ITIL®. 3ra*. Holanda. Van Haren Publishing, Zaltbommel.

WifiSafe. (2021). *Switch 8 Puertos PoE 24-48V para equipos Ubiquiti gestion VLANs*.

https://www.wifisafe.com/switch-8-puertos-poe-24-48v-para-equipos-ubiquiti-gestion-vlans.html: https://www.wifisafe.com/switch-8-puertos-poe-24-48v-para-equipos-ubiquiti-gestion-vlans.html

Zabbix LLC. (2016). *Zabbix Features*. Zabbix.

https://www.zabbix.com/

ANEXO A. Mapeo ITIL v3 y FCAPS

	FALLOS	CONFIGURACIÓN	CONTABILIDAD	RENDIMIENTO	SEGURIDAD
• Gestión de la Demanda					
• Gestión de Relaciones con el Negocio					
• Gestión Financiera para los servicios de TI			X		
• Gestión del Portafolio de Servicios					
• Gestión de la Estrategia para los servicios de TI					
• Coordinación del Diseño					
• Gestión del Catálogo de Servicios					
• Gestión de Nivel de Servicio (SLM)				X	
• Gestión de la Disponibilidad				X	
• Gestión de la Capacidad				X	
• Gestión de la Continuidad del Servicio de TI (ITSCM)				X	
• Gestión de la Seguridad de Información					X
• Gestión de Proveedores					
• Planeación y soporte de la transición					
• Gestión de Cambios		X			
• Gestión de Entregas y Versiones					
• Gestión de la Configuración y Activos del Servicio		X			
• Gestión de Liberaciones e implementaciones		X			
• Evaluación del Cambio					
• Validación y Pruebas del Servicio					
• Gestión del Conocimiento					
• Gestión de Eventos					
• Gestión de Incidentes	X				

• Gestión de Problemas	X				
• Gestión de Peticiones					
• Gestión de Accesos					
Funciones:					
• Mesa de servicios	X				
• Gestión de aplicaciones					
• Gestión Técnica					
• Gestión de Operaciones de TI					

ANEXO B. Especificación de Requerimientos de software

1. Introducción

El presente documento ha sido organizado de acuerdo a la especificación IEEE 29148:2018 (antes el IEEE 29148:2011), con el fin de definir claramente los requisitos para la implementación del software de gestión de red, para la empresa JASSA TELECOM, empleando las buenas prácticas sugeridas por el estándar.

1.1 Propósito

El software a definir tiene el propósito de monitorear los equipos y controlar los servicios de la red, ayudando al administrador con notificaciones cuando el comportamiento de estos no es el deseado.

1.2 Alcance

El software de gestión de red debe tener las características necesarias para cubrir las cinco áreas operativas del modelo de gestión de red ISO/OSI: gestión de configuración, gestión de fallos, gestión de contabilidad, gestión de prestaciones y gestión de seguridad e ITIL v3.

1.3 Descripción general del producto

Esta sección describe la perspectiva del producto, define la relación del sistema con otros productos relacionados, sus funciones, características del usuario, y limitaciones del producto.

1.3.1 Perspectiva del producto

El software a especificarse debe ser compatible con los modelos de equipos de red existentes en la empresa JASSA TELECOM, además, debe tener una interfaz de usuario amigable e intuitiva.

1.3.2 Funciones del producto

- Autodescubrimiento de la red
- Monitorización
- Notificaciones y alertas
- Inventariar componentes
- Visualización en forma gráfica
- Escalabilidad
- Notificación de e-mail

1.3.3 Características del usuario

• Administrador de red: Ingeniero en Electrónica y redes de Comunicación, Responsable Infraestructura Tecnológica, Desarrollo Tecnológico e Informático.

1.3.4 Limitaciones

- El software debe ser Open Source.
- El software debe soportar el protocolo de gestión de red SNMP.
- Debe ser compatible con los equipos de red presentes en la misma.
- Debe ser un software versátil

1.4 Definiciones

• Especificación de Requisitos Software: Conjunto de requerimientos que describen la funcionalidad que el software debe tener para cumplir con los objetivos de implementación.

• Open Source: Open Source o código abierto es el software distribuido y desarrollado libremente.

2. Requisitos Específicos

2.1 Interfaces externas

El administrador de la red podrá acceder al sistema remotamente desde un PC o computador portátil utilizando su cuenta de usuario. Desde allí podrá visualizar el estado de la red, así como ejecutar las acciones relacionadas al control de red.

2.2 Requisitos Funcionales

• RQ01: Monitorización y control. El software debe recuperar la información de los agentes en tiempo real. Además, debe tener la posibilidad de realizarlo de manera remota.

• RQ02: Notificaciones y alertas. En caso de encontrarse una falla, el software debe notificarla inmediatamente, ya sea desde la interfaz de usuario o en el mejor de los casos enviando un correo electrónico al administrador de la red.

• RQ03: Generación de reportes. El software debe ser capaz de emitir reportes (informes, historiales y datos estadísticos) acerca de los dispositivos gestionados.

• RQ04: Soporte de envío de correo electrónico. El software deberá enviar correos electrónicos informando cuando ocurra un fallo en algún dispositivo gestionado que sea considerado como prioritario.

• RQ05: Visualización en forma gráfica. Ver la información de la red de manera gráfica para un mejor entendimiento e interpretación.

• RQ06: Soporte SNMP

El software deberá soportar el envió de información mediante SNMP.

• RQ07: Documentación suficiente El software deberá poseer información suficiente y clara, de una comunidad que lo respalde.

2.3 Requisitos de usabilidad

• RQ08: El software deberá ser de fácil instalación, configuración y uso.

2.4 Requisitos de rendimiento

RQ09: Performance. - El funcionamiento de los dispositivos monitoreados no debe ser afectado por nuevas funciones instaladas en los mismos.

2.5 Atributos del sistema

• RQ10: Seguridad. El administrador de la red estará autorizado para acceder al sistema de gestión, mediante un login y password.

• RQ11: Disponibilidad. El sistema deberá estar en funcionamiento las 24 horas del día todos los días para emitir alertas en cualquier momento que se produzca un fallo.

• RQ12: Escalabilidad. Se debe poder añadir más elementos al sistema de gestión de red en caso de que sea necesario.

3. Siglas y Abreviaturas

• IEEE: Institute of Electrical and Electronic Engineers ó Instituto de Ingenieros Eléctricos y Electrónicos.

• ERS: Especificación de Requisitos Software.

• SNMP: Protocolo simple de administración de red

4. Referencias

Systems and software engineering — Life cycle processes — Requirements engineering. ISO/IEC/IEEE 29148.

ANEXO C. Características generales de las herramientas de gestión

- **MRTG (Multi Router Transfer Grapher).**

Es un software que supervisa en tiempo real, una gran cantidad de dispositivos, servicios y aplicaciones, principalmente ruteadores y switchs (Oetiker, 2017). También se pueden implementar otras funcionalidades utilizando las tablas MIBS de los diferentes equipos y el protocolo SNMP. Está escrito en Perl y funciona tanto en Linux como en Windows, la aplicación puede generar páginas HTML con los gráficos como figuras GIF.

- **NFSEN**

Es una interfaz gráfica basada en web, para las herramientas Netflow de Cisco y Nfdump (colector de datos de flujos). Sus prestaciones principales son:

- Muestra datos de flujo de red: flujos, paquetes y bytes utilizando RRD (base de datos Round Robin).
- Fácil navegación a través de los datos de netflow.
- Procesamiento de datos de netflow, dentro del lapso de tiempo especificado.
- Crea historial, así como perfiles continuos.
- Establece alertas, en función de diversas condiciones.
- Escribe sus propios complementos para procesar datos de netflow en un intervalo regular (Haag, s/f).

- **NFSight**

Brinda una solución flexible y práctica para visualizar la actividad de la red, y ofrece de manera rápida y gráfica puntos de vista sobre el estado de los activos de ésta, además construye flujos bidireccionales y los utiliza para la detección e identificación de actividad cliente/servidor, así como para la detección de intrusos.

- **SSHCure**

Muestra procesos de reconocimientos hechos a la red en busca de servicios SSH abiertos, en períodos previos de 24 horas o más.

- **Webacula**

Es la herramienta que facilita la gestión y empleo de los resguardos de Bacula a través de una interface web.

- **SmokePing**

Es una herramienta que realiza un registro histórico de los tiempos de latencia en una red. Cuenta con un sistema de alerta y una ventana gráfica en tiempo real con mediciones de retraso y pérdida de paquetes. Además, define rangos estadísticos para generar alarmas enviadas por correo electrónico. (Oetiker, 2017).

- **LibreNMS**

Software basado en el uso del protocolo SNMP, diseñado para descubrir la red y chequear el hardware de los diferentes dispositivos que la forman. Derivado de Observium y escrito en PHP como una aplicación de Web. No solo brinda apoyo a un gran rango de fabricantes de hardware (Cisco, Linux, FreeBSD, Juniper, rocade, Foundry, HP y muchos más), sino también a una enorme variedad de dispositivos: CPU, memoria, sistemas de almacenamiento, tráfico de interfaces, estadísticas de paquetes y errores muy detallados.

- **Rancid**

Rancid se encarga de mantener un archivo histórico de los cambios en la configuración y otros componentes de los equipos (Cisco, HP, Juniper, Foundry, etc.). Funciona con enrutadores y conmutadores (Switchs) mediante la automatización de la recolección y

resguardo de los archivos de configuraciones. Entre las principales funciones de Rancid, se destacan tanto el resguardo de las configuraciones de algunos equipos de hardware, como las auditorías de los usuarios que accedieron e hicieron cambios en éstos.

- **AlienVault OSSIM.**

Se trata de una colección de software bajo la licencia GPL, agrupadas con el objetivo de ofrecer una herramienta que ayude al manejo de eventos de seguridad mediante un motor de correlación y una colección detallada de aplicaciones útiles al administrador para tener una vista de todos los aspectos relativos a la seguridad en su infraestructura. OSSIM se ha diseñado para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y vulnerabilidades. Entre las aplicaciones más conocidas que lo forman, podrían mencionarse Arpwatch, Pads, para la detección de anomalías en servicios, el Openvas para detectar de intrusos utilizando un escáner de vulnerabilidades, el Snort o Suricata para los eventos de la red, entre otros (ATT Cybersecurity, 2022).

- **Sendmail analyzer**

Software empleado para monitorear el funcionamiento de sistemas de correos basados en sendmail o postfix y el tráfico de correos generado por éstos. Es libre y está programado para procesar archivos de registros de Postfix o Sendmail y generar, en tiempo real, estadísticas dinámicas en HTML con salida gráfica.

ANEXO D. Encuesta

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

Encuesta dirigida al Personal de la Empresa JassaTelecom

El objetivo de esta encuesta es el de realizar el levantamiento de información de la situación actual y requerimientos técnicos de la red de telecomunicaciones, aplicando conceptos de buenas prácticas e involucrando a todas las áreas de gestión de servicios, siguiendo los lineamientos de ITIL, para que contribuya al desarrollo de los objetivos establecidos en el proyecto denominado "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".

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

Nombre: _____

Fecha: _____

Área en la que se desempeña: _____

#	Procesos de gestión (relacionados)	Preguntas	S SI	N NO	TAL VEZ
11.		¿Se encuentra claramente definida la Gestión de Servicio en el Departamento de TI?			
2.		¿Tienen funciones y procesos claramente definidos a través del ciclo de vida?			
33.		¿Dentro del área de TI, el objetivo principal de un proceso es resolver la necesidad del usuario?			
4	Gestión Financiera de servicios de TI	¿Se encuentra definido el proceso de Gestión financiera para servicios de TI?			
51.		¿Se encuentran definidos los pasos del proceso, las interfaces con otros procesos y funciones internas de la organización, los roles y las responsabilidades			
62.		¿Se identifican y evalúan los procedimientos que influyen sobre la elaboración del presupuesto?			
7	Gestión del nivel del Servicio	¿Está establecido el proceso de gestión del nivel de servicio (SLM)?			
81.		¿Se encuentran definidos los pasos del proceso, las interfaces con otros procesos y funciones dentro de la organización, los roles y las responsabilidades?			
22.		¿Se tiene una completa visión y control de los servicios que se prestan? (Definición, documentación, acuerdo, seguimiento (Service Level Agreement - SLA), medición y revisión de los servicios y sus respectivos acuerdos con el cliente)			
13.		¿Proporciona SLM un único punto de contacto tanto para los clientes como para la			

		administración de la organización para todos los problemas relacionados con el nivel de servicio?			
14.		¿Se producen requisitos de nivel de servicio para todos los servicios?			
15.		¿Se supervisa el rendimiento del servicio según el SLA?			
16.		¿La medición y mejora de la satisfacción del cliente se realiza, documenta y se definen medidas de mejora con regularidad?			
1	Gestión de la Capacidad	¿Está establecido el proceso de Gestión de la capacidad?			
11.		¿Está implementada la gestión de la capacidad del servicio?			
12.		¿Se encuentran definidos los pasos del proceso, las interfaces con otros procesos y funciones dentro de la organización, los roles y las responsabilidades?			
13.		¿Se crea y mantiene el plan de capacidad?			
14.		¿El personal de Gestión de la Capacidad evalúa, identifica y acuerda los requisitos de capacidad y desempeño con el cliente?			
55.		¿Existen actividades iterativas (medición, análisis, ajuste e implementación) con responsabilidades definidas?			
2	Gestión de la disponibilidad	¿Está establecido el proceso de Gestión de la disponibilidad?			
21.		¿Se encuentran definidos los pasos del proceso, las interfaces con otros procesos y funciones dentro de la organización, los roles y las responsabilidades?			
22.		¿Se produce y mantiene un plan de disponibilidad?			
23.		¿Se definen la disponibilidad, la confiabilidad, la capacidad de mantenimiento,			

		la capacidad de servicio y la función comercial vital?			
24.		¿Se realiza el seguimiento, la medición, el análisis, la generación de informes y la revisión de la disponibilidad de componentes y servicios?			
25.		¿La gestión de la disponibilidad está involucrada en la planificación y el diseño de servicios nuevos o modificados?			
2	Gestión de la Seguridad de la Información	¿Existen políticas de seguridad de la información?			
21.		¿Están definidos y documentados los requisitos de seguridad de la información?			
22.		¿Existe la gestión de riesgos?			
23.		¿Están identificados y documentados los controles de seguridad de la información?			
34.		¿Se definen los roles y responsabilidades a lo largo del proceso?			
3	Gestión del cambio	¿Está establecido el proceso de Gestión del Cambio			
31.		¿Se definen los pasos del proceso, las interfaces con otros procesos y funciones dentro de la organización, los roles y las responsabilidades?			
32.		¿Existe un modelo de autorización para diferentes tipos de cambios?			
33.		¿Está definido el cumplimiento de los requisitos reglamentarios?			
34.		¿Existe una Junta Asesora de Cambios?			
3	Activos de Servicio y Gestión de la configuración	¿Está establecido el proceso de Gestión de la configuración y los activos del servicio (SACM)			
31.		¿Se definen los pasos del proceso, las interfaces con otros procesos y funciones dentro de la organización, los roles y las			

		responsabilidades?			
32.		¿Se produce y mantiene el plan SACM?			
33.		¿Existe un sistema de gestión de la configuración (CMS)?			
44.		¿Se identifican, etiquetan (cuando es posible) los elementos de configuración (CI) y se identifican y documentan los atributos y las relaciones de los CI?			
45.		¿Se documentan los estados de los CI en caso de que se produzcan cambios en los CI a lo largo de su ciclo de vida?			
4	Gestión de liberación y despliegue	¿Está establecido el proceso de Gestión de lanzamiento y despliegue (RDM)?			
41.		¿Se definen los pasos del proceso, las interfaces con otros procesos y funciones dentro de la organización, los roles y las responsabilidades?			
42.		¿Existen planes de RDM para las versiones y se acuerdan con el cliente para cada servicio o componente de servicio nuevo o modificado?			
43.		¿Se prueban los paquetes de lanzamiento?			
44.		¿Se produce una política de liberación para cada cliente?			
45.		¿Se gestiona y documenta la compilación y prueba de las versiones?			
46.		¿Se planifica, gestiona y verifica la implementación de las versiones?			
4	Operación del servicio	¿Se ha definido en el departamento de TI propósitos, metas y objetivos de la Gestión de Incidentes?			
51.		¿Se establecen y se llevan a cabo políticas, principios, conceptos básicos de la gestión de incidentes?			
52.		¿Existen un catálogo de incidencias?			

53.		¿Se lleva un registro de todos los incidentes?			
54.		¿Existe la categorización de incidentes?			
55.		¿Existe una matriz de priorización de incidentes y se priorizan los incidentes de acuerdo con la matriz?			
56.		¿Existen procedimientos de escalamiento funcional y jerárquico?			
57.		¿Existen limitaciones de tiempo para la investigación y el diagnóstico de incidentes (tiempo de resolución acordado)?			
58.		¿Se actualiza el registro de incidentes a medida que avanza hacia la resolución?			
59.		¿Existen pautas para la reapertura de incidentes?			
5	**Manejo de Problemas**	¿Se ha definido propósitos, metas y objetivos del manejo de problemas en el departamento de TI?			
61.		¿Se establecen y se llevan a cabo políticas, principios, conceptos básicos del manejo de problemas?			
62.		¿Se identifican, documentan y comunican las fuentes del problema?			
63.		¿Se registran todos los problemas?			
64.		¿Existe la categorización de problemas?			
65.		¿Existe una matriz de priorización de problemas y se priorizan los problemas de acuerdo con la matriz de prioridades?			
66.		¿Está definida la responsabilidad de garantizar que se lleve a cabo el análisis de la causa raíz?			
67.		¿Existen procedimientos de escalada?			
68.		¿Se gestiona la resolución y el cierre del problema, es decir, el procedimiento de escalamiento (en caso de que se infrinja el			

		Tiempo de resolución objetivo) así como la responsabilidad del cierre del problema?			
69.		¿Existe un historial de problemas? ¿Se actualiza el registro de problemas a medida que avanza hacia la resolución?			

Realizado por

Lila Hermosa

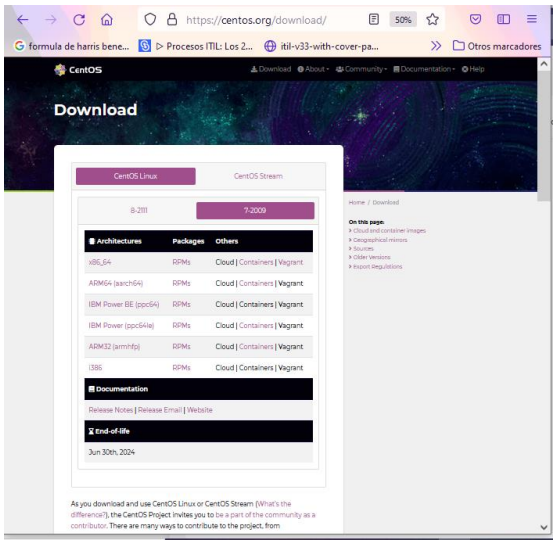
~~Revisado y Aprobado por~~

Msc. Fabián Cuzme Rodríguez

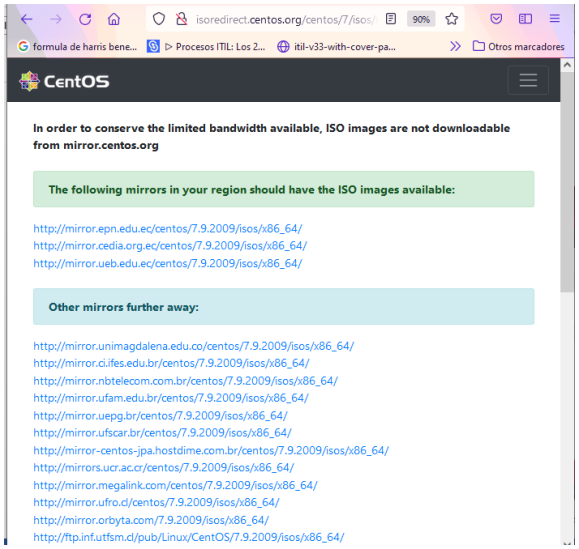
Enlace al formulario de google form: https://forms.gle/g8V8MSgg1T9YXc6q7

ANEXO E. Instalación Centos 7 en MVware ESXi

- Para ello ingresamos a la página https://centos.org

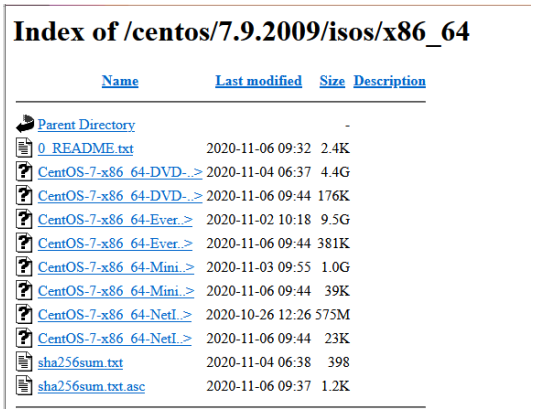


- Seleccionar el instalador acorde a nuestro sistema operativo



- Muestra la página en donde se encuentran los sistemas espejo, clic en el enlace que nos lleva a los instaladores de CentOS 7 y procedemos a realizar la descarga.

Figura E 1. Enlace de descarga CentOS 7



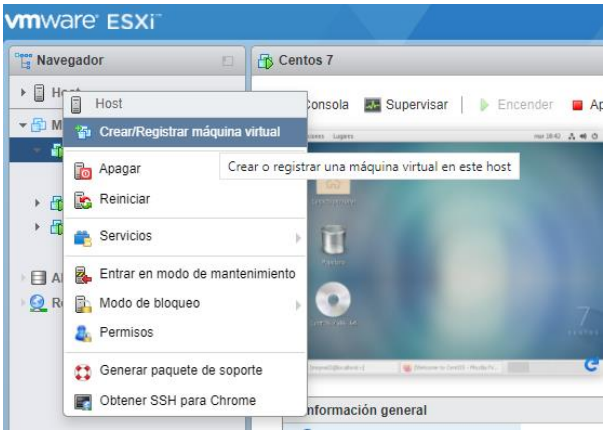
Index of /centos/7.9.2009/isos/x86_64

Name	Last modified	Size	Description
Parent Directory		-	
0_README.txt	2020-11-06 09:32	2.4K	
CentOS-7-x86_64-DVD-..>	2020-11-04 06:37	4.4G	
CentOS-7-x86_64-DVD-..>	2020-11-06 09:44	176K	
CentOS-7-x86_64-Ever..>	2020-11-02 10:18	9.5G	
CentOS-7-x86_64-Ever..>	2020-11-06 09:44	381K	
CentOS-7-x86_64-Mini..>	2020-11-03 09:55	1.0G	
CentOS-7-x86_64-Mini..>	2020-11-06 09:44	39K	
CentOS-7-x86_64-NetI..>	2020-10-26 12:26	575M	
CentOS-7-x86_64-NetI..>	2020-11-06 09:44	23K	
sha256sum.txt	2020-11-04 06:38	398	
sha256sum.txt.asc	2020-11-06 09:37	1.2K	

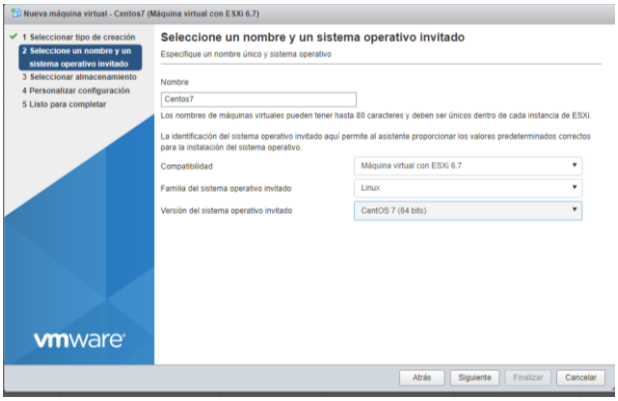
Fuente: Captura de CentOS

Para la creación de máquina Virtual en VMware ESXi.

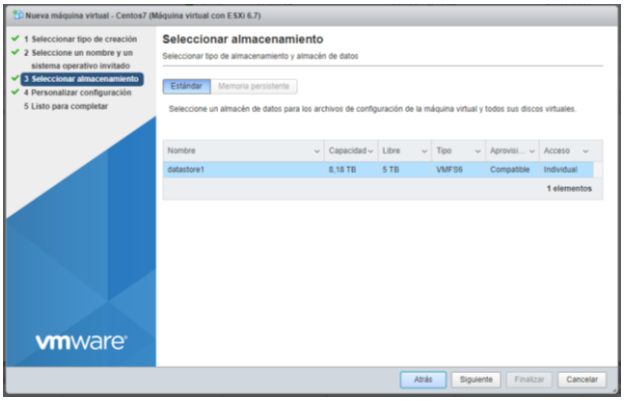
- Dar clic en Crear/Registrar máquina virtual



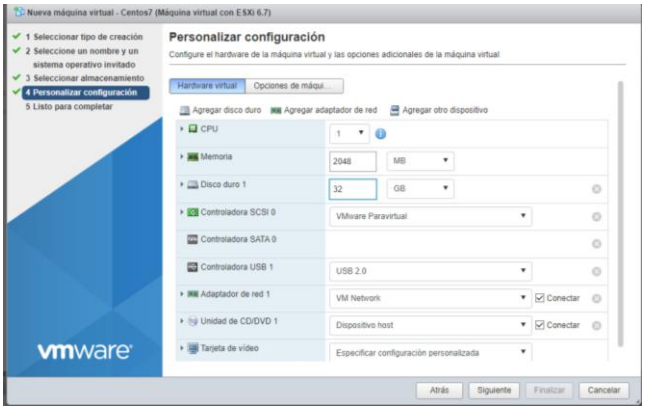
- Seleccionar un nombre y un sistema operativo invitado



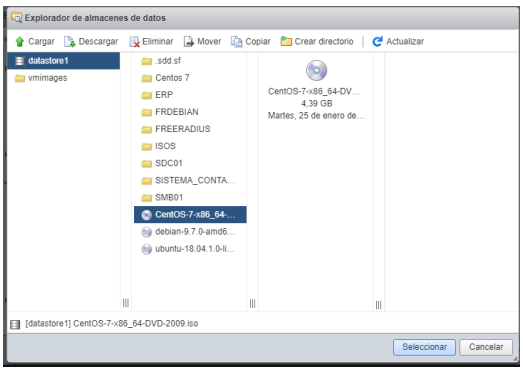
- Asignar el tamaño de la memoria



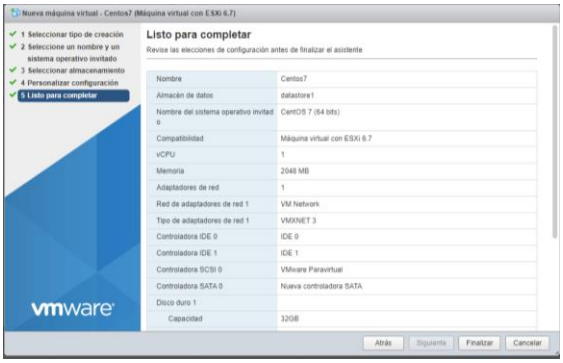
- Personalizar configuración, asignar tamaño de memoria, archivo ISO del almacén de datos, clic en siguiente.



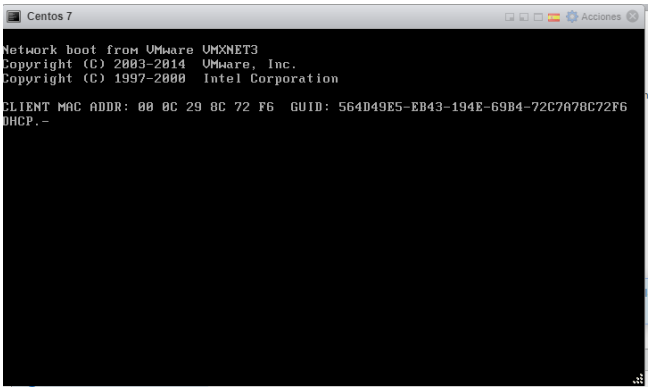
- Seleccionar la carpeta en donde se encuentra el instalador, damos clic en crear.



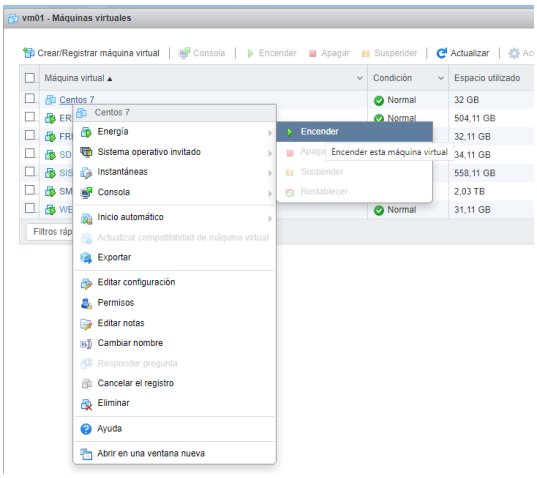
Una vez guardada la configuración surge la siguiente pantalla con los datos de la máquina creada, seleccionar finalizar.



- Una vez creada la máquina, el siguiente paso es ejecutar el instalador de CentOS 7.
- Para esto ingresar en la opción sistema y procedemos a realizar la instalación por defecto y finalizamos.



Una vez terminada la instalación de la máquina virtual procedemos a encender y configurar



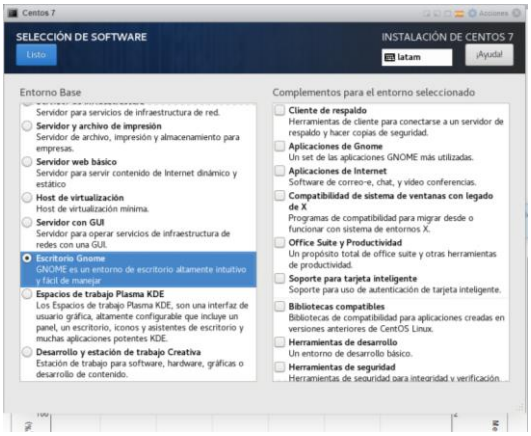
- Aparece la pantalla de inicio de CentOS 7

  Figura E 2. Pantalla de inicio de CentOS 7

Nota: Captura de CentOS

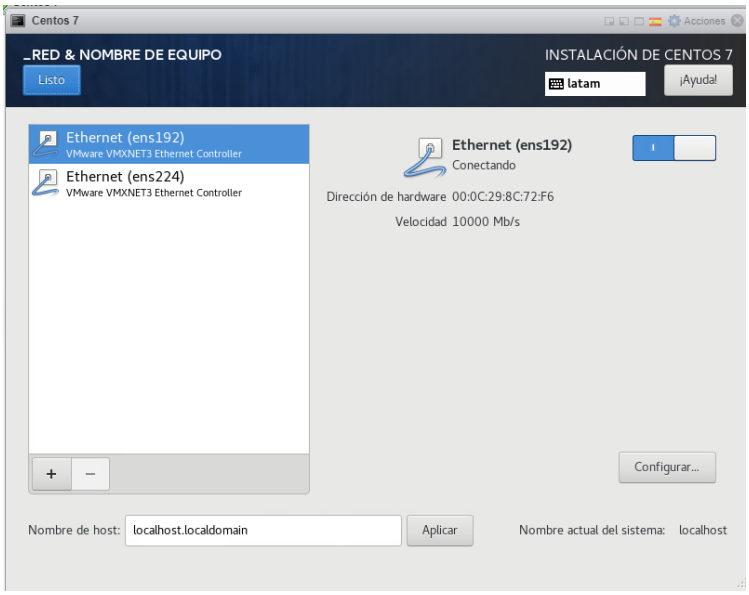
- Una vez instalado el sistema operativo procedemos a configurar
- Elegir el idioma.

- Configurar la fecha y hora
- Seleccionar el software, en este caso Gnome ya que es un entorno amigable y que permite trabajar con gráficas.



- Elegir el disco en que va a ser instalado

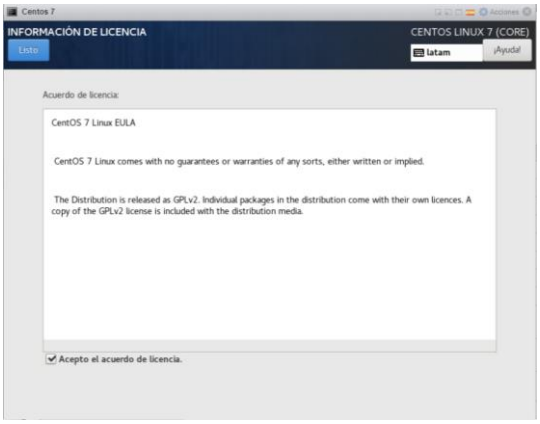
- Configurar la red, llenar los campos principales, aplicar los cambios y encender.



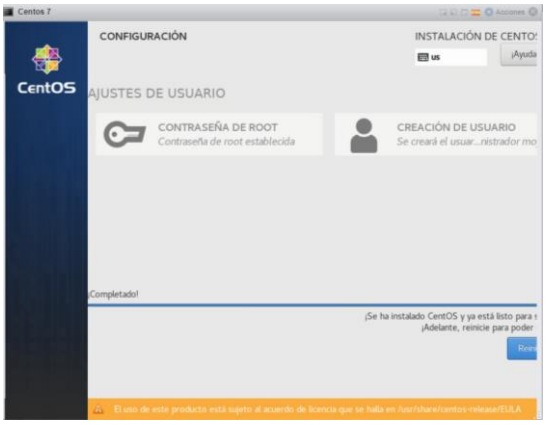
- Se presenta la ventana de Resumen de Instalación en la que se puede configurar según las necesidades del sistema a utilizar, dar clic en Empezar instalación.

Una vez iniciada la instalación se crea el usuario administrador

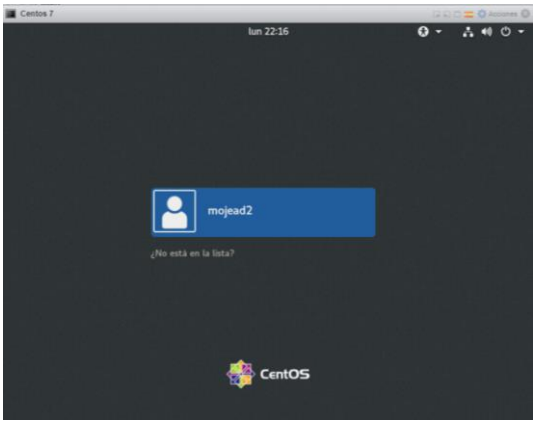
- Aceptar acuerdos de licencia



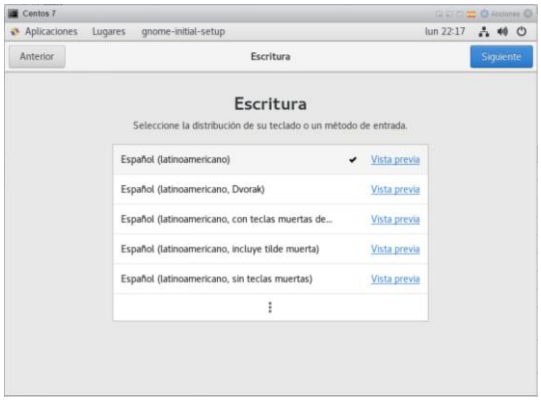
- Se anuncia el fin del proceso, hacer clic en reiniciar el sistema.



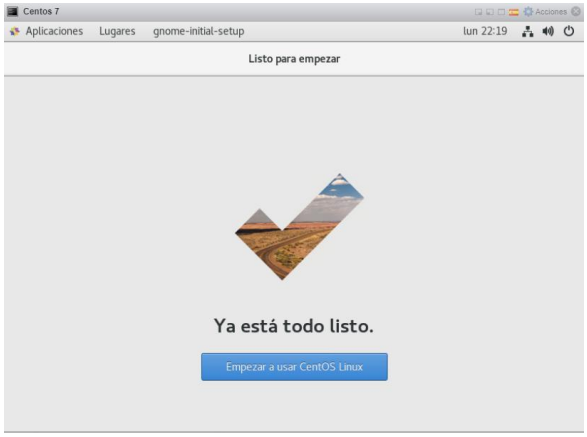
Una vez realizado este proceso inicia la pantalla de Centos 7 con el usuario creado anteriormente



- Una vez iniciada la sesión configurar Escritura, privacidad, clic en siguiente y está listo el sistema para iniciar



Para finalizar con la configuración hacer clic en Empezar a usar CentOS Linux.



ANEXO F. Instalación de Nagios en Centos 7

Emplearemos una máquina que funciona como servidor (mojead2) que se monitorizará a sí misma y a las máquinas remotas que configuremos, donde instalaremos:

- Nagios Core.
- Los plugins de Nagios.
- El plugin NRPE.

Y por otro lado tendremos una máquina que monitorizaremos remotamente (admin2), en la que instalaremos:

- Los plugins de Nagios.
- El servicio Nagios NRPE.

Entre los archivos de Nagios más importantes se encuentran los siguientes:

- **Archivo de configuración principal.** - Este archivo (nagios.cfg) contiene una serie de directivas que afectan el funcionamiento del sistema de monitoreo de Nagios. Este archivo de configuración es leído tanto por el agente de Nagios como por los CGI.
- **Archivos de recursos.** - Sirven para almacenar macros definidas por el administrador. El objetivo principal de tener archivos de recursos es usarlos para almacenar información de configuración confidencial, como contraseñas, sin ponerlos a disposición de los CGI.
- **Archivos de definición de objetos.** - Dentro de estos archivos se define todo lo que se debe monitorear y cómo se debe monitorear cada uno de los dispositivos administrados. El archivo cfg, que se encuentra dentro del archivo de configuración principal, le permite especificar uno o más archivos de definición de objetos.
    - **Objectos.** - Se utilizan para definir hosts, servicios, grupos de host, contactos, comandos, etc., como se detalla a continuación:

- **Host.** - Los hosts son dispositivos físicos de red (por ejemplo, servidores y enrutadores) que tienen algún tipo de dirección (IP o MAC). Tienen uno o más servicios asociados con ellos.
- **Grupos de Hosts.** - Estos son grupos de uno o más hosts que pueden facilitar la visualización del estado de ciertos dispositivos conectados entre sí a través de la interfaz web de Nagios y así simplificar la configuración.
- **Comandos.** - Estos comandos le indican a Nagios qué complementos debe ejecutar para realizar las siguientes tareas: comprobaciones de host y servicio, notificaciones y eventos.
- **Servicios.** - Los servicios están relacionados con el host, y estos pueden ser atributos (carga de CPU, uso de disco, etc).
- **Grupo de Servicios.** - Los grupos de host, por otro lado, simplifican la configuración y facilitan la visualización del estado de los servicios relacionados en la interfaz web de Nagios.
- **Contactos.** - Son las personas que serán notificadas si ocurre algo inusual en los dispositivos de la red y tiene las siguientes características:
  - Los contactos deben contar con uno o más medios de comunicación, como los generados por el software (mensajes de texto a teléfonos móviles, correo electrónico, etc.).
  - Los contactos reciben notificaciones sobre las máquinas y servicios de los que son responsables.
- **Grupos de Contacto.** - Son grupos de uno o más contactos.

- **Períodos de tiempo.** - Se utiliza para determinar cuándo se pueden monitorear hosts y servicios y cuándo los contactos pueden recibir notificaciones.

    - **Plantillas. -** Estos son archivos que le permiten simplificar la configuración de dispositivos y servicios de red.

- **Archivos de configuración CGI. -** Archivos que permiten al administrador recopilar datos de aplicaciones ejecutadas por Nagios y mostrarlos en su interfaz web.

Directorios principales de Nagios

Las siguientes secciones describen los subdirectorios en /usr/local/nagios:

- **bin. -** Este directorio contiene el ejecutable de Nagios, que es el programa que se ejecuta en segundo plano.
- **etc.-** Este directorio almacena toda la configuración para el correcto funcionamiento de Nagios, es decir, los archivos que especifican los hosts y servicios a monitorear, los comandos a usar para monitorear, los intervalos de tiempo para verificar y los contactos de notificación.
- **libexec. -** Este directorio almacena todos los complementos ejecutables que se utilizarán para ejecutar los servicios. Estos pueden ser archivos binarios o scripts escritos en lenguajes como C, PHP, Bash, Perl y otros.
- **sbin. -** Este directorio contiene archivos CGI ejecutables que permiten solicitar información a un programa, los mismos que se encuentran en ejecución en un servidor web. Estos archivos le permiten ver la interfaz web de Nagios.
- **share. -** Este directorio almacena información que se mostrará en la interfaz web, como logotipos, imágenes, páginas de destino y documentación de ayuda.
- **var. -** Dentro de este directorio se tiene un registro de toda la información recopilada como resultado del monitoreo, tales como estadísticas de verificación, logs e información recopilada.

1. Prerrequisitos

Para administrar Nagios vía web, ejecutamos el siguiente comando:

 # yum install -y wget httpd php gcc glibc glibc-common gd-devel make net-snmp unzip

Instalación de plugins de Nagios en Centos 7

Instalación de plugins tanto en el servidor Nagios Core como en las máquinas remotas:

 # yum install -y epel-release

Actualizar las listas de paquetes:

 # yum update

Paquete completo de plugins de Nagios:

 # yum install -y nagios-plugins-all

Una vez descargado e instalado el paquete y sus dependencias, tendremos un nuevo directorio ***/usr/lib64/nagios/plugins/*** en el que se ubicarán todos los comandos ejecutables de los complementos.

Instalación de Nagios Core en Centos 7

Instalación del paquete Nagios en la máquina que actuará como servidor:

 # yum install -y nagios

Activación del servicio nagios y arranque con el inicio de Centos 7:

~$ sudo systemctl enable nagios

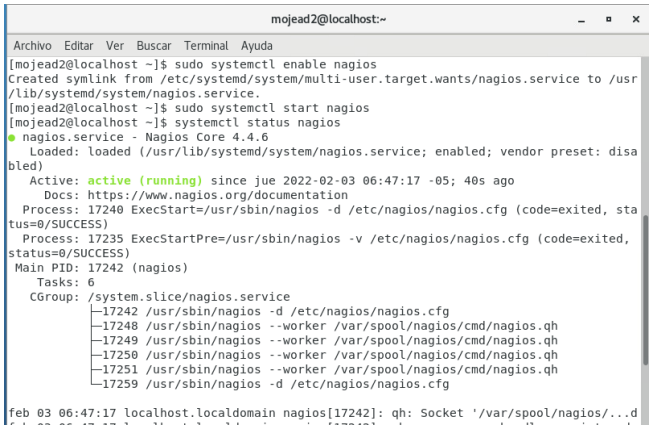
Iniciar el servicio por vez primera

~$ sudo systemctl start nagios

Podemos comprobar el estado del servicio nagios en cualquier momento con el comando *~$ systemctl status Nagios*

Figura F 1

Estado del servicio de Nagios



Nota: Captura de Centos 7

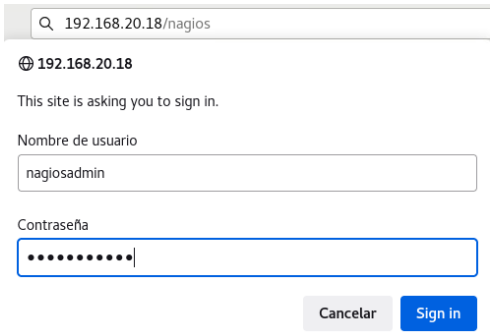
Acceso a Nagios Core en Centos 7

Para acceder a Nagios Core desde el navegador añadimos el alias /nagios a la dirección IP o dominio del servidor, por lo que la URL http://192.168.20.18/nagios será la que utilicemos.

Se nos presentará una ventana de inicio de sesión:

Figura F 2

Pantalla inicio de sesión Nagios Core



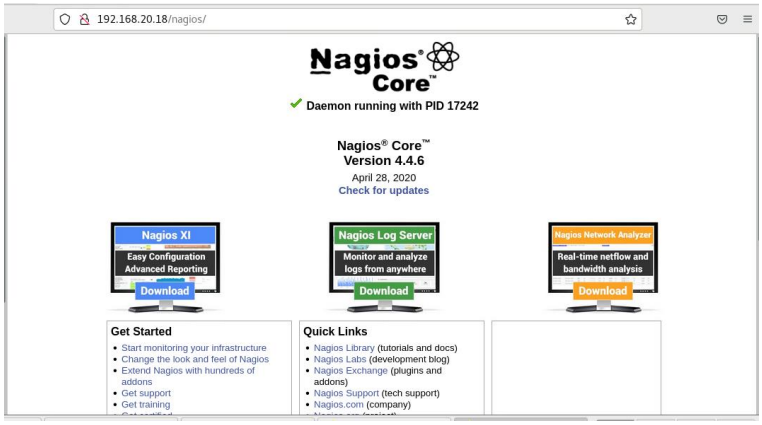
Nota: Captura de Nagios

El usuario por defecto es *nagiosadmin* y su contraseña es también *nagiosadmin*.

Accederemos a la página principal de Nagios Core:

Figura F 3

Pantalla principal de Nagios Core

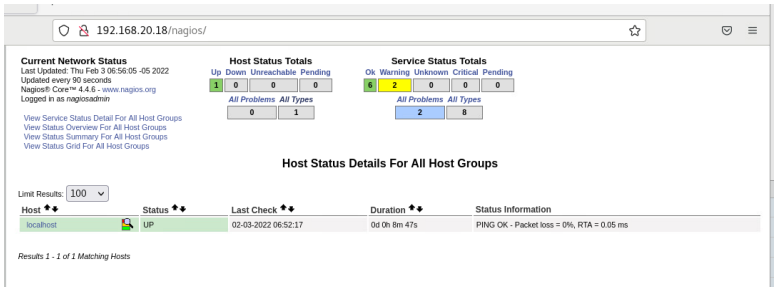


Nota: Captura de Nagios

En la sección «*Hosts*», se observa la máquina local configurada y la monitorización activa:

Figura F 4

Sección Hosts de Nagios Core

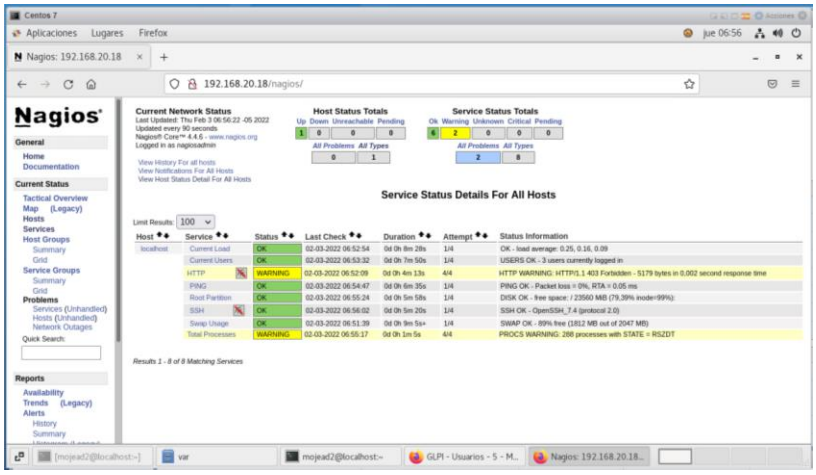


Nota: Captura de Nagios

En la sección «*Services*», se encuentra una vista más detallada, de los servicios monitorizados (en este caso sólo aparece la máquina local) y el estado de cada uno de ellos:

Figura F 5

Sección Services de Nagios Core



Nota: Captura de Nagios

Instalar Nagios NRPE en máquina remota Centos 7

Instalar los plugins de Nagios en la máquina remota siguiendo los pasos mencionados anteriormente. Ahora procedemos a instalar y configurar el servicio Nagios NRPE, que recibirá solicitudes de datos del servidor Nagios Core y este reaccionará con los resultados.

Ingresar en consola el siguiente comando para instalar el paquete nrpe:

~$ sudo yum install -y nrpe

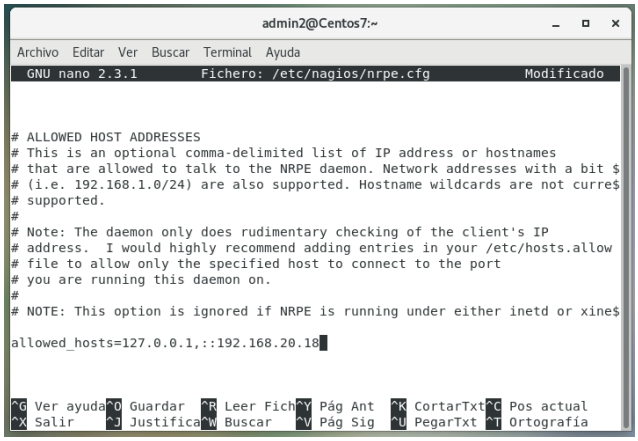
En CentOS 7, se crea un nuevo servicio llamado nrpe.service o nrpe. Para activarlo primero debemos hacer algunos ajustes en su archivo de configuración usando el comando.

~$ sudo nano /etc/nagios/nrpe.cfg

Buscamos la directiva *allowed_hosts*: y añadimos a la lista la dirección del servidor Nagios Core que conectará con el servicio NRPE

Figura F 6

Archivo de configuración nrpe.cfg de Nagios máquina remota



Nota: Captura de Centos

Después de completar la configuración, ahora podemos activar e iniciar el servicio NRPE con el siguiente comando:

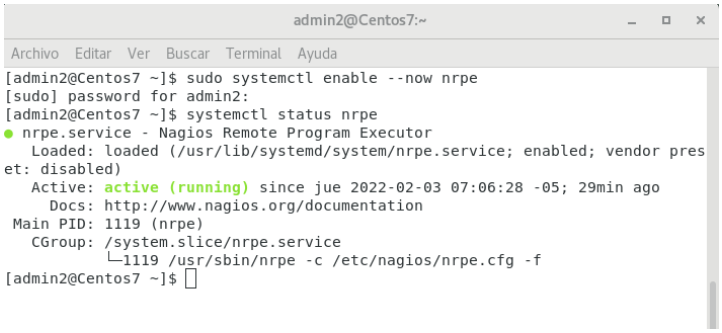
~$ sudo systemctl enable --now nrpe

Para verificar el estado del servicio Nagios NRPE, podemos usar el comando:

systemctl status nrpe

Figura F 7

Estado del servicio Nagios NRPE



Nota: Captura de Centos

Configuración del firewall en Centos 7 para Nagios NRPE

El firewall de CentOS 7 suele estar activado de forma predeterminada, lo que bloqueará las conexiones al servicio NRPE. Agregamos una regla que permite conexiones:

~$ sudo firewall-cmd --permanent --add-service=nrpe

Recargar la configuración del firewall:

~$ sudo firewall-cmd –reload

El trabajo en la máquina remota ahora está completo.

Configuración de máquinas remotas en Nagios Core para CentOS 7

Instalar el paquete nagios-plugins-nrpe, que contiene el plugin NRPE y permite conectar el servidor Nagios con el servicio NRPE de las máquinas remotas, ejecutamos el siguiente comando:

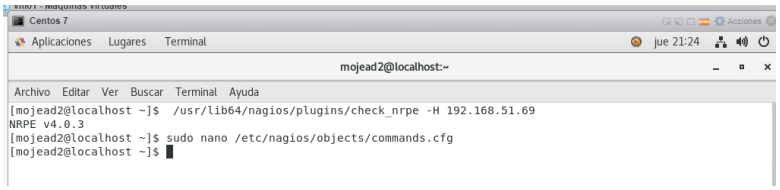
~$ sudo yum install -y nagios-plugins-nrpe

Podemos usar el complemento instalado directamente en consola para verificar la conectividad con la máquina remota configurada:

~$ /usr/lib64/nagios/plugins/check_nrpe -H 192.168.51.69

Figura F 8

Conectividad de máquina remota



Nota: Captura de Centos

Dado que la máquina CentOS 7 remota responde con la versión instalada del servicio NRPE, podemos verificar que la conectividad es correcta.

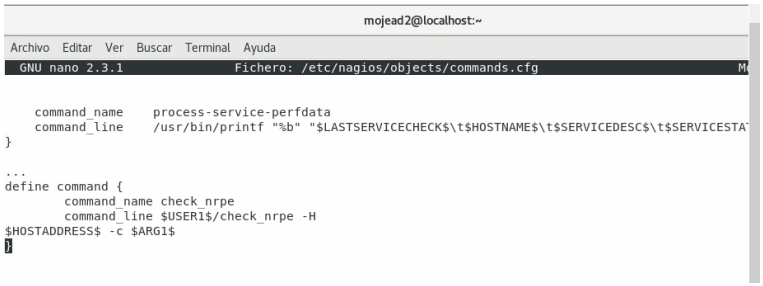
Ahora creamos un comando para habilitar este plugin en Nagios Core:

~$ sudo nano /etc/nagios/objects/commands.cfg

Definimos un nuevo comando al final del archivo que llamaremos check_nrpe.

Figura F 9

Definición de comando check_nrpe



Nota: Captura de Centos

Guardamos los cambios y cerramos el archivo.

Creamos la configuración de las máquinas remotas

Para permitir que Nagios Core cargue las configuraciones de las distintas máquinas, habilitaremos un directorio donde se almacenarán los archivos de configuración para cada máquina remota.

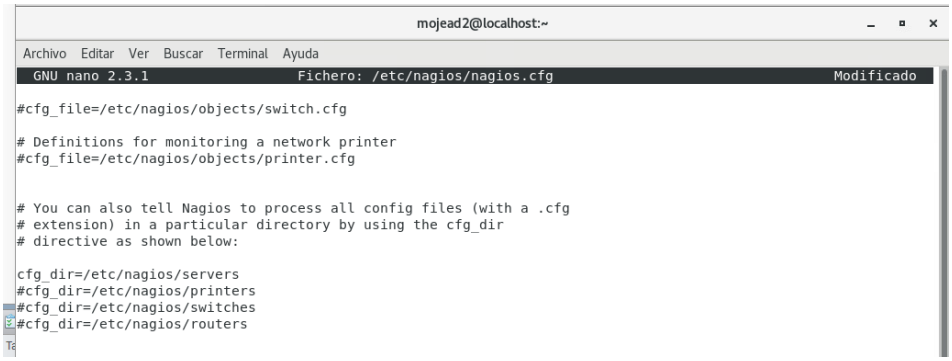
Editar el archivo principal de configuración de Nagios Core:

~$ sudo nano /etc/nagios/nagios.cfg

Buscar la siguiente línea *#cfg_dir=/etc/nagios/servers y e*liminar el carácter # inicial, con lo que se cargarán todas las configuraciones existentes en la ruta indicada:

Figura F 10

Archivo de configuración nagios.cfg



Nota: Captura de Centos

Guardamos los cambios y cerramos el archivo.

Creamos la ruta anterior, con el siguiente comando:

~$ sudo mkdir /etc/nagios/servers

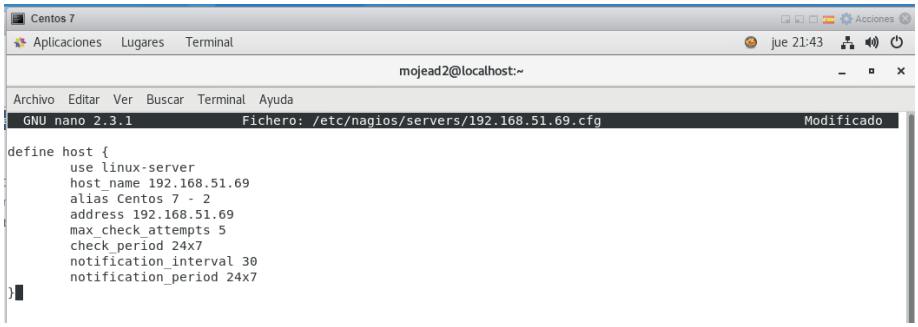
El archivo de configuración para la máquina remota que preparamos previamente se creará dentro de ese directorio:

~$ sudo nano /etc/nagios/servers/192.168.51.69.cfg

Añadimos los datos de la máquina:

Figura F 11

Archivo de configuración 192.168.51.69.cfg

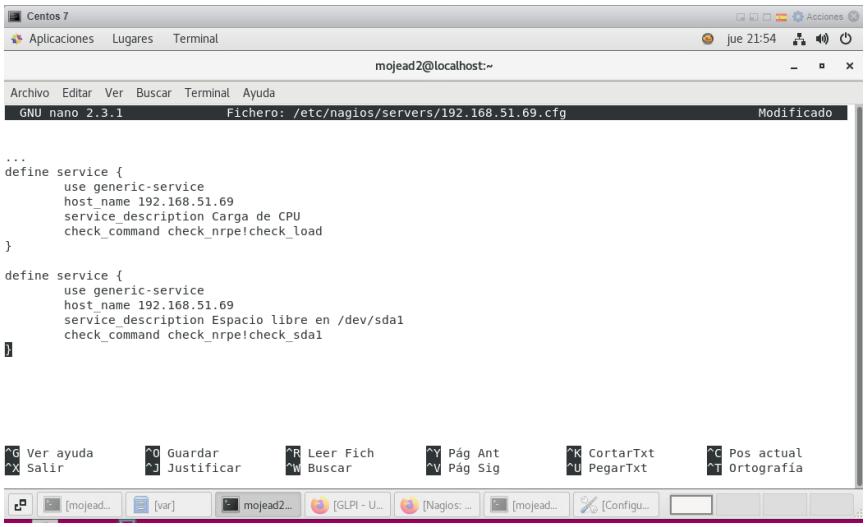


Nota: Captura Centos

A continuación, definimos algunos servicios, por ejemplo, la carga de CPU y el espacio libre en la partición principal:

Figura F 12

Creación de servicios



Nota: Captura de Centos

En la llamada al comando check_nrpe (comando que creamos antes) se le pasa como argumento un comando que debe estar definido como tal en la máquina remota.

Guardamos los cambios y cerramos el archivo.

Finalmente, recargamos la configuración del servicio Nagios para activar todos estos

cambios:

~$ sudo systemctl reload nagios

Abrimos la interfaz web de Nagios Core y en la sección «Hosts» ahora además de la máquina local aparecerá la nueva máquina remota recién configurada. Tras finalizar la

instalación de CentOS 7, actualizamos los paquetes que tenemos instalados, mediante el siguiente comando:

~$ sudo yum update

ANEXO G. Instalación de GLPI

Para la instalación de GLPI, es necesario contar con un entorno LAMP, este es un servidor web que ejecuta PHP a partir de la versión 7.4 y utiliza MariaDB/MySQL para bases de datos.

Instalación servidor web con PHP y bases de datos MariaDB/MySQL.

- **Configurar repositorios EPEL**

EPEL (Extra Packages for Enterprise Linux) contiene paquetes de software adicionales para el entorno empresarial. El repositorio de CentOS Extras contiene este paquete y viene activado por defecto. Para ello ejecutamos el siguiente comando:

~$ sudo yum -y install epel-release yum-utils

Configurar repositorios para PHP

Agregar el repositorio más reciente de PHP con el siguiente comando:

~$ sudo yum install -y http://rpms.remirepo.net/enterprise/remi-release-7.rpm

Existen varias versiones de PHP en el repositorio, por lo que podemos habilitar la versión estable que mejor se adapte a nuestras necesidades, por ejemplo, PHP 7.4, con el siguiente comando:

~$ sudo yum-config-manager --enable remi-php74

Configurar repositorios para MariaDB

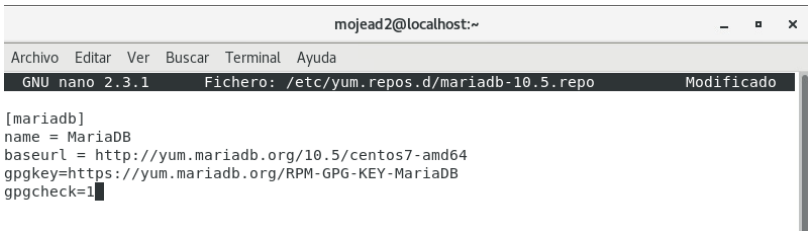
Para esto ejecutamos el comando:

~$ sudo nano /etc/yum.repos.d/mariadb-10.5.repo

Y añadimos el siguiente contenido:

Figura G 1

Archivo de repositorio MariaDB 10.5



Nota: Captura de Centos

Actualizar la información de los repositorios con el siguiente comando:

~$ sudo yum update -y

El sistema CentOS 7 ya está listo para comenzar la instalación y configuración del sistema LAMP.

Instalación servidor LAMP en CentOS 7

Para eso ejecutamos el siguiente comando:

~$ sudo yum -y install httpd mariadb-server php php-mysqlnd

Actualmente, se ha instalado todo el software necesario; sin embargo, se requerirán ajustes para que funcione.

Arranque de los servicios

Después de la instalación, los servicios web y de base de datos no se inician de forma predeterminada. Habilitamos los servicios para que arranquen automáticamente en cada inicio del sistema con el siguiente comando:

~$ sudo systemctl enable httpd mariadb

Debido a que los servicios no comenzarán como resultado de esto, los iniciaremos manualmente por esta vez, ejecutando el comando:

~$ sudo systemctl start httpd mariadb

Con el comando systemctl, los servicios se encuentran funcionando desde ahora y, además, arrancarán con cada inicio del sistema.

Ajustes del firewall

El firewall de CentOS 7 impide la conexión desde otros equipos mediante navegadores, para acceder al contenido web añadimos una excepción para el servicio HTTP:

~$ sudo firewall-cmd --permanent --zone=public --add-service=http

Otra para el servicio seguro HTTPS:

~$ sudo firewall-cmd --permanent --zone=public --add-service=https

Y finalmente recargamos la configuración del firewall para que hagan efecto los cambios:

~$ sudo firewall-cmd --reload

Ahora se puede acceder al servicio web desde otras máquinas mediante los protocolos HTTP y HTTPS.

Apache

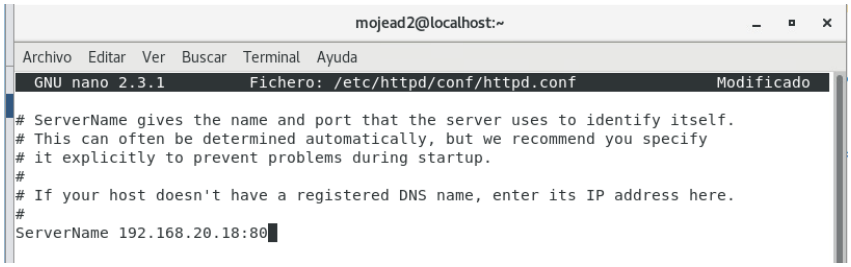
Debido a que el servidor no tiene un nombre por defecto, es posible que recibamos una alerta al inicio de cada servicio si no se ha configurado correctamente el nombre de la máquina CentOS 7. El archivo de configuración que cambiaremos para darle un nombre al servidor es el siguiente:

~$ sudo nano /etc/httpd/conf/httpd.conf

Buscar la directiva ServerName, que ahora está deshabilitada, eliminar el carácter # y asignar un valor (normalmente, la dirección IP del servidor, el nombre DNS, el nombre de dominio, etc.):

Figura G 2

Archivo de configuración httpd.conf



Nota: Captura de Centos

Actualizar la configuración del servidor web con el comando:

~$ sudo systemctl reload httpd

El directorio de archivo web está configurado de forma predeterminada en */var/www/html/*.

Servicio de base de datos

Ejecutamos el siguiente comando

~$ sudo mysql_secure_installation

Con este script conseguiremos:

- Crear una contraseña para el usuario raíz de MariaDB. La primera pregunta que plantea el script es la contraseña de root, que ahora está en blanco.
- Deshacerse de los usuarios anónimos
- El acceso remoto de MariaDB para el usuario raíz debe estar deshabilitado.
- Eliminar la base de datos de prueba.

El servicio de base de datos ahora está disponible para trabajar con él.

PHP

La configuración de PHP se realiza a través de los ajustes del archivo /etc/php.ini.

Lo básico a modificar en una nueva instalación sería:

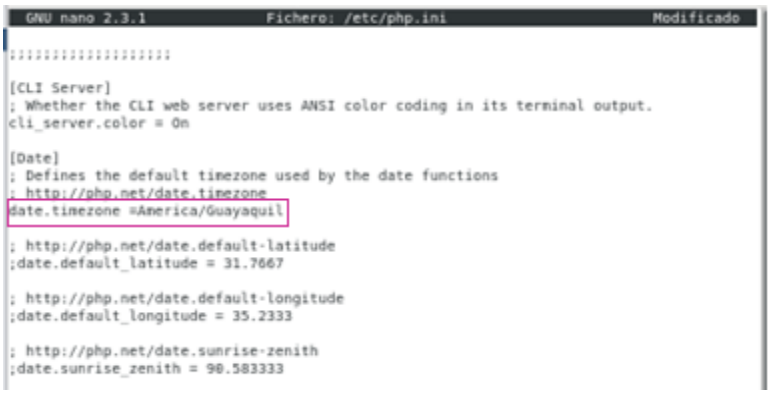
- Zona horaria del servidor
- Tratamiento de errores

En cuanto a los valores para el tratamiento de errores de PHP, en el propio archivo /etc/php.ini vienen como ejemplo los valores de desarrollo y de producción. Editar el archivo:

~$ sudo nano /etc/php.ini

Figura G 3

Archivo de configuración php.ini



Nota: Captura de Centos

Tras estos mínimos cambios, podemos guardar y cerrar php.ini. Recargar la configuración del servidor web tras cada cambio en la configuración de PHP con el comando:

~$ sudo systemctl reload httpd

Probar la pila LAMP en CentOS 7

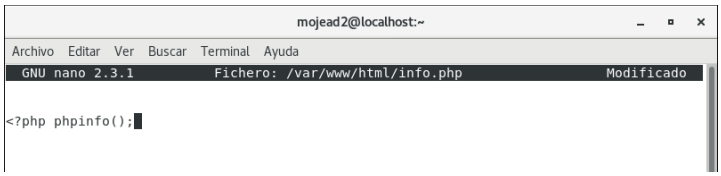
Crearemos un pequeño script en PHP accesible vía web:

~$ sudo nano /var/www/html/info.php

El contenido de este archivo será la siguiente línea:

Figura G 4

Archivo de configuración php.ini



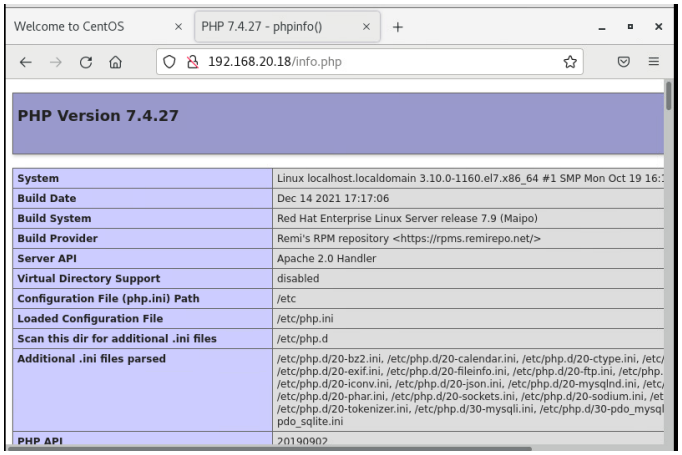
Nota: Captura de Centos

Accedemos desde el navegador, añadiendo la ruta /info.php a la dirección IP o dominio del servidor CentOS 7 en el que hemos alojado la pila LAMP.

La página que obtenemos nos anuncia la versión de PHP instalada y su configuración, extensiones disponibles, etc.

Figura G 5

Página de PHP instalada



Nota: Captura de PHP

En este momento ya contamos con los requerimientos para realizar la instalación de GLPI.

Actualizar las listas de paquetes con el siguiente comando

~$ sudo yum update

Ejecutamos el siguiente comando para instalar las herramientas y utilidades:

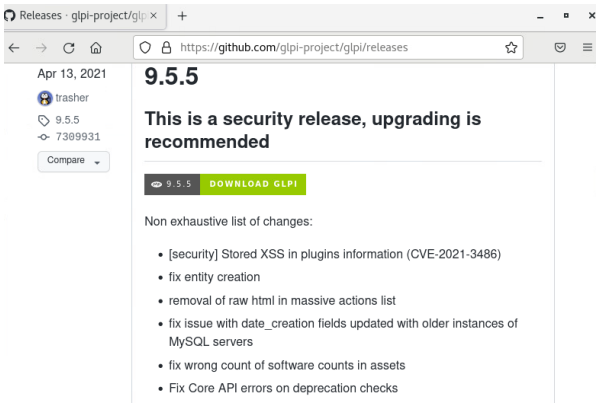
~$ sudo yum install -y policycoreutils-python wget

Descargar GLPI para CentOS 7

Descargar GLPI para CentOS 7 desde el sitio web del proyecto https://github.com/glpi-project/glpi/releases, donde obtendremos la versión más reciente:

Figura G 6

Sitio web proyecto github



Nota: Captura de glpi-project

Encontraremos los archivos .zip y .tar.gz para su descarga inmediata.

Copiar el enlace del paquete.tar.gz y descargar desde la consola con el siguiente comando:

~$ wget -q https://github.com/glpi-project/glpi/releases/download/9.5.5/glpi-9.5.5.tgz

Instalación de GLPI en CentOS 7

- **Directorio para GLPI**

Descomprimir el paquete descargado y colocar en la ubicación adecuada para la configuración del servidor web:

~$ sudo tar xf glpi-9.5.5.tgz -C /var/www/html

GLPI necesita escribir en algunos de los subdirectorios de su ruta de instalación, concederemos la propiedad de los mismos al usuario con el que corre el servicio web (Apache en CentOS 7):

~$ sudo chown -R apache: /var/www/html/glpi/

PHP

Ejecutaremos el siguiente comando:

~$ sudo yum install -y php-{gd,imap,intl,ldap,mbstring,opcache,pear-CAS,pecl-apcu,xmlrpc,pecl-zip}

Recargar la configuración del servicio PHP:

~$ sudo systemctl reload httpd

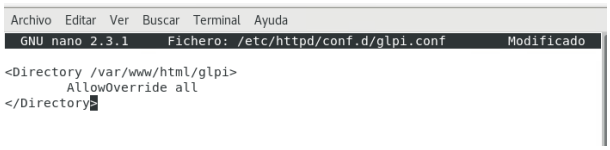
Servidor web

Crear una configuración para GLPI, mediante una directiva AllowOverride permitiremos la carga de archivos .htaccess en el directorio de GLPI con el comando:

~$ sudo nano /etc/httpd/conf.d/glpi.conf

Figura G 7

Archivo de configuración glpi.conf



Nota: Captura de Centos

Guardamos los cambios y cargamos la nueva configuración:

~$ sudo systemctl reload httpd

Configuración de SELinux

Crear un contexto de lectura/escritura del servicio web para los directorios en los que necesita escribir GLPI con el comando:

~$ sudo semanage fcontext -a -t httpd_sys_rw_content_t "/var/www/html/glpi(/.)?"*

Aplicaremos este nuevo contexto con restorecon:

~$ sudo restorecon -R /var/www/html/glpi/

Activar ciertos permisos para el servidor web, como la realización de peticiones de red con el siguiente comando:

~$ sudo setsebool -P httpd_can_network_connect on

Igualmente, para el acceso a bases de datos por red:

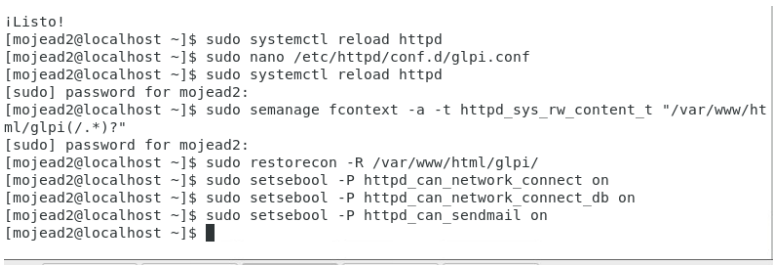
~$ sudo setsebool -P httpd_can_network_connect_db on

Y el envío de correo electrónico:

~$ sudo setsebool -P httpd_can_sendmail on

Figura G 8

Ventana de comandos, configuración SELinux



Nota: Captura de Centos

Base de datos

GLPI se apoya sobre el servicio de bases de datos de CentOS 7, concretamente MariaDB. Conectar al servicio el cliente de consola mysql y el usuario administrador que usemos habitualmente, ejecutamos el comando:

~$ mysql -u root –p

Crear una base de datos para GLPI:

> create database glpi charset utf8mb4 collate utf8mb4_unicode_ci;

En MariaDB crear el usuario para GLPI con la siguiente sentencia:

> create user glpi@localhost identified by 'glmojasa';

Dar permisos al usuario sobre la base de datos:

> grant all privileges on glpi. to glpi@localhost;*

Dar permiso sobre la tabla de nombres de zonas horarias de MySQL:

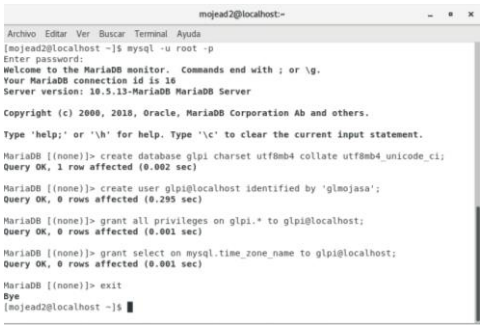
> grant select on mysql.time_zone_name to glpi@localhost;

Cerrar sesión:

> exit

Figura G 9

Ventana de comandos, Base de datos de GLPI



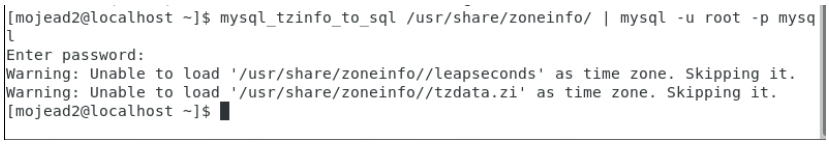
Nota: Captura de Centos

En ciertas ocasiones las tablas de zona horaria de MySQL no están cargadas por defecto, así que debemos cargarlas con ayuda de la herramienta *mysql_tzinfo_to_sql*:

~$ mysql_tzinfo_to_sql /usr/share/zoneinfo/ | mysql -u root -p mysql

Figura G 10

Ventana de comandos, Carga de tablas de zona horaria de MySQL



Nota: Captura de Centos

Instalación vía web

Acceder desde el navegador indicando la URL con la que está configurada la aplicación. Añadir la ruta /glpi a la dirección IP o dominio del servidor CentOS 7. Seleccionar el idioma del instalador, dar clic en OK.

Figura G 11

Instalador de GLPI vía web

Nota: Captura de GLPI

Aceptar acuerdos de licencia, presionar en continuar

Figura G 12

Acuerdos de licencia de GLPI

Nota: Captura de GLPI

En nuestro sistema CentOS 7, el instalador permite realizar una instalación nueva de GLPI o actualizar una instalación existente, en este caso damos clic en instalar

Figura G 13

Instalación de GLPI

Nota: Captura de GLPI

Antes de la instalación, muestra una larga lista de requisitos del sistema para verificación, dar clic en continuar:

Figura G 14

Comprobación de ítems instalados

Nota: Captura de GLPI

A continuación, llenar los campos de acceso al servicio de base de datos con las credenciales creadas anteriormente

Figura G 15

Parámetros de conexión de la base de datos de GLPI

Nota: Captura de GLPI

Indicar la base de datos glpi y continuar:

Figura G 16

Prueba de conexión a la Base de Datos

Nota: Captura de GLPI

En la siguiente pantalla seleccionar continuar

Figura G 17

Inicialización de la base de datos

Nota: Captura de GLPI

Tras la instalación, se da la opción de activar el servicio de envío de estadísticas de uso anónimo y completar una encuesta GLPI, dar clic en continuar:

Figura G 18

Pantalla de recolección de datos de Glpi

Nota: Captura de GLPI

El instalador también nos informa sobre la posibilidad de utilizar servicios de apoyo profesional y asignación de donaciones:

Figura G 19

Pantalla informativa de GLPI

Nota: Captura de GLPI

Una vez finalizada la instalación, informa de la existencia de varios usuarios y sus contraseñas por defecto, dar clic en utilizar GLPI.

Figura G 20

Pantalla de instalación finalizada

Nota: Captura de GLPI

Para acceder a la página de inicio de sesión, utilizar uno de los usuarios mencionados anteriormente, utilizando la contraseña por defecto.

Figura G 21

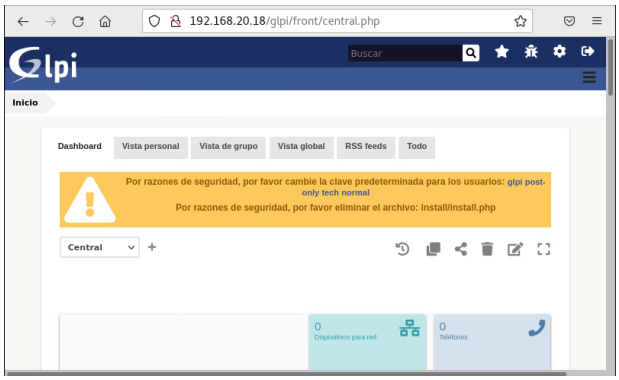
Pantalla de instalación finalizada

Nota: Captura de GLPI

La página principal de GLPI muestra una serie de alertas relacionadas con el instalador en línea y los usuarios predeterminados cuando se inicia la sesión por primera vez:

Figura G 22

Página principal de GLPI



Nota: Captura de GLPI

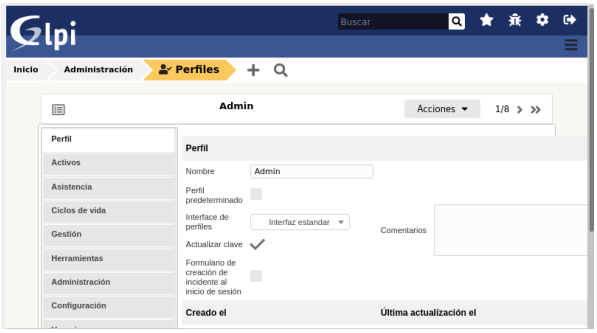
Para eliminar el archivo del instalador web, ejecutar el siguiente comando en consola:

~$ sudo rm /var/www/html/glpi/install/install.php

Para cambiar las contraseñas por defecto, acceder a la sección "Usuarios" del menú "Administración". Allí, se encuentra una lista de todos los usuarios activos.

Figura G 23

Perfiles de usuarios activos en GLPI



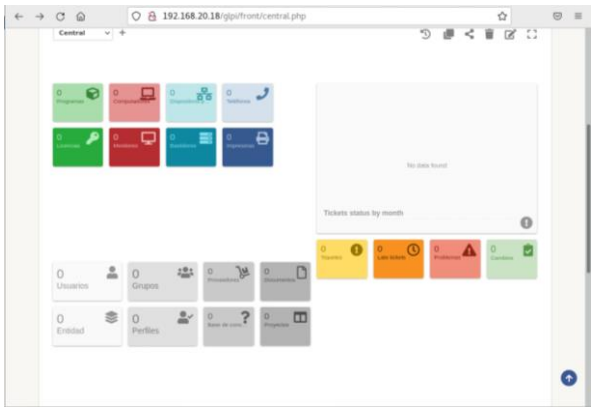
Nota: Captura de GLPI

Elegir el usuario cuyo perfil nos interesa y acceder a él, podemos cambiar la contraseña y cualquier otra información, incluido el nombre de usuario para el inicio de sesión. Las alertas al inicio de sesión desaparecerán después de realizar estos cambios.

Una vez realizados estos pasos tenemos la página principal de GLPI, lista para trabajar en la gestión de usuarios y equipos.

Figura G 24

Tablero principal de GLPI



Nota: Captura de GLPI

ANEXO H. Instalación OCS Inventory Server

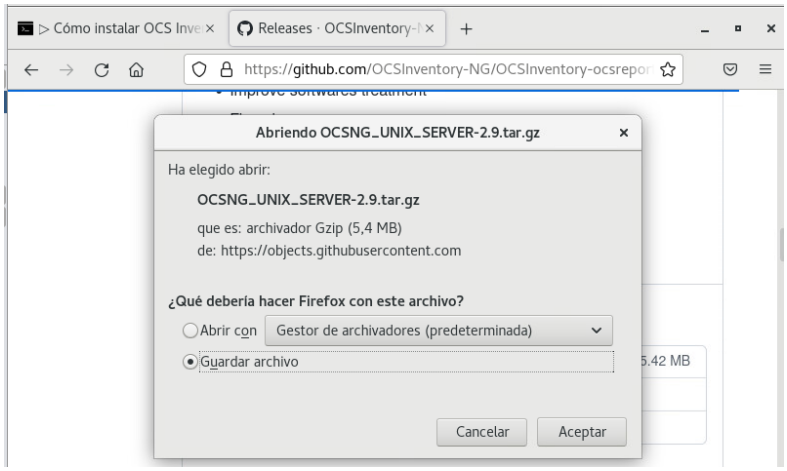
Para la instalación de OCS INVENTORY necesitamos descargar algunas herramientas y utilidades del sistema, para esto utilizamos el comando:

~$ sudo yum install -y policycoreutils-python tar wget

Descargar el paquete OCS Inventory NG Server para CentOS 7 en la fuente del proyecto en Github. Copiar el enlace y descargar desde consola con el siguiente comando wget:

Figura H 1

Descarga de paquete OCS Inventory



Nota: Captura de github OCS Inventory

Para instalar OCS Inventory NG Server en CentOS 7 hay una serie de tareas previas que describiremos a continuación.

Dependencias

Descargar varios paquetes de dependencias, para lo que usaremos los repositorios de CentOS 7, ejecutando el comando:

~$ sudo yum install -y mod_perl perl-Apache-DBI perl-DBD-MySQL perl-XML-Simple perl-Net-IP perl-Archive-Zip perl-Mojolicious perl-Switch perl-Plack php-gd php-mbstring php-soap php-xml

Reiniciar el servicio web para que cargue los nuevos módulos y la configuración de PHP:

~$ sudo systemctl restart httpd

Archivos de OCS Inventory

Descomprimir el archivo descargado anteriormente, en el directorio de trabajo actual:

~$ tar xf OCSNG_UNIX_SERVER-2.9.tar.gz

Cambiar el directorio de trabajo a la carpeta que se acaba de crear con los archivos de OCS Inventory:

~$ cd OCSNG_UNIX_SERVER-2.9

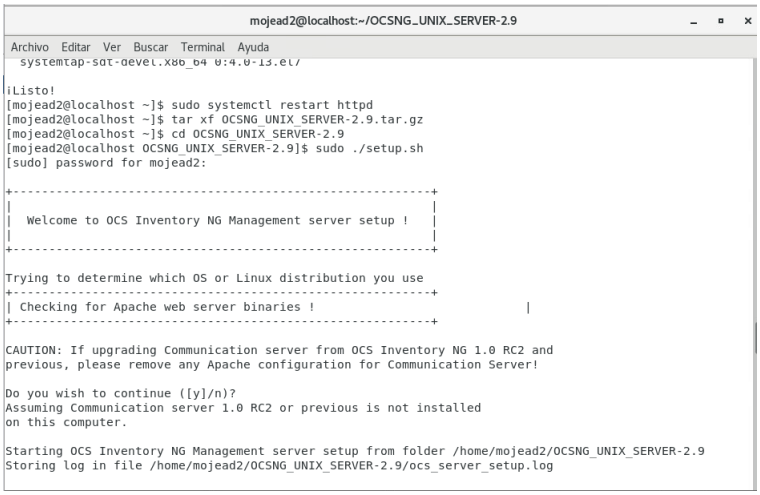
Ejecutar con privilegios el script *setup.sh* que hay en la carpeta:

$ sudo ./setup.sh

Este script verifica que las dependencias estén instaladas, las herramientas necesarias ubicadas en el lugar adecuado y que los archivos de la aplicación y su configuración se creen y copien.

Figura H 2

Configuración del servidor de gestión de inventario OCS Inventory



Nota: Captura de Centos

Todas las preguntas deben ser respondidas por defecto. Para salir del directorio digitar:

$ cd ..

Eliminar definitivamente con el comando:

~$ sudo rm -rf OCSNG_UNIX_SERVER-2.9

Hacer escribible por el servidor web el directorio /var/lib/ocsinventory-reports/, para cambiar la propiedad al usuario con el que corre el servicio web:

~$ sudo chown apache /var/lib/ocsinventory-reports/

SELinux

Definir un contexto de lectura/escritura para el servidor web en la carpeta /usr/share/ocsinventory-report/ocsreports/ con semanage:

~$ sudo semanage fcontext -a -t httpd_sys_rw_content_t "/usr/share/ocsinventory-reports/ocsreports(/.)?"*

Aplicar con restorecon:

~$ sudo restorecon -R /usr/share/ocsinventory-reports/ocsreports/

Base de datos

Crear el soporte de base de datos para la aplicación con el cliente mysql y nuestro usuario administrador:

~$ mysql -u root -p

Crear la base de datos con el nombre por defecto, ocsweb, para facilitar el trabajo:

*> create database **ocsweb**;*

Usar el nombre por defecto para el usuario, ocs. Para MariaDB o MySQL crear el usuario con su contraseña de la siguiente manera:

*> create user ocs@localhost identified by '*XXXXXXXX*';*

Finalmente dar al usuario los permisos sobre la base:

> grant all privileges on ocsweb. to ocs@localhost;*

Salir del cliente mysql:

> exit

Si hemos usado una contraseña distinta a ocs, que es lo recomendable, debemos modificarla manualmente en el archivo de configuración de Apache z-ocsinventory-server.conf:

~$ sudo nano /etc/httpd/conf.d/z-ocsinventory-server.conf

Modificar la siguiente directiva PerlSetVar:

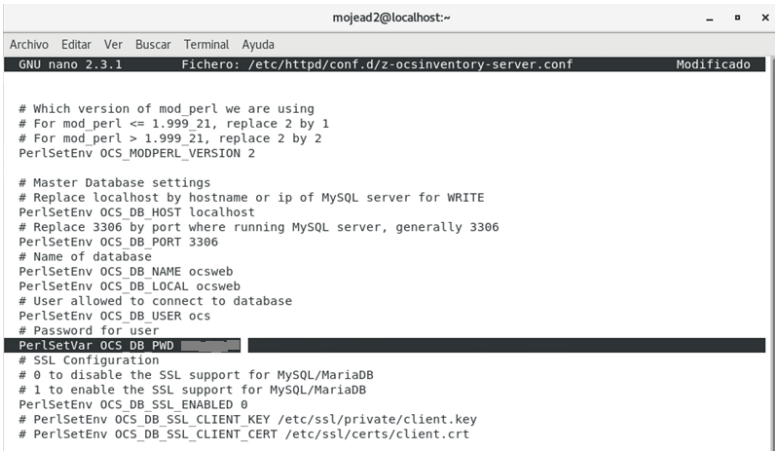
PerlSetVar OCS_DB_PWD ocs

Y reemplazar ocs por la contraseña actual:

PerlSetVar OCS_DB_PWD XXXXXXXX

Figura H 3

Archivo de configuración z-ocsinventory-server.conf



Nota: Captura de Centos

Guardar los cambios y recargar la configuración de Apache:

~$ sudo systemctl reload httpd

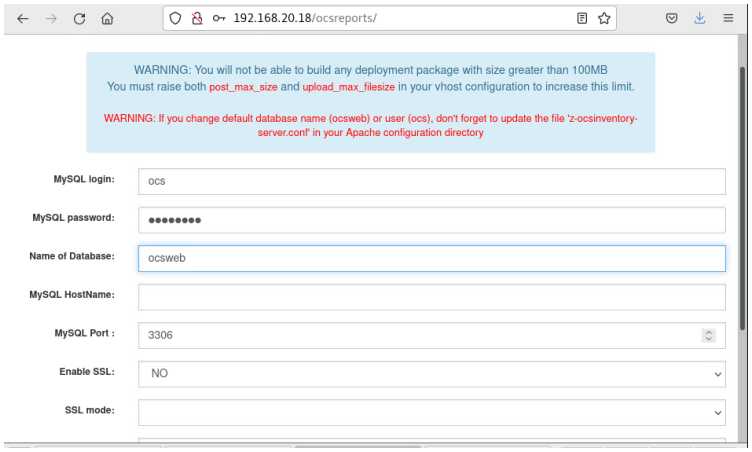
INSTALACIÓN WEB

Para instalar OCS Inventory NG Server utilizamos como URL: 192.168.20.18/ocsreports.

La página inicial del instalador, solicita los datos de conexión con el sistema de bases de datos:

Figura H 4

Instalador OCS Inventory NG Server vía web

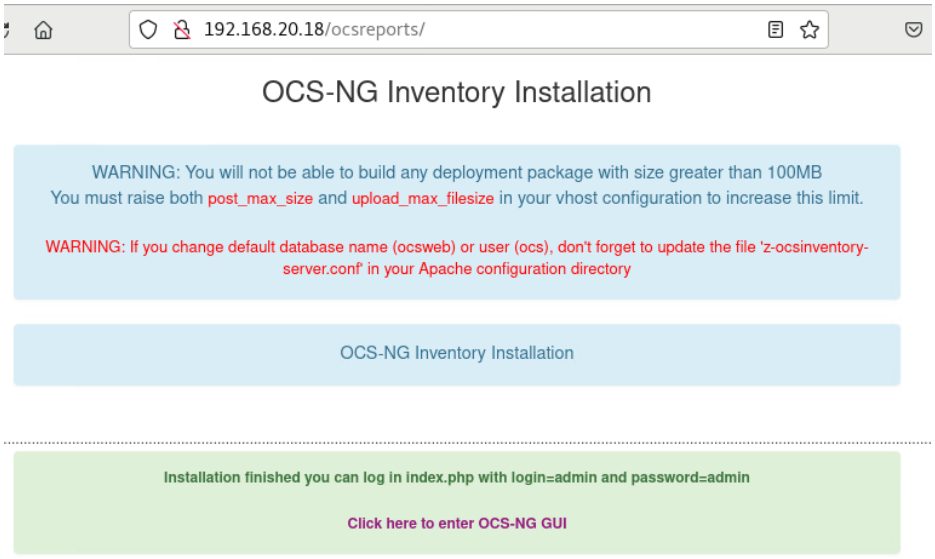


Nota: Captura de OCS Inventory

Ingresar los datos tal como fueron creados previamente, la instalación e inicialización de la base de datos se completará en unos instantes. Un mensaje informa cuando finalice la instalación y seguiremos el enlace que nos da acceso a la aplicación.

Figura H 5

Instalación de OCS-NG Inventory



Nota: Captura de OCS Inventory

A continuación, muestra la página de inicio de sesión de la aplicación:

Figura H 6

Página de inicio de OCS Inventory

Nota: Captura de OCS Inventory

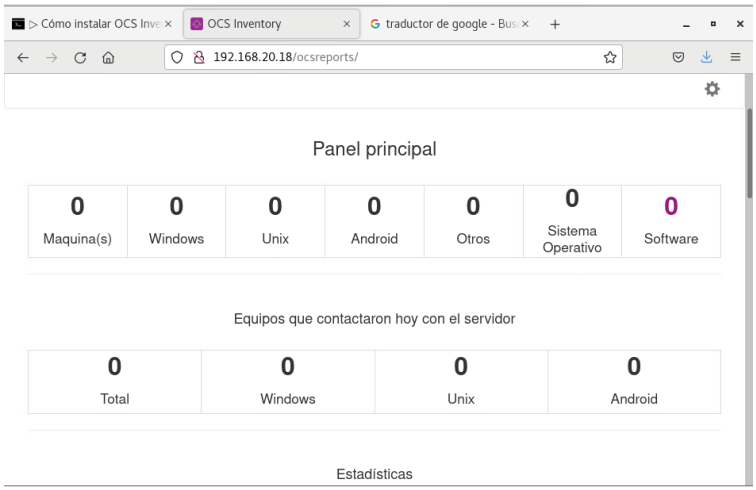
Eliminamos manualmente el instalador web de OCS Inventory NG antes de iniciar la sesión, con el comando:

~$ sudo rm /usr/share/ocsinventory-reports/ocsreports/install.php

En el menú desplegable, elegimos nuestro idioma e iniciamos sesión con las credenciales predeterminadas. De manera inmediata mostrará la página principal de OCS Inventory NG en CentOS 7 y el sistema estará listo para empezar a recibir conexiones de los clientes que estaremos instalando.

Figura H 7

Panel principal de OCS Inventory



Nota: Captura de OCS Inventory

Acceder al menú «MI CUENTA», para actualizar la información de la cuenta de administrador y cambiar la contraseña por defecto.

Instalar los paquetes necesarios en la máquina remota (admin2)

~$ sudo yum install -y epel-release tar wget

Descargar OCS Inventory Agent para CentOS 7

Al no haber paquetes para la distribución, vamos a descargar OCS Inventory Agent para CentOS 7 desde la página del proyecto en Github, con el comando wget.

El proceso de instalar OCS Inventory Agent en CentOS 7 requiere satisfacer algunos requisitos previamente, tal y como detallamos a continuación.

Dependencias

Instalar los paquetes necesarios para cumplir las dependencias con *yum*:

~# yum install -y nmap pciutils perl-ExtUtils-MakeMaker perl-Digest-MD5 perl-LWP-Protocol-https perl-Net-IP perl-Net-Netmask perl-Net-SNMP perl-Proc-Daemon perl-Proc-PID-File perl-XML-Simple

Instalar OCS Inventory Agent

Descomprimir el paquete que descargamos anteriormente:

~# tar xf Ocsinventory-Unix-Agent-2.8.1.tar.gz

Cambiar el directorio de trabajo al subdirectorio que se acaba de crear:

~# cd Ocsinventory-Unix-Agent-2.8.1

Verificar los requisitos y creamos el archivo Makefile mediante el script en perl Makefile.PL presente en el directorio:

 # perl Makefile.PL

Al crearse el archivo Makefile ya podemos lanzar make para la preparación del agente OCS Inventory y sus componentes:

 # make

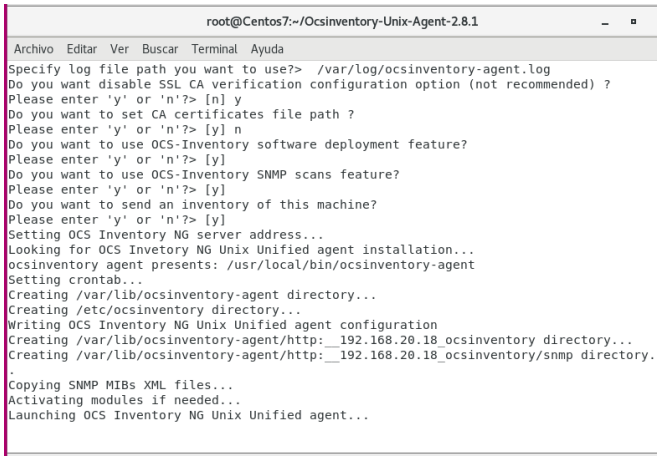
Y realizamos la instalación:

make install

Después de la instalación se lanza automáticamente un script de configuración que nos hará una serie de preguntas:

Figura H 8

Pantalla de script de configuración



Nota: Captura de Centos

La mayoría de preguntas tienen respuestas predeterminadas, sin embargo, en ciertos casos debemos elegir una opción y en otros dar un valor específico:

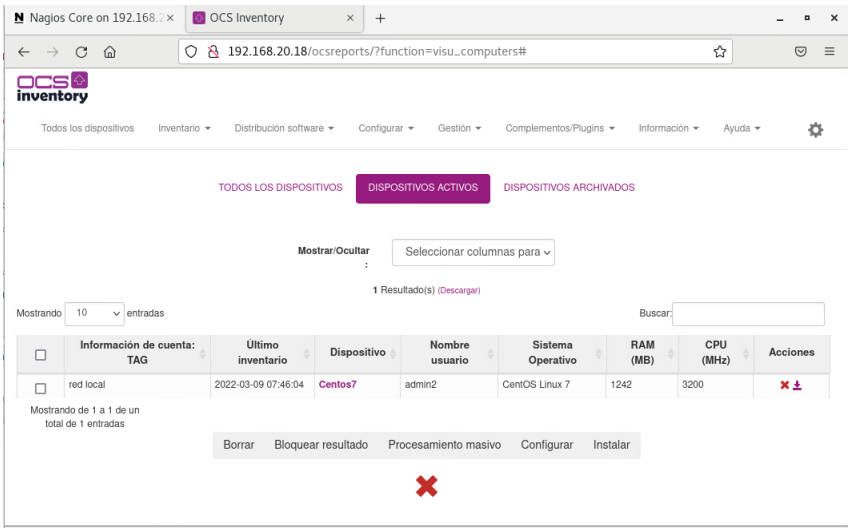
- Para la ubicación de los archivos de configuración de OCS Inventory Agent, en este ejemplo hemos elegido la opción número 0 del menú.
- Dirección del servidor de inventarios, en este caso 192.168.20.18
- Una etiqueta administrativa, en el ejemplo «*red local*«, que ayuda a identificar la máquina, ubicarla geográficamente, etc.
- Archivo de registro o log, en este ejemplo */var/log/ocsinventory-agent.log*.
- En este ejemplo no usamos un servidor de inventarios con seguridad SSL configurada, aunque es recomendable, por lo que no se verifica la conexión con certificados CA y no se necesita indicar la ubicación de estos certificados.

Terminadas las preguntas se guarda la configuración y se lanza el agente por primera vez para contactar con el servidor de inventarios. Una tarea creada en */etc/cron.d/* se encargará de volver a conectar al servidor diariamente.

De manera inmediata, comprobamos que la máquina CentOS 7 se ha registrado correctamente.

Figura H 9

Inventario de OCS Inventory



Nota: Captura de OCS Inventory

Instalación de MRTG

Instalar el servidor web Apache.

Instalación básica del servidor web apache con el siguiente comando:

 # yum -y install httpd

Iniciar el servicio web de apache.

 # systemctl start httpd.service

Habilitar el servicio en el arranque automático

 # systemctl enable httpd.service

Instalar MRTG a través de yum

El siguiente comando es para la dependencia y la utilidad de instalación de mrtg y snmp.

 # yum -y install net-snmp mrtg net-snmp-utils

Configurar SNMP

Para monitorear la interfaz de red y otros recursos como CPU, memoria, debemos configurar snmpd "/etc/snmp/snmpd.conf".

Editar el archivo de configuración.

 # vim /etc/snmp/snmpd.conf

Realizar los siguientes cambios.

(a) Comentar la línea con hash en la línea número 41 como se muestra a continuación.

com2sec notConfigUser predeterminado público

(b) Descomentar el número de línea 74,75, elimine NETWORK/24 y reemplazar con su red.

(c) Descomentar la línea 78,79, reemplazar techtransit.

grupo MyRWGroup v2c local

grupo MyROGroup v2c mi red

(d) Descomentar la línea 85.

ver todo incluido .1 80

(f) Descomentar la línea 93,94, reemplazar techtransit de su nombre.

acceder a MyROGroup "" v2c noauth 0 todos ninguno ninguno

acceder a MyRWGroup "" v2c noauth 0 todos todos todos

Iniciar el servicio snmpd y actívelo desde el inicio automático.

 # systemctl start snmpd.service

```
# systemctl enable httpd.service
```

Mostrar estado (reemplazar "techtransit" por el nombre de la comunidad). Una vez realizado los cambios tenemos la pantalla de MRTG.

ANEXO I. Manual de administración sistema GLPI

Gestión de usuarios, incidencias y Administración de Activos.

Iniciar Sesión en el Sistema GLPI con las credenciales de administrador.

1. Url	192.168.20.18/glpi
Credenciales	Usuario: glpi Contraseña: XXXXXX

Figura I 1

Pantalla de inicio de sesión

Nota: Panel de Información, captura de GLPI

En la página principal aparece una pestaña predeterminada que muestra los paneles de información personalizables para su gestión.

Figura I 2

Pantalla general de GLPI

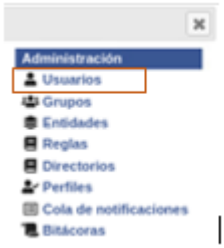
Nota: Captura de GLPI

Creación de usuarios

Ir a la pestaña configuración – Administración- Usuarios

Figura I 3

Pantalla de Administración de GLPI

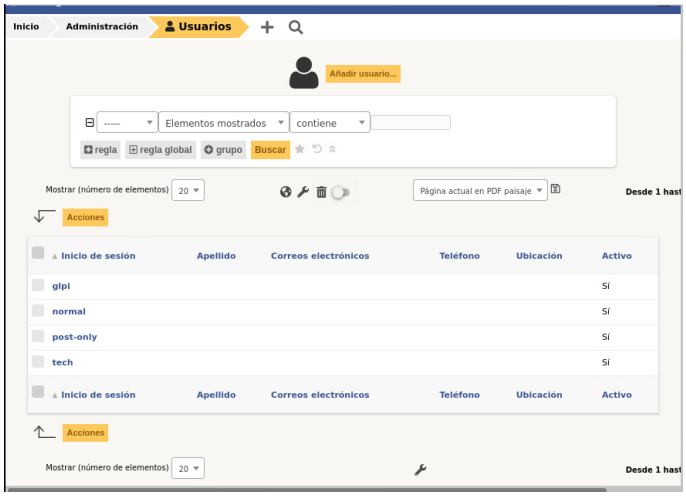


Nota: Captura de GLPI

Se desplega la siguiente plantilla que nos ayuda a agregar la información del usario.

Figura I 4

Pantalla de generación de usuarios

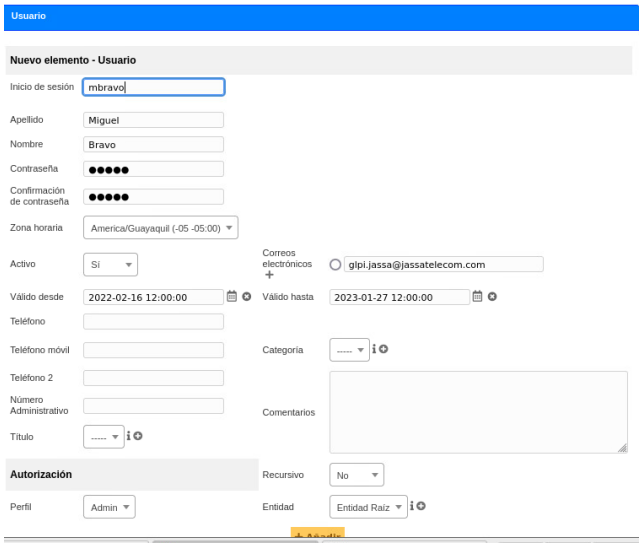


Nota: Captura de GLPI

Añadir la información del usuario, en este campo se agregan los permisos de cada usuario que ingresa a la red, llenar los campos solicitados (*), estos son obligatorios.

Figura I 5

Pantalla e ingreso de datos



Nota: Captura de GLPI

Una vez ingresados los datos, el usuario aparecerá agregado en la lista.

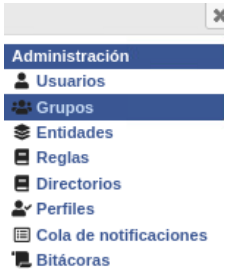
Grupos GLPI

GLPI lleva una planificación y administración tanto de usuarios como de equipos tecnológicos. En este campo se generan los grupos con sus respectivos accesos.

Ir a la pestaña configuración – Administración- Grupos

Figura I 6

Administración-Grupos

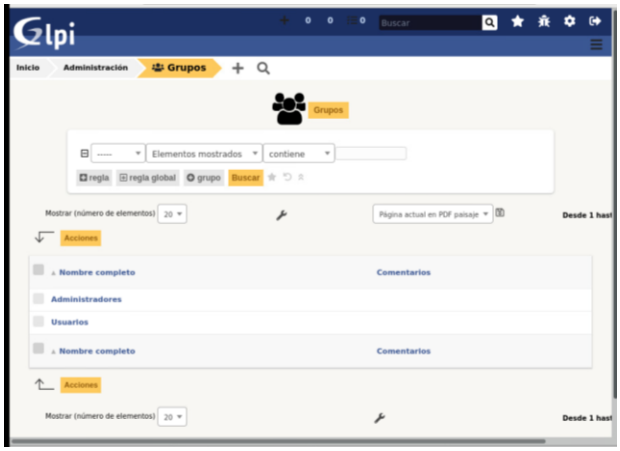


Nota: Captura de GLPI

Se despliega la siguiente plantilla que nos permite agregar grupos en GLPI.

Figura I 7

Plantilla de Grupos

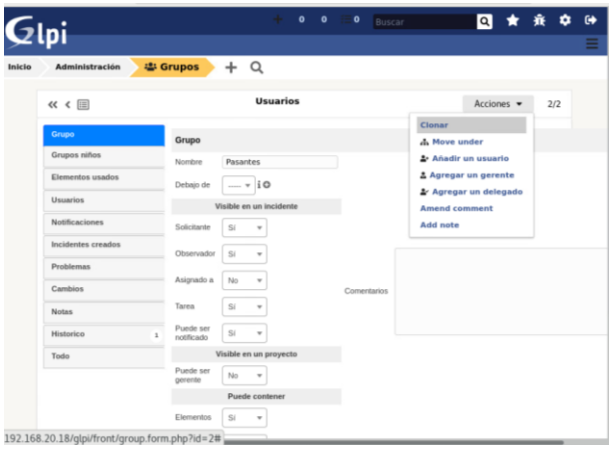


Nota: Captura de GLPI

En este caso crearemos el grupo pasantes

Figura I 8

Creación del grupo pasantes



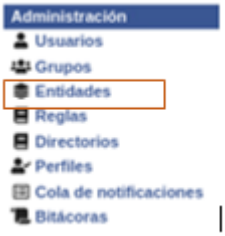
Nota: Captura de GLPI

Entidades en GLPI

Ir a la pestaña configuración – Administración- Entidades

Figura I 9

Administración-Entidades



Nota: Captura de GLPI

En la siguiente plantilla se nos permite agregar entidades en GLPI.

Las entidades son el elemento estructural que divide el parque de información y se relacionan con ubicaciones físicas.

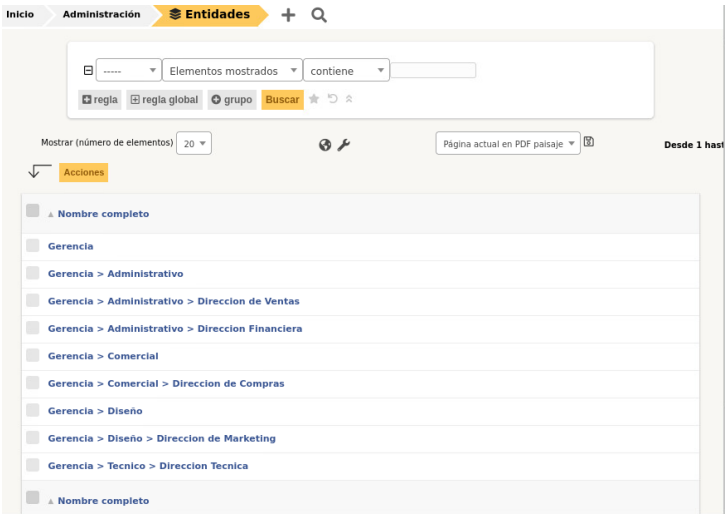
Dependiendo del perfil asignado, cada usuario verá una o más entidades, y el acceso a sus datos podrá realizarse mediante lectura o escritura.

Una nueva entidad debe agregarse de las siguientes maneras:

-Añadir un nuevo elemento- llenamos los campos y damos prioridad a cada uno antes de añadir la entidad.

Figura I 10

Plantilla de asignación de Entidades



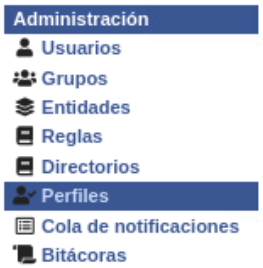
Nota: Captura de GLPI

Perfiles GLPI

Ir a la pestaña configuración – Administración- Perfiles

Figura I 11

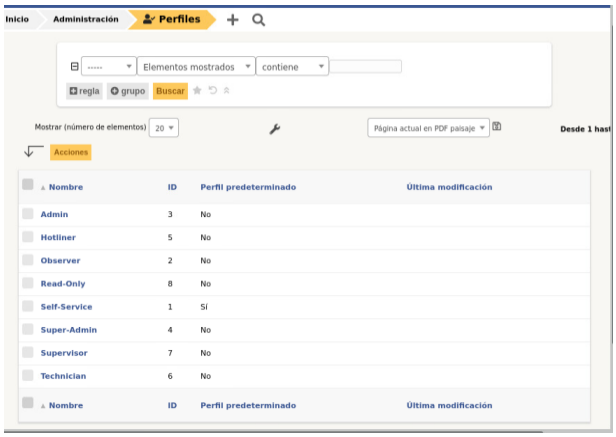
Administración de Perfiles



Nota: Captura de GLPI

Figura I 12

Plantilla de perfil de Administrador



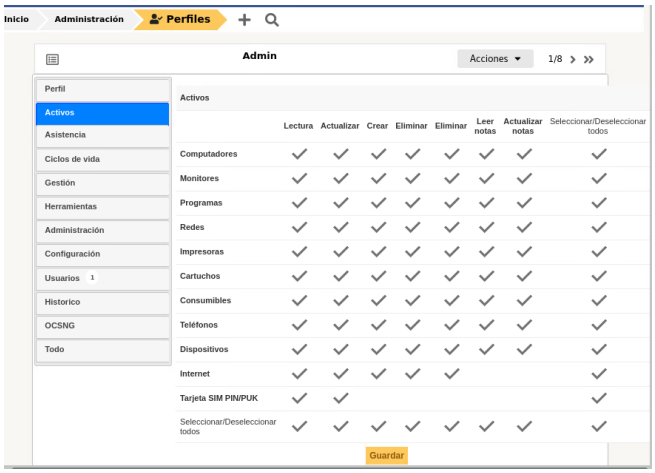
Nota: Captura de GLPI

Admin: Este perfil maneja toda la administración de permisos de software GLPI. Sin embargo, no todos pueden acceder a la configuración de reglas, entidades que pueden afectar las acciones de GLPI.

Activos: En este perfil se puede configurar y asignar los permisos que puede tener el perfil de administrador.

Figura I 13

Permisos a los que pueden acceder los usuarios según su asignación



Nota: Captura de GLPI

Self-Service

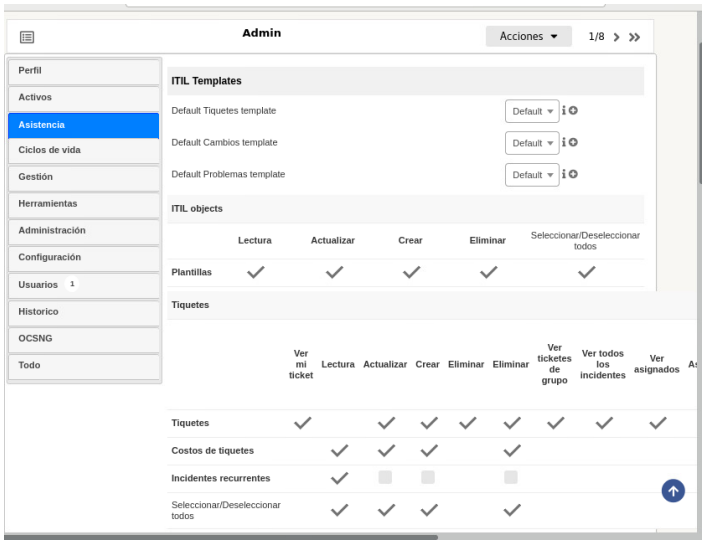
Está destinado a usuarios que requieren de una gestión y asistencia de incidentes a través de una interfaz sencilla. Esta asistencia consistirá en la creación de incidencias asociadas a los sistemas de información, y será específica tanto de las actividades como del hardware y software.

Asistencia:

Es un rol relacionado con el servicio de incidencias de los usuarios.

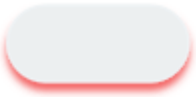
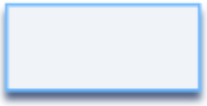
Figura I 14

Administración-Asistencia



Nota: Captura de GLPI

ANEXO J. Simbología utilizada para elaboración de diagramas de flujo

Nombre Símbolo	Descripción	Símbolo
Inicio/Fin	Representa el inicio o fin de un diagrama de flujo.	
Proceso	Representa una actividad o proceso.	
Decisión	Representa la bifurcación de un proceso.	
Flecha	Representa el camino que une los elementos del diagrama.	
Documento	Representa documentos en el soporte papel.	
Base de Datos	Representa información en soporte digital.	

ANEXO K. Acta de entrega recepción de Políticas de gestión y Manuales de procedimiento.

Quito, 6 de Enero del 2023

Señor
MSc. Alexander Trejo
PRESIDENTE EJECUTIVO

A través del presente, Yo, Rosa Lila Hermosa Torres estudiante de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, en calidad de autora del proyecto de grado "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", cordialmente solicito me permita efectuar la entrega de las Políticas de gestión y Manuales de Procedimiento de administración y gestión de red, elaborado en beneficio de la red de la empresa, con el propósito de que esta información sea difundida a los encargados de la infraestructura de red y aplicaciones para su revisión y uso.

Atentamente,

Recibido
06/01/2023
11:24

Rosa Lila Hermosa Torres
C.I.: 100273667-4