UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"SISTEMA DE GESTIÓN DE CONFIGURACIÓN PARA LA INFRAESTRUCTURA DE NETWORKING DE LA EMPRESA PÚBLICA YACHAY E.P."

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: JONATHAN GONZALO TERÁN ESCANTA

DIRECTOR: MSC. JAIME ROBERTO MICHILENA CALDERÓN

Ibarra-Ecuador

2020

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:		1003499884	
APELLIDOS Y NOMBRES:		Terán Escanta Jonathan Gonzalo	
DIRECCIÓN:		Ibarra - Agustín Rosales S/N y 12 de octubre	
EMAIL:		jgterane@utn.edu.ec	
TELÉFONO FIJO:	(06)2-632 002	TELÉFONO MÓVIL:	0983932884

DATOS DE LA OBRA	
TÍTULO:	Sistema de gestión de configuración para la infraestructura de networking de la Empresa Pública Yachay E.P.
AUTOR:	Jonathan Gonzalo Terán Escanta
FECHA:	28 de Febrero del 2020
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ PREGRADO ☐ POSGRADO
TITULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Jaime Michilena Calderón, MSc.

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 asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 27 días del mes de febrero del 2020.

EL AUTOR:

.....

Jonathan Gonzalo Terán Escanta

CI: 1003499884

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN.

MAGISTER JAIME MICHILENA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación "SISTEMA DE GESTIÓN DE CONFIGURACIÓN PARA LA INFRAESTRUCTURA DE NETWORKING DE LA EMPRESA PÚBLICA YACHAY E.P." Ha sido desarrollado por el señor Jonathan Gonzalo Terán Escanta, bajo mi supervisión.

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

.....

Ing. Jaime Michilena, MSc.

1002198438

DIRECTOR

DEDICATORIA.

Dedicado a:

A mis padres María Inés Escanta y Gonzalo Terán, por ser quienes han estado presentes en cada etapa de mi formación profesional y personal, por su constancia y sacrificio.

A mi familia y amigos por todo el apoyo y motivación que me brindaron para nunca decaer y para ser siempre una mejor persona.

JONATHAN G. TERÁN E.

AGRADECIMIENTO.

A Dios por darme la sabiduría, las fuerzas y vitalidad para llegar a culminar esta etapa de la vida con bastos conocimientos de esta hermosa carrera.

A mi madre María Inés y a mi padre Gonzalo por su amor, paciencia, apoyo incondicional y motivación constante para ser siempre una mejor persona cada día, y a toda mi familia por estar cuando más lo he necesitado, con una palabra de aliento e incluso con su ayuda en cada uno de los retos que se me han presentado.

A mi tutor de tesis Ing. Jaime Michilena y a un gran profesional Ing. Carlos Vázquez, por su apoyo, motivación, aliento y sobre todo por transmitirme cada uno de sus conocimientos dentro y fuera del aula.

Al personal del departamento de tecnologías de la anteriormente denominada "Yachay E.P." actualmente "Siembra E.P.", Ing. Nataly Culqui, Ing. Fernando Ortiz, Ing. Fabian Jiménez, por su apoyo, guía y constancia, que permitieron que el proyecto de tesis se cumpla a cabalidad en la empresa de principio a fin.

A mis amigos y compañeros que con su guía, consejos y conocimientos han ayudado en mi formación profesional.

JONATHAN G. TERÁN E.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

RESUMEN.

El presente trabajo tiene como finalidad la implementación de una herramienta que permita a la Empresa Pública Yachay E.P. la gestión de configuración enmarcada en las FCAPS, enfocado en el registro del equipamiento de red del área del Data Center y además en la gestión de tickets de nivel 2 para la unidad de operaciones tecnológicas.

El sistema que se implementa trabaja bajo las buenas prácticas de ITIL, para brindar a la empresa pública Yachay E.P. una herramienta que le permita inventariar los equipos de red de manera rápida, continua, automática y manual del equipamiento de networking de la red del Data Center, así también, esta herramienta permite gestionarlos de manera más rápida en caso de presentarse algún problema o mantenimiento, de forma que la información se encuentre centralizada, evitando la pérdida de tiempo en la búsqueda documentación pertinente como es el caso de contratos, proveedores o SLAs con entes externos de la empresa.

Se puede observar la gran utilidad de esta herramienta debido a que está implementada no solo para el registro e inventario de equipamiento de red, sino también para el registro automático mediante escaneos de red de cada uno de los equipos que cuenten con una tarjeta de red y una dirección IP, además del registro manual de todo el equipamiento o documentación que pueda considerarse necesaria para la unidad de operaciones tecnológicas de la empresa pública Yachay E.P. Hay que resaltar que la información contenida dentro del inventario del sistema puede ser adaptada a las necesidades del técnico responsable o del administrador del sistema pues, será éste quien pueda agregar, modificar o borrar la información existente. El sistema también cuenta con un escaneo de red que no solo facilita al técnico responsable la actualización automática del inventario, sino también le permite mantener el control de la información por medio de un inventario actualizado.

ABSTRACT

The purpose of this document is the implementation of a tool that allows the Public Company Yachay E.P. the configuration management framed in the FCAPS, focused on the registration of the network equipment of the Data Center Area and also on the management of level 2 tickets for the technological operations unit.

The system that is implemented works under the good practices of ITIL, to provide the public company Yachay E.P. with a tool that allows it to inventory the network equipment in a fast, continuous, automatic and manual way of the networking equipment of the Data Center Network. Also, this tool allows to manage them in a faster way in case of any problem or maintenance, so that the information is centralized, avoiding the loss of time in the search of pertinent documentation, such as contracts, suppliers or SLAs with external entities of the company.

The great usefulness of this tool can be observed because it is implemented not only for the registration and inventory of network equipment, but also for the automatic registration by means of network scans of each one of the equipment that has a network card and an IP address, in addition to the manual registration of all the equipment or documentation that may be considered necessary for the technological operations unit of the public company Yachay E.P. It is necessary to emphasize that the information contained within the system's inventory can be adapted to the needs of the responsible technician or the system's administrator, since it will be this one who can add, modify or delete the existing information. The system also has a network scan that not only facilitates the technician in charge of the automatic updating of the inventory, but also allows him to maintain control of the information by means of an updated inventory.

CAPÍTULO I. ANTECEDENTES

1.1.Tema

SISTEMA DE GESTIÓN DE CONFIGURACIÓN PARA LA INFRAESTRUCTURA DE NETWORKING DE LA EMPRESA PÚBLICA YACHAY E.P.

1.2. Problema.

Yachay E.P. es una Empresa Pública Ecuatoriana, la cual está encarga legalmente de la administración del proyecto "Ciudad del Conocimiento Yachay", por lo que su infraestructura de red está en crecimiento. La Dirección de Operaciones Tecnológicas y Servicios HPC (High Performance Computing por sus siglas en ingles) para llevar a cabo su trabajo diario depende del uso de herramientas informáticas, por lo que ha implementado las buenas prácticas de ITIL en cada uno de sus procesos internos. Dentro de La Dirección de Operaciones Tecnológicas y Servicios HPC (de aquí en adelante DOTSHPC), se encuentra la Unidad de Operaciones Tecnológicas y Servicios HPC (de aquí en adelante UOTSHPC), la que se encargada de la gestión de los servicios de Tecnologías de la Información (TI), en especial de la administración, gestión y monitorización de la infraestructura de Networking siendo la parte principal de toda la infraestructura de telecomunicaciones ubicada en el Data Center, el cual se encarga de distribuir los servicios de Internet e Intranet a la Empresa Pública Yachay E.P. y a diferentes sectores que conforman la denominada ciudad del conocimiento Yachay, entre estos: el Centro de Emprendimiento, la Hacienda San Eloy, el Instituto Superior 17 de Julio, la Universidad Yachay Tech, Bloques de residencias, Hoja Blanca, el mercado las Manuelas, Planta de Agua, y el Centro Infantil del Buen Vivir, teniendo usuarios como: personal administrativo de Yachay EP, docentes, estudiantes y público en general que visitan las instalaciones de la Empresa Pública Yachay E.P.

La Empresa Pública Yachay E.P. cuenta con registro de equipamientos interno, mismo que es gestionados por el área administrativa, siendo registros contables y demasiado generales, razón por la cual la UOTSHPC no cuenta con un detalle de cada componente de los servicios de tecnología de información (TI) y considera necesario un registro de activos que permita incluir información técnica a detalle como: contratos, direcciones IP, ubicaciones, hostnames, técnicos responsables, registros de cambios e incidencias presentadas, entre otros, de tal manera que facilite un control de inventario y soporte técnico al presentarse eventos o incidencias, en especial del equipamiento de Networking ubicado en el Data Center. Estos eventos o incidencias son registradas en el servidor OTRS (Sistema de Solicitud de Entradas de Código abierto por sus siglas en inglés), sistema que permite la asignación de tickets de manera muy general, el cual no permite una gestión de activos en base a ITIL, estos tickets generados son gestionados por la Unidad de Operaciones Tecnológicas y Servicios HPC (UOTSHPC) y distribuidos en dos niveles dependiendo de la gravedad de la falla o incidencia, en efecto los tickets de nivel uno son requerimientos de los usuarios respecto a sistemas y equipos informáticos cuya falla pueda resolverse de manera rápida como en el caso de un mantenimiento preventivo de un computador que se apagó inesperadamente, un equipo de red apagado, una impresora sin tinta, entre otros, pero si en caso el problema presente necesita mayor atención como en el caso de que un equipo de red presenta fallas continuas, o a su vez necesita de otra configuración, una impresora o equipo de usuario tiene falla con algún componente interno, por mencionar algunos ejemplos, estas incidencias o fallas generadas para nivel dos al ser de mayor gravedad necesitan ser más específicas con el problema encontrado y reportados a la unidad encargada de solventar el evento o incidencia, razón por la que la UOTSHPC, ha visto que el OTRS no permite la gestión para tickets de nivel dos si no una gestión muy general a nivel de eventos o fallas de nivel uno, por lo que se requiere además un sistema de tickets que permita gestionar los activos de manera más específica, donde se pueda

incluir: el equipamiento activo, su garantía y soporte, el motivo detallado de la incidencia o evento presentado, el procedimiento a seguir en dicha incidencia, su técnico responsable, y su solución.

Con lo anteriormente mencionado el presente proyecto tiene la finalidad de implementar una herramienta basada en software libre que permita a la UOTSHPC la gestión de los servicios de Tecnologías de Información del área de mayor prioridad, en este caso la infraestructura de Networking ubicada en el Data Center, para así contar con un registro de los activos a detalle de cada componente, es decir, que cuente con toda la información, a nivel de hardware y especificaciones técnicas, y a su vez éste sistema permita la generación, asignación, procesamiento y solución de tickets de nivel dos, según lo establecido en el manual de buenas prácticas de ITIL para la gestión de servicios de TI, cumpliendo de esta forma la fase de transición de servicios con el proceso de gestión de la configuración y activos y la fase de Operación del Servicio en los procesos de gestión de eventos, gestión de petición, gestión de servicios y gestión de acceso. Para lo cual ITIL en su versión 2 justifica la aplicación del término CMDB como una “base de datos de gestión de configuración”, por lo que la herramienta a implementar será un servidor CMDB para solventar las necesidades que la Empresa Pública Yachay E.P. en específico la Unidad de Operaciones Tecnológicas y Servicios HPC tiene actualmente

1.3.Objetivos´

1.3.1. Objetivo General

Implementar un sistema de gestión de configuración basado en software libre, aplicando las buenas prácticas de ITIL, para la gestión de activos e incidencias del área de Networking del Data Center de la Empresa Pública Yachay E.P.

1.3.2. Objetivos específicos.

Establecer criterios de la gestión de configuración para los servicios de Tecnologías de Información (TI) competentes al registro y gestión de activos del área de Networking de Yachay E.P.

Normalización de los tipos de incidencias para establecer criterios de eventos e incidencias de nivel uno y nivel dos y su proceso de solución basado en las buenas prácticas de ITIL y sus áreas funcionales.

Implementación de la plataforma de gestión de configuración para el registro y gestión de activos e incidentes para la UOTSHPC.

1.4. Alcance.

Se realizará la implementación de un sistema para la gestión de configuración del modelo FCAPS de la ISO, basado en los procesos competentes en base al estudio preliminar; este sistema será basado en software libre, y permitirá la recolección de información de cada componente del área de Networking del Data Center y tres nodos adicionales, de manera automática mediante el protocolo SNMP en su versión 2 debido a su facilidad para obtener

grandes bloques de datos y rendimiento mejorado en comparación a SNMP en su versión 1; permitiendo la recolecciones información como: direcciones IP, VLANS, estados de puertos, hostnames, ubicaciones, de cada equipo y permitiendo la inclusión de información adicional de manera manual como el caso del técnico responsable de cada equipo y el registro de cambios e incidencias de tal manera que permita a la UOTSHPC de la Empresa Pública Yachay E.P. una buena gestión del equipamiento activo, conforme a lo presentado en las buenas prácticas de ITIL en su versión 3 en la fases de transición de servicios con el proceso de gestión de la configuración y activos y la fase de Operación del Servicio en los procesos de gestión de eventos, gestión de petición, gestión de servicios y gestión de acceso. Para lograr este objetivo se requiere establecer lo siguiente:

Se realizará el análisis de la infraestructura, conectividad, y el método de llevar a cabo el inventario del equipamiento de networking ubicado en el Data Center, así como también se definirán los requerimientos y cada uno de los elementos que deben ser tomados en cuenta para una buena gestión de activos, estos parámetros serán los elementos que deben ser registrados dentro del sistema.

Posteriormente se realizará la normalización de los procesos para los registros, actualización, mantenimiento y baja de equipos de networking, así como también la normalización de los procesos para los eventos e incidencias con la finalidad de clasificarlas para nivel uno y nivel dos para luego definir el procedimiento a seguir para la resolución de un ticket nivel uno o a su vez el escalamiento a ticket de nivel dos, detallando todo el proceso que se realizará y los elementos necesarios que se deben incluir desde la generación, asignación y solución de tickets nivel uno y nivel dos.

Se establecerá criterios para la selección del sistema de gestión de configuración basado en software libre y realizar una comparativa para poder seleccionar el sistema que cumpla con los parámetros establecidos utilizando la metodología IEEE 29148. Una vez realizada la comparativa de los sistemas se procederá a realizar el dimensionamiento de los recursos necesarios para el sistema en base a la cantidad de información que será incluida y procesada. Luego se realizará la implementación del servidor, así como también la instalación de actualizaciones, mejoras o plugin necesarios para su mejor funcionamiento, de tal manera que el servidor permitirá recolectar información de manera automática y continua de los equipos de red ubicados en el Data Center mediante el uso de SNMP v2; permitirá además la modificación e inclusión de parámetros adicionales en los equipos registrados y de ser el necesario la inclusión de más equipos de red de manera manual, así como también el sistema permitirá el registro de eventos e incidencias de nivel dos como tickets específicos con el problema y su solución, de manera manual por la UOTSHPC de la Empresa Pública Yachay E.P., una vez implementado el sistema se procederá a realizar las pruebas de funcionamiento y se realizara un análisis costo beneficio con enfoque al tiempo de asignación y resolución de tickets.

1.5.Justificación.

Yachay al ser una Empresa Pública, debe cumplir normativas generales como las normas de control interno de la contraloría general del estado; siendo la norma 410 referente a tecnologías de la información dentro de la cual se tiene el articulo 09 denominado "Mantenimiento y control de la infraestructura tecnológica", literal 7 "Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables" (CONTRALORÍA GENERAL DEL ESTADO, 2014). En base a este articulo el DOTSHPC

pretende actualizar los registros de manera más detallada a un nivel técnico que permita tener un control de la infraestructura de TI, y dar continuidad a lo nombrado en el literal 6 de “la elaboración de un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica…” (CONTRALORÍA GENERAL DEL ESTADO, 2014).

Todos los procesos que se realizan en la Unidad de Operaciones Tecnológicas y Servicios HPC, se basan en las buenas prácticas de ITIL y sus áreas funcionales, de las cuales enfocándose en el área de diseño de servicio ITIL en su versión 3

Capítulo II. Justificación Teórica

El presente capitulo cuenta con información necesaria para la implementación del sistema de configuración, basados en la administración y gestión de redes de tal manera que estos conceptos faciliten el entendimiento del funcionamiento previo del sistema. Dentro de esta temática se menciona principalmente conceptos de la gestión de configuración y las buenas prácticas de ITIL, y se hace un énfasis en un análisis del funcionamiento de estas dos.

2.1.Administración

Según Idalberto Chiavenato, administración es "el proceso de planear, organizar, dirigir y controlar el uso de los recursos para lograr los objetivos organizacionales" (Chiavenato, 2014), todo este proceso se lo realiza con la finalidad de alcanzar los objetivos definidos, teniendo en cuenta que dependiendo su forma de administración y gestión la organización tendrá o no éxito, razón por que la parte de administración y gestión tiene un gran impacto en las organizaciones.

2.1.1. Administración de redes

Basados en el concepto anterior podemos decir que Administración de red es un proceso de planeación y control de actividades afines con el manejo y funcionamiento de las redes de datos, entre estas pueden considerarse redes MAN, LAN, WAN, entre otras, de una organización, con la finalidad de mejorar la continuidad del servicio, mejorar la utilización de los recursos, proteger la red, controlar cambios y actualizaciones. (Bosmediano Cárdenas, 2017)

2.2.Gestionar

En el glosario de términos usados en la norma ISO 9001 del 2015 se considera el termino gestionar como “actividades coordinadas para dirigir y controlar una organización” (ISO, 2015), ampliando un poco este concepto este término hace referencia a la organización y utilización de recursos que mediante acciones u operaciones afines con la parte administrativa que permitan a la organización su buena dirección.

2.2.1. Gestión de red

Tomando como referencia el concepto anterior se puede decir que la gestión de red es toda aquella actividad que permiten el seguimiento, control y monitoreo del equipo conectado a una red de telecomunicaciones, con el objetivo de garantizar una adecuada Calidad de Servicio (QoS) (Alarcón Ávila, 2017), buscando principalmente proporcionar una buena prestación de servicios, tiempos de caída mínimos, seguridad y flexibilidad adecuada para la red.

2.2.2. Elementos de la gestión de redes

En un sistema de gestión de redes basado en una comunicación gestor - agente se pueden mencionar los siguientes elementos: el gestor, el agente, el protocolo de gestión y la base de información de gestión (MIB, Management Información Base) (Kurose, Redes de Computadoras, 2016)

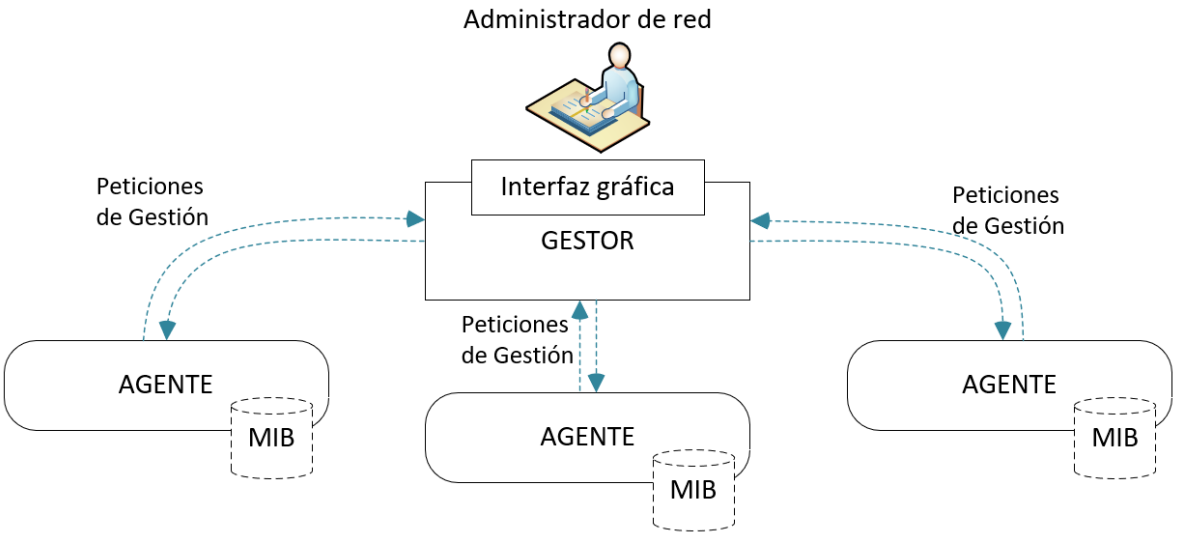


Figura 1. Elementos de la gestión de red

Fuente: Adaptado de (Guzmán López, 2016) , (Oracle, 2016)y (Lara Garcia, 2015)

2.2.2.1.Agente

Es también denominado como la entidad de gestión de red (Network Management Entity o NME), mismo que es considerado como el conjunto de software que permite la gestión dentro de cada nodo en la red que es parte del sistema de gestión (Foroughi , 2014), el cual tiene las siguientes funciones:

- Recolectar información sobre las actividades que se realizan en la red.
- Almacenar la información recolectada de manera local
- Responder a peticiones de un gestor, entre estas podemos mencionar el envío de estadísticas de funcionamiento, envío de información del estado de los nodos, envío de información propia del dispositivo de red, cambio de parámetros de funcionamiento del equipo.

2.2.2.2.Gestor

El gestor es también conocido como aplicación de gestión de red (Network Management Application o NMA). (Ren & Li, 2016) Dentro de una red de comunicación al menos un nodo debe ser considerado como un NMA, el cual realiza entre otras la función de permitir gestionar la red al personal autorizado mediante una interfaz gráfica que permita la intercomunicación hacia equipos locales y remotos, mediante un protocolo de gestión de red a nivel de aplicación.

Al mencionar algunos ejemplos de gestores podemos hablar sobre aplicaciones de consola que permitan la administración SNMP, permitiendo un control remoto de los dispositivos como routers, o switchs y demás equipos gestionables de red; otro ejemplo claro son plataformas desarrolladas para el monitoreo de red a detalle como es el caso de PRTG Network Monitor, Solarwinds, Manage Engine / OPManager misms, Nagios entre otros, que muestran un análisis de rendimiento de los nodos conectados en la red; así también existen plataformas que permiten diferentes métodos de gestión de red como la obtención de información de los nodos conectados, registro de incidencias y fallos del equipamiento instalado, y una administración de recursos de red, como es el caso de GLPI, ManageEngine, iTop, por mencionar algunas. Al momento de seleccionar una de estas hay que tener muy claro cuál es el objetivo con la implementación de tal o cual herramienta.

2.2.2.3.Protocolo de comunicación

El protocolo es un elemento que actúa entre la unidad administradora y los dispositivos administrados, dicho en otras palabras, entre el agente y el gestor, permitiendo al gestor consultar el estado y realizar acciones indirectas de los equipos gestionados a través de sus

agentes, y a su vez el agente puede usar el protocolo para informar a los gestores la existencia de eventos e incidencias como es el ejemplo del fallo de algún componente de la red.

Existen varios protocolos de gestión, entre los cuales se destacan:

- Protocolo Simple de Administración de Redes (SNMP del inglés Simple Network Management Protocol), ya que este es perteneciente a los protocolos TCP/IP, además este es muy utilizado en las redes empresariales ya que es soportado por la mayoría de dispositivos de red.
- Protocolo de administración de información común (CMIP del inglés Common Management Information Protocol) es otro protocolo de gestión de red,este pertenece a la familia de protocolos OSI[1] de la ISO[2], el cual fue creado con el propósito de reemplazar a SNMP, ya que presenta una mejor seguridad y flexibilidad.
- NetFlow es un protocolo creado por Cisco para la recolección de información permitiendo la monitorización de trafico de red, al ser un protocolo privativo no existen muchos equipos que soporten este protocolo, (CISCO, 2014)aunque actualmente funcionan en algunos sistemas operativos de software libre como Linux, y en plataformas como Cisco IOS y NXOS, su compatibilidad no deja de ser una gran debilidad.

[1] OSI (Open Sysem Interconnection), es un modelo desarrollado por la ISO el cual divide las comunicaciones en siete capas y cada una cumple sus tareas específicas hasta completar la comunicación.
[2] ISO (International Organization for Standarization) Es una organización internacional para estandarización de tecnologías, procesos de pruebas científicas, condiciones de trabajo problemas sociales, entre otros

2.2.2.4.Base de información de gestión (MIB)

La base de información de Gestión (Management Information Base o MIB), permite representar la información que se está transmitiendo, utilizando o modificando mediante el protocolo de comunicación (McCloghrie, 1991).

Las MIB tienden a ser modificadas y actualizadas de tal manera que se añadan más funciones y eliminar fallos existentes, todos estos cambios se los realiza de acuerdo al RFC 2578.

En el MIB se definen dos tipos de nodos:

- Los nodos estructurales los que tienen una ubicación en el árbol haciendo como referencia a las “ramas” del mismo.
- Los nodos con información son nodos "hoja", son los que muestran como su nombre lo indica la información final, y de este no se desprenden más nodos.

Cada agente tiene su propia MIB, misma que es una colección de todos los objetos que el administrador puede administrar.

La MIB se componer de estructuralmente de los siguientes nodos:

- **System**: nodo del cual se desprenden objetos que brindan información gen de este nodo cuelgan objetos que proporcionan información genérica del sistema gestionado. Un ejemplo es el lugar donde se encuentra el sistema y la persona encargada de la administración.
- **Interfaces**: como su nombre lo indica muestra la información de las interfaces por medio de la cual está conectado el sistema, además incluye estadísticamente eventos que han suscitado en este.

- **Traducción de direcciones** (Address Traslation o AT), en este se almacenan las direcciones de nivel de enlace que correspondan a una dirección IP, este campo ya no es muy utilizado, pero se lo conserva para mantener compatibilidad con versiones de MIB antiguas.
- **Ip**: en este tipo de nodos se almacena exclusivamente información de capa IP, tal como la configuración y estadísticas.
- **ICMP**: en este grupo se almacenan la cantidad de paquetes ICMP entrantes y salientes, como si fuera un contador.
- **TCP**: En este se conforma de información elacionada con las estadísticas configuración y estado del protocolo TCP.
- **UDP**: configuración y estadísticas del protocolo UDP es la información que se incluye en este grupo.
- **EGP**: al igual que en TCP y UDP, este grupo se concentra en obtener información referente a la configuración y estadísticas de operación del protocolo EGP
- **Transmission:** De este nodo cuelgan grupos referidos a las distintas tecnologías del nivel de enlace implementadas en las interfaces de red del sistema gestionado.
- **SNMP:** Este objeto define información general relacionada con el propio SNMP.

Antes de realizar una ubicación jerárquica de la estructura MIB, en la Figura 2, se muestra la ubicación jerárquica de la ubicación de la MIB, misma que es una rama de la gestión de Internet del árbol OID (Object Identifier o en español Identificador de Objeto) siendo esta dirección .iso.org.dod.Internet.mgmt.mib o de la forma numérica .1.3.6.1.2.1

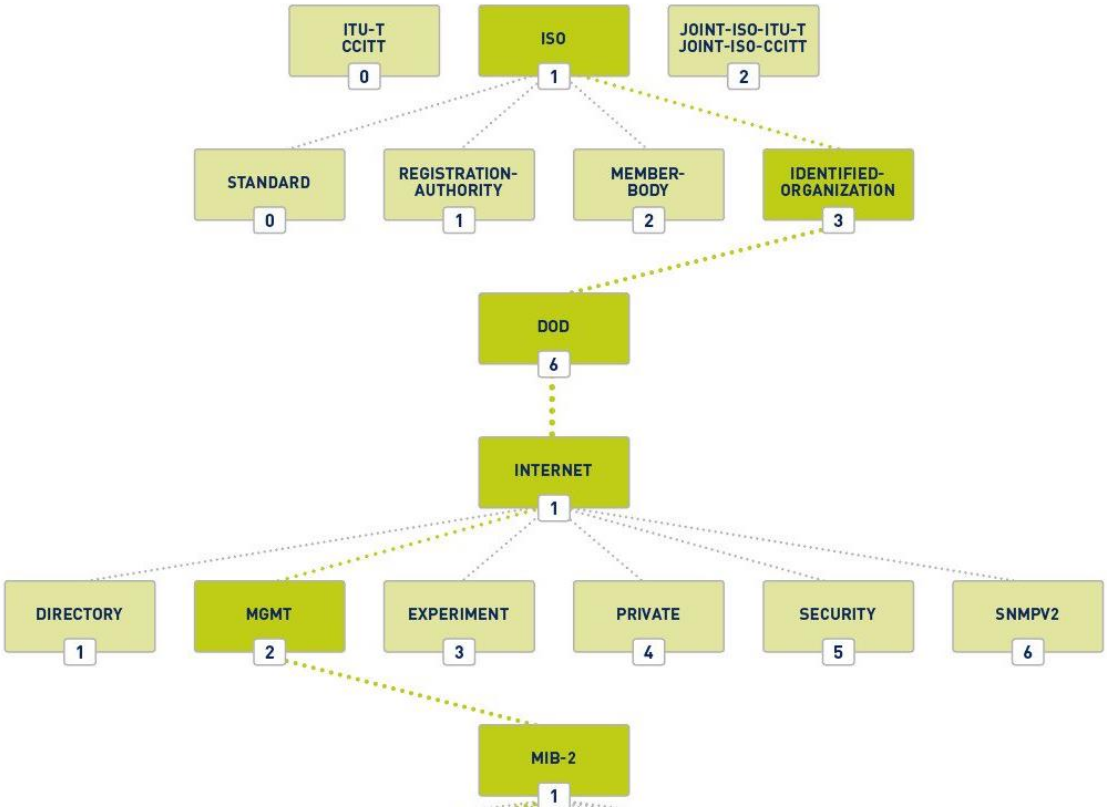


Figura 2. Árbol MIB OID

Fuente: (PAESSLER, 2019)

Una vez entendido el árbol organizacional entramos a la ubicación de los elementos que conforman la estructura de la MIB, los que se ubicarían debajo del bloque de MIB-2. Como se muestra en la Figura 3.

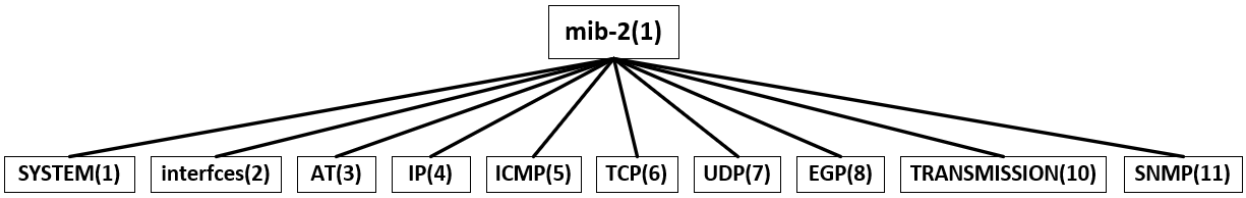


Figura 3. Estructura de MIB

Fuente: (Kurose & Ross, Computer Networking: A Top-Down Approach, 2016)

Para comprender la estructura de la MIB y los árboles hay que tener en cuenta que es un OID. Un identificador de objeto (Object Identiffier u OID) es un mecanismo de identificación ampliamente utilizado y desarrollado conjuntamente por el UIT-T y la ISO / IEC para nombrar cualquier tipo de objeto, concepto o "cosa" con un nombre global que requiere un nombre persistente o de larga vida útil. No está diseñado para ser utilizado para nombres transitorios, además los OID, una vez asignados, no deben reutilizarse para un objeto / cosa diferente. Se basa en una estructura de nombre jerárquica basada en el "árbol OID". Esta estructura de nombres usa una secuencia de nombres, cuyo primer nombre identifica un "nodo" de nivel superior en el árbol OID, y el siguiente proporciona una identificación adicional de arcos que conducen a subnodos debajo del nivel superior, y así sucesivamente para cualquier profundidad. La definición formal de OID proviene de la recomendación (UIT-T X.680, 2015) en su última revisión definido en el capítulo 32.

2.3.Protocolo simple de admiración de red (SNMP)

El proceso de gestionar la red implica que la red debe ser monitoreada constantemente para que la red funcione como se pretende que lo haga, para eso se han creado diferentes protocolos y estándares que permitan un fácil y permanente control de la red, entre estos se desarrolló el protocolo simple de administración de red SNMP (del inglés Simple Network Management Protocolo)

SMP es un protocolo que permite la gestión de la red, haciendo que el agente y el gestor puedan comunicarse de manera remota (Acosta Maza, 2017), mediante el intercambio de información basándose en un método de solicitud y respuesta, mostrando información de tres tipos: Información de estado, advertencias y alarmas.

Este protocolo fue definido por la IETF[3] que público una serie de RFC[4] según las versiones que SNMP ha ido desarrollando.

2.3.1. Comparativa de las versiones de SNMP.

A continuación, se muestra una comparativa entre las versiones existentes en la actualidad, las cuales son SNMP v1, SNMP v2 y SNMP v3.

SNMP v1 fue la primera versión de este protocolo lanzado hace casi 30 años, este es un protocolo de sondeo básico que no utiliza muchos recursos ya que este no cuenta con métodos de cifrado para la transmisión de información, esta versión es muy fácil de utilizar, aunque su principal desventaja es la falta de cifrado ya que en los entornos de redes actuales esta es considerada como una vulnerabilidad para los sistemas críticos, debido a esto su uso ha sido reducido a nivel empresarial.

SNMP v2 se crea en base a la gran demanda de la red, misma que fue lanzada en la década de 1990, actualmente cuenta con al menos tres tipos con un subprotocolo conocido como SNMP v2c, haciendo referencia a SNMP de comunidad versión 2, entre las ventajas que esta versión tiene se puede destacar la seguridad agregada, además agrega dos operaciones de

[3] IETF Internet Engineering Task Force (en español, Grupo de Trabajo de Ingeniería de Internet1) es una organización internacional abierta de normalización.

[4] RFC (Request For Coments) son documentos numerados que describen y definen protocolos, métodos, conceptos y programas de internet, la gestión de estos documentos la realiza la IETF

traps[5]: GetBulke e Inform , la primera se utiliza para la recuperación de bloques de datos grandes, y la segunda permite enviar traps de información a un agente o gestor y permitir su respuesta. SNMPv2 además mejora aspectos de gestión como la funcionalidad mejorando la estructura de funcionamiento de tal manera que un dispositivo pueda usarse como agente y como gestor, la eficiencia de operación es otra mejora importante al permitir un mayor procesamiento de información, y por último tenemos un rendimiento mejorado mismo que se ve afectado al momento de implementar mayores seguridades y encriptaciones de la información.

SNMP v3 es un protocolo de interoperabilidad mismo que está basado en estándares de gestión de red, este protocolo proporciona acceso de manera segura a dispositivos conectados en red, mediante la autenticación y encriptación de los paquetes de información, esta es la más relevante mejora de las otras versiones de este protocolo. SNMP v3 usa el Código de Autenticación de Mensaje Hash (HMAC) para la encriptación de información, su mayor desventaja es la compatibilidad con los equipos de red actuales.

A continuación, se muestra una tabla comparativa con información destacada en cada una de las versiones de SNMP mencionadas previamente.

Tabla 1. Comparativa de las versiones de SNMP

Contenido	**SNMPv1**	**SNMPv2**	**SNMPv3**
Normas	RFC-1155.1157.1212	RFC-1441,1452 RFC-1909.1910 RFC- 1901 a 1908	RFC-1902 a 1908,2271 a 2275

[5] SNMP Traps: son mensajes enviados de forma remota desde los dispositivos SNMP activos hacia el agente SNMP, comunicando de esta manera eventos de la red.

Seguridad	No hay seguridad de acceso a la red.	No se pudo mejorar la seguridad.	Su característica principal es la seguridad mejorada.
Complejidad	Limitaciones de rendimiento y seguridad.	Más potente pero más complejo que SNMPv1.	SNMPv3 se centra en mejorar el aspecto de seguridad.
Operaciones del protocolo	GetRequest GetNextRequest SetRequest Trap Respuesta	Se aumentan dos mensajes más (solicitud de información "Inform", solicitud de obtención masiva "GetBulke")	Implementa las especificaciones SNMP v1 y v2
MIB	Define MIB limitado, fácilmente implementado de variables escalares y tablas bidimensionales	Define el marco general con el que se define y construye la MIB.	Puede configurar agentes para proporcionar una cantidad de niveles de acceso a MIB
Cadenas de texto sin formato	Sí	Sí	No
Tráfico cifrado, Detección de paquetes mal formados.	No	Sí	Sí

Fuente: Adaptado de (Shingote & Bagwe, 2018) y (CISCO, 2014)

2.4.Modelo funcional de la ISO (FCAPS).

FCAPS es un marco de gestión de red creado por la Organización Internacional de Normalización (ISO), este término es un acrónimo que significa Fault, Configuration, Accounting, Performance and Security. (ISO, 2015)

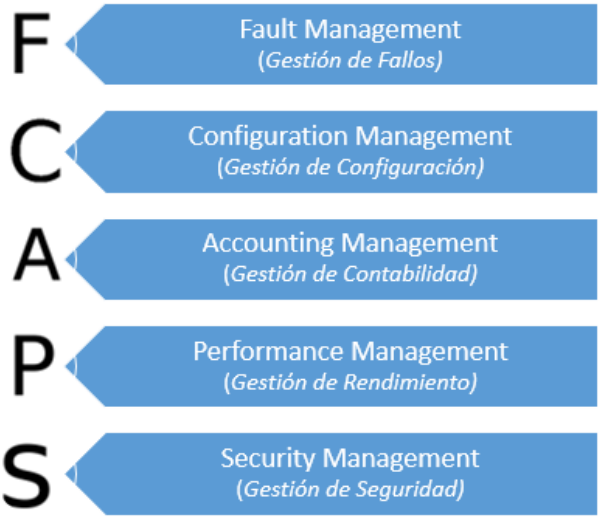


Figura 4. Modelo Funcional FCAPS de la ISO para gestión de redes

Fuente: Adaptado de (CIC, 2019)

El modelo FCAPS es utilizado para los Sistemas de gestión de elementos (EMS), los Sistemas de gestión de redes (NMS) y los Sistemas de soporte de operaciones (OSS), siendo así un modelo universal, este modelo ha sido reconocido como un método simple, debido a que los usuarios pueden describir y clasificar características de las áreas del mismo modelo. (Rizos, 2016)

- **Gestión de Fallos**: Esta área de gestión tiene como objetivo detectar, aislar y solucionar errores que afectan al funcionamiento y disponibilidad de la red gestionada, además realiza el mantenimiento, el análisis de los registros de fallos, secuencias de pruebas de diagnóstico y presentación de informes o notificaciones de fallos. (Ayala Yandun, 2015)
- **Gestión de Configuración**: la administración efectiva de la configuración garantiza que los dispositivos contengan la configuración correcta según la política. También proporciona un mecanismo para volver rápidamente a las operaciones de los dispositivos con fallas, ya que una herramienta de administración de la configuración efectiva almacenará la configuración de cada

dispositivo en un repositorio de búsqueda independiente. En el entorno actual de estrictas regulaciones de cumplimiento, solo a través de una configuración efectiva, una red pasará la revisión de un auditor.

- **Gestión de Contabilidad**: es conocida también como administración de facturación, se basa en el registro del uso de los recursos y servicios facilitados por la red a los usuarios. Dentro de las funciones de la gestión de contabilidad tenemos la recopilación de datos sobre el manejo de los recursos, mantenimiento del registro de cuentas de usuario, sostenimiento de estadísticas de uso, mantenimiento del rendimiento de la red favorablemente y definición de procedimientos para tarifación. (Ayala Yandun, 2015)
- **Gestión de Rendimiento**: esta área se encarga de un monitoreo constante de evaluación del comportamiento y el correcto funcionamiento de los dispositivos gestionados y la efectividad de determinadas actividades, además, recoge y procesa los datos medidos y lo presenta en informes, (Ayala Yandun, 2015) garantizando que la red supervisada funciona según lo esperado y que los recursos de red disponibles se asignen de manera eficiente.
- **Gestión de Seguridad:** se encarga de proteger las redes de accesos no autorizados, por lo que se relaciona con la generación, distribución y almacenamiento de claves de cifrado, información de contraseñas, también brinda protección a los equipos de comunicación, servidores y estaciones de trabajo de ataques provenientes de terceros que ayuda en la conservación de la integridad del sistema (Ayala Yandun, 2015), en este caso la red está protegida contra hackers, usuarios que no están autorizados y daño físico o electrónico. La confidencialidad de los datos del usuario se conserva cuando sea necesario o se justifique, también estos sistemas de seguridad permiten a los

> administradores de red vigilar lo que cada usuario autorizado puede o no hacer con el sistema. (Rouse, 2007)

2.4.1. Gestión de configuración.

Esta gestión se refiere a conservar información referente al diseño y configuración actual de la red. En esta área funcional encontraremos todo lo relacionado con el funcionamiento detallado de la configuración de hardware y software como la gestión de configuración de hardware donde su objetivo es presentar lo que hace la infraestructura e ilustrar las ubicaciones físicas y vínculos entre cada elemento, que se conocen como elementos de configuración (CI), y la gestión de configuración de software en la que se incluye la identificación de la configuración, el control de cambios de configuración, la determinación del estado de configuración y la configuración de autenticación. (Ayala Yandun, 2015)

Para la configuración se debe tomar en cuenta aspectos como:

- El lugar desde donde se realizará a configuración,
- El almacenamiento de la configuración,
- La validez de la configuración (estática o dinámica)
- La interface de usuario de configurador. (Agudelo, 2001)

Además, proporciona una configuración centralizada de dispositivos y redes, que también ofrece configuración inicial de los elementos de red y de sus componentes, seguimiento y sincronización de parámetros de configuración de red, configuración masiva con plantillas, configuración de parámetros avanzados, como VLAN, QoS, protección de radio, etc., y copia de seguridad y restauración de la configuración. (Rizos, 2016).

Un sistema de administración o monitoreo debe permitir a los usuarios realizar un descubrimiento profundo de su red, a fin de descubrir no solo todos los elementos de red (NE) administrados, sino también sus objetos "contenidos", incluyendo tarjetas, puertos, conexiones, etc. esto se puede realizar de tres maneras distintas:

- Manualmente: añadiendo dominios uno por uno en cada uno de los elementos de red.
- De manera masiva: importación de un archivo que contiene la configuración de toda la red.
- Programada: automático de la red planificada previamente en base a horarios definidos por el usuario. (Rizos, 2016)

La topología de la gestión de configuración es muy útil para grandes redes distribuidas, permitiendo a los usuarios monitorear el estado operativo de su red, en tiempo real, a través de un mapa gráfico integrado, también se admite a través de mapas de fondo configurables, vectorizados o imágenes, donde los dominios y los elementos gestionados se representan gráficamente. (Rizos, 2016)

2.4.1.1.Gestión de configuración y otras áreas funcionales

La gestión de configuración dentro de las FCAPS, es un proceso muy centralizado por lo que se conecta con las demás gestiones del modelo, a continuación, se muestra la Tabla 2, donde se muestra la interacción que existe entre las diferentes áreas de la FCAPS con relación a la gestión de configuración.

Tabla 2. Relación de la Gestión de Configuración y las demás áreas de FCAPS

Relación	Gestión de Configuración
Gestión de Fallos	Se busca las causas de las incidencias, se documenta, para crear una nueva configuración. A su vez de acuerdo a la configuración solicitada por el usuario se coordina con herramientas que ayuden a detectar incidentes y luego comunicarlos, para que posteriormente con el historial eliminar las causas o minimizar el impacto de fallo mediante una reconfiguración de la red.
Gestión de Contabilidad	En este proceso se incluye la optimización de la red y se revisa permanente los servicios de tal manera que si existe una falta con algún SLA la gestión de configuración entra a realizar sus procesos para levantar el servicio y cumplir con el SLA respectivo, aplicando planes de contingencia y de mantenimiento preventivo.
Gestión de Rendimiento	En esta gestión se realiza la vigilancia del rendimiento de la red y a partir de esto se verifica los recursos necesarios para un buen funcionamiento, monitoreando, recolectando, registrando y analizando datos necesarios, la gestión de configuración ayuda a esta gestión a mejorar los servicios, en el caso de que se necesiten configurar nuevos equipos o realizar nuevas actualizaciones.
Gestión de Seguridad	Juntamente con el usuario-cliente se determina los parámetros de seguridad de la red, determinando dentro de la configuración los elementos de acceso a redes, a sistemas información y a sistemas de tránsito. A su vez determinar las Políticas que ayudan a disminuir la vulnerabilidad e impacto de posibles ataques. La manifestación de quejas de los clientes y la accesibilidad de la información deben ser configuradas con herramientas simples.

2.5.ITIL.

Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infraestructure Library o ITIL) es definida como el conjunto de "buenas prácticas" para la gestión de servicios de Tecnología Informática (TI)[6], desde un enfoque integral como lo propone la IEC/ISO 20000. Los servicios de TI abarcan a personas, procesos, tecnologías y proveedores, permitiendo que conjuntamente se pueda brindar servicios de calidad enfocándose a la satisfacción del cliente.

ITIL está conformado por cinco libros los que conforman el denominado "ciclo de vida ITIL", con sus títulos originales en ingles son los siguientes:

- ITIL v3 Estrategia de Servicio (SS del inglés Service Strategy)
- ITIL v3 Diseño de Servicio (SD del inglés Service Design)
- ITIL v3 Operación de Servicio (SO del inglés Service Operation)
- ITIL v3 Mejora Continua del Servicio (CSI del inglés Continual Service Improvement)
- ITIL v3 Transición de Servicio (ST del inglés Service Transition)

[6] Servicios de TI: se lo denomina al conjunto de actividades que tienen la finalidad de responder las necesidades de un cliente de tal manera que el valor de este servicio sea potenciado y sus costos de operación y riesgo reducidos

2.5.1. Ciclo de vida de ITIL.

ITIL cumple un ciclo de vida el cual se muestra en la Figura 5, cabe recalcar que existe un orden secuencial entre las fases Estrategia, Diseño, transacción y Operación, y dentro de cada una de estas fases se sitúan diferentes procesos, los cuales no deben ser precisamente secuenciales en su orden de ejecución, sino más bien pueden ejecutarse al mismo tiempo. El Ciclo de Vida del Servicio es un modelo conceptual de la v3 de ITIL

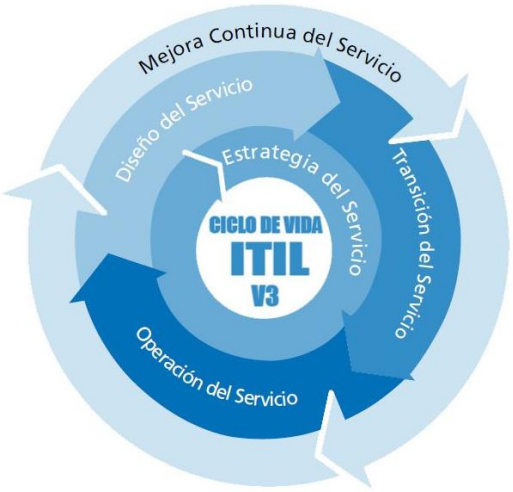


Figura 5. Ciclo de Vida de ITIL v3

Fuente: (Bi-Tecing, 2014)

2.5.2. Estrategia de servicio.

Diseña el plan de acción que permitirá desarrollar una estrategia en la Organización en cuanto a las Tecnologías de la Información.

Este apartado trata de aspectos relacionados con el estudio de nuevas oportunidades de mercado, la distribución de los servicios, catálogos de servicios, considerando esto como una estrategia a lo largo del ciclo de vida de los procesos.

Desarrolla varias áreas; entre ellas se incluyen las siguientes:

- Creación de Valor a través del Servicio
- Gestión de la Cartera de Servicios
- Gestión de la demanda
- Gestión financiera Estrategia general.

2.5.3. Diseño del servicio.

En esta fase se proporcionan guías de como diseñar y desarrollar servicios con la finalidad de convertir estos objetos estratégicos en portafolios de servicio. El diseño de servicio es considerada como la transición de una estrategia de negocio a un modelo de servicio, teniendo en cuenta la planificación, monitorización, mejoramiento, para su muestra al cliente y una posterior gestión interna para ajustarse a la estrategia de la empresa de tal manera que en base a sus necesidades su puesta en marcha y mantenimiento se lo realice mediante los requerimientos, expectativas y aspectos de valor agregado para el cliente, y que internamente sean considerados para brindar un equilibrado servicio en cuanto a costo y eficiencia en los resultados.

En esta área se consideran los siguientes procesos.

- Gestión de los niveles de servicio.
- Gestión del catálogo de servicio
- Gestión de seguridad de la información
- Gestión de proveedores
- Gestión de la capacidad (de recursos)
- Gestión de continuidad

2.5.4. Transición de servicio.

El principal objetivo de esta fase es la implementación de los servicios nuevos o modificados teniendo un mínimo impacto para el negocio cumpliendo con los parámetros de costo tiempo y calidad permitidos. Al tener una eficaz transacción de servicios se brinda a la organización mejor adaptabilidad al cambio, el cual es un aspecto muy importante en entornos cambiantes como es el entorno de las redes de comunicación. (ITIL, 2015)

Para dar cumplimiento a esta fase se incluyen los siguientes procesos.

- **Planificación y Soporte de Transición (TPS):** este proceso se ocupa de la gestión y control del plan de transición.
- **Servicio de validación y pruebas (SVT)**: se ocupa de la calidad de los servicios ofrecidos.
- **Evaluación de cambios:** tiene como objetivo evaluar cambios importantes, como la introducción de un nuevo servicio o un cambio sustancial en un servicio existente, antes de que dichos cambios puedan pasar a la siguiente fase de su ciclo de vida.
- **Gestión de lanzamiento e implementación:** tiene como objetivo crear, probar y entregar la capacidad para proporcionar los servicios especificados por el diseño del servicio y que cumplirán los requisitos de los interesados para entregar la solución prevista.
- **Gestión del cambio**: este proceso garantiza la gestión y el control del proceso de gestión del cambio. También evita que se produzcan cambios no autorizados. ITIL recomienda que esta actuación se realice y se disponga de una CMDB (Change Management Data Base) o base de datos para la gestión del cambio, donde se recojan los datos provenientes de las RFC (Request for Change - peticiones de

cambio), de la que se obtendrán para su posterior análisis, evaluación y se planifique un posible cambio

- **Gestión de activos y configuración de servicios (SACM):** Mantiene la base de datos para CI tales como servidores, conmutadores, enrutadores, etc.
- **Conocimiento administrativo**: este proceso trata de recopilar, almacenar, analizar y compartir conocimientos.

2.5.4.1.Gestión de activos y configuración de servicios (SACM)

El propósito del proceso de SACM es garantizar que los activos necesarios para prestar los servicios estén adecuadamente controlados y que la información precisa y confiable sobre esos activos esté disponible cuando y donde sea necesaria. Esta información incluye detalles sobre cómo se han configurado los activos y las relaciones entre los activos.

Persigue los siguientes objetivos:

- Asegurar que los activos bajo el control de la organización de TI se identifiquen, controlen y cuiden adecuadamente a lo largo de su ciclo de vida
- Identificar los servicios de control, registro, informe, auditoría y verificación y otros CI, incluidas las versiones, líneas de base, componentes de los componentes, sus atributos y relaciones
- Tener en cuenta, administrar y proteger la integridad de los CI a lo largo del ciclo de vida del servicio trabajando con la administración de cambios para garantizar que solo se utilicen los componentes autorizados y solo se realicen los cambios autorizados.

- Asegure la integridad de los CI y las configuraciones requeridas para controlar los servicios al establecer y mantener un sistema de gestión de la configuración (CMS) preciso y completo.
- Mantener información de configuración precisa sobre el estado histórico, planificado y actual de los servicios y otros CI

La optimización del rendimiento de los activos y configuraciones del servicio mejora el rendimiento general del servicio y optimiza los costos y riesgos causados por activos mal administrados, por ejemplo, interrupciones del servicio, multas, tarifas de licencia correctas y auditorías fallidas. (ITIL, 2015)

SACM proporciona visibilidad de representaciones precisas de un servicio, lanzamiento o entorno que permite:

- El personal de TI debe comprender la configuración y las relaciones de los servicios y los elementos de configuración que los proporcionan.
- Mejor previsión y planificación de cambios.
- Evaluación exitosa, planificación y entrega de cambios y lanzamientos.
- Resolución de incidencias y problemas dentro de los objetivos de nivel de servicio.
- Entrega de niveles de servicio y garantías.

Como se define en ITIL v3, el proceso SACM tiene seis subprocesos que operan bajo este. A continuación, se muestran la descripción de esos subprocesos

- **Gestión y planificación:** El objetivo principal de este subproceso de Gestión y Planificación es definir la estrategia, política, alcance, objetivos, procesos, procedimientos, funciones y responsabilidades del proceso de SACM. También

define la ubicación de las áreas de almacenamiento y las bibliotecas utilizadas para almacenar hardware, software y documentación. Además, gestiona los esquemas y diseños CMDB[7], CMS[8], DML[9]. ITIL define a este subproceso como el punto de referencia central de todo el proceso SACM. (ITIL, 2015)

- **Identificación de la configuración**: Este subproceso se ocupa de la selección, identificación, etiquetado y registro de las entidades de crédito. Es responsable de determinar qué CI se registrarán, cuáles son sus atributos y qué relaciones existen con otros CI. Este proceso mantiene la estructura del CMS para que pueda contener toda la información requerida sobre los CI.

  Los atributos potenciales que puede querer capturar incluyen:

  - El identificador de CI único y el tipo de CI: ITIL recomienda que cada CI tenga su número de identificación único.
  - El nombre y descripción del IC.
  - Números de versión, ya que a menudo existen múltiples versiones o versiones del mismo CI
  - Ubicación e información del propietario, para que sepa dónde encontrarla.
  - Estado actual (ordenado, en desarrollo, en producción, etc.)

[7] Base de datos de gestión de la configuración (CMDB), es un repositorio que está diseñado para almacenar muchos de los componentes de un sistema de información.
[8] Sistema de gestión de la configuración (CMS), incluye todas las herramientas para un buen proceso de Gestión de Configuración y Activos del Servicio una de estas herramientas es la CMDB
[9] Biblioteca Definitiva de Medios (DML): repositorio seguro en el que las versiones autorizadas definitivas de todos los medios de comunicación, software, licencia de CIS están almacenados y protegidos

  - Cuando sea necesario, información del proveedor, documentación relacionada, etc.

- **Control de configuración:** El propósito principal es revisar las modificaciones realizadas al Sistema de administración de configuraciones (CMS) para proteger la integridad de la base de datos. Asegura que la información almacenada en el CMS esté completa y que la modificación haya sido realizada únicamente por personal autorizado. Este subproceso se inicia cada vez que se realiza una alteración en la CMDB o en los RFC recibidos del proceso de gestión de cambios.
- **Estado de contabilidad y presentación de informes:** Es el medio de obtener e informar todos los datos actuales e históricos relacionados con cada CI a lo largo de su ciclo de vida. Puede obtener y proporcionar datos sobre las líneas de base de configuración, las últimas versiones de software, el historial de incidentes / cambios de CI y sobre la persona que cambió el estado de CI. (ITIL, 2014)

  Los informes de estado generalmente incluyen cosas como:

  - Un inventario de las entidades de crédito y sus configuraciones de línea de base.
  - Un detalle de cualquier CI no autorizado
  - Actualizaciones sobre cambios recientes o excepciones
  - Una detallada de los activos de hardware y software.
- **Verificación y Auditoría:** Responsable de ejecutar una auditoría para revisar y verificar la existencia de los CI y verificar si están correctamente registrados en la CMDB. También comprueba si hay alguna diferencia entre las líneas de base documentadas y el entorno real al que se refieren.
- **Información de gestión:** Este subproceso garantiza que la integridad de su configuración y los datos de activos se mantengan correctamente.

Como parte del proceso de ITIL, debe realizar copias de seguridad periódicas de CMS y CMDB, mantener registros detallados de las versiones de CI archivadas e históricas y tomar las medidas adecuadas para garantizar la integridad de los datos durante todo el ciclo de vida.

2.5.4.2.Gestión del cambio

Según ITIL, un Cambio es "la adición, modificación o eliminación de cualquier servicio o componente de servicio autorizado, planificado o con soporte que pueda tener un efecto en los servicios de TI". La mayoría de las veces, un cambio es un evento que ha sido aprobado por la autoridad de cambio, se evalúa e implementa a la vez que minimiza el riesgo, ajusta el estado de un elemento de configuración (CI) y agrega valor al negocio y a sus clientes. (ITIL, 2014)

ITIL define diferentes tipos de cambio los cuales se menciona en la siguiente tabla para su mejor comprensión.

Tabla 3. Tipos de Cambio definidos por ITIL v3

TIPO DE CAMBIO	DESCRIPCIÓN
Cambio de emergencia / Cambio urgente	Es uno que debe evaluarse e implementarse lo más rápido posible para resolver un incidente grave. Estos tienden a ser más perturbadores y tienen un alto índice de fallas, por lo que deben mantenerse al mínimo. La definición exacta de un cambio de emergencia debe definirse en la política de gestión de cambios.
Cambio estándar	Uno que ocurre con frecuencia, es de bajo riesgo y tiene un procedimiento preestablecido con tareas documentadas para completar. Estos están sujetos a una aprobación previa para acelerar el proceso de gestión de cambios. Si el tipo de cambio estándar aumenta el riesgo para la organización, puede convertirse en un cambio normal.
Cambio importante	Un cambio que puede tener implicaciones financieras significativas y / o ser de alto riesgo. Tal cambio requiere una

	propuesta de cambio en profundidad con justificación financiera y niveles apropiados de aprobación de la administración. Un cambio en este caso puede cambiar de ser operativo a táctico, o táctico a estratégico y requerir un nivel diferente de autoridad para la aprobación.
Cambio normal	Generalmente requiere un cambio importante en un servicio o en la infraestructura de TI. Un cambio normal está sujeto al proceso completo de revisión de la administración de cambios. Las solicitudes de cambio adicionales pueden incluir: • Cambios en la aplicación • Cambios de hardware y software • Cambios de red • Cambios de documentación • Cambios ambientales

Fuente: Adaptado de (Padmavathy Sankaran, 2017) y (Tucker, 2016)

2.5.5. Operación de servicios.

En esta fase es en la que los servicios aportan un valor al negocio donde el plan de negocios, diseños y mejoras del ciclo de vida del servicio se ejecutan y se evalúan. En esta fase se realizan todas las actividades que son necesarias para la presentación y el soporte de los servicios.

Esta manera de gestionarse incluye el estar atentos y poder cumplir adecuadamente con las peticiones del usuario; la solución de los posibles errores de servicio; la eliminación de los problemas (investigando de sus causas), así como la realización de actividades comerciales por el contacto directo con los usuarios y, por lo tanto, con el cliente. (ITIL, 2014) Para esto ITIL nos brinda cinco procesos a seguir siendo estos:

- **Gestión de eventos**: la gestión de eventos gestiona eventos a lo largo de su ciclo de vida. Este ciclo de vida incluye actividades de coordinación para detectar eventos. Darles sentido y determinar la acción de control apropiada.

- **Gestión de incidencias**: la gestión de incidentes se concentra en restaurar los servicios degradados o degradados inesperadamente a los usuarios lo más rápido posible, a fin de minimizar el impacto en el negocio.
- **Gestión de problemas**: implica el análisis de causa raíz para determinar y resolver las causas subyacentes de los incidentes y las actividades proactivas para detectar y prevenir futuros problemas / incidentes. Esto también incluye la creación de registros de errores conocidos, que documentan las causas raíz y las soluciones para permitir un diagnóstico más rápido, y la resolución en caso de que ocurran más incidentes.
- **Cumplimiento de la solicitud:** es el proceso para administrar el ciclo de vida de todas las solicitudes de servicio. Las solicitudes de servicio se gestionan a lo largo de su ciclo de vida, desde la solicitud inicial hasta el cumplimiento, utilizando registros / tablas de cumplimiento de solicitudes separadas para registrar y rastrear su estado. Son el mecanismo por el cual los usuarios solicitan formalmente algo a un proveedor de servicios de TI Como parte de ese modelo de solicitud, los cambios estándar y otros tipos de solicitudes de cambio (RFC5) pueden ser necesarios para completar las acciones de cumplimiento.
- **Gestión de acceso:** es el proceso de otorgar a los usuarios autorizados los derechos para utilizar un servicio y restringir el acceso a usuarios no autorizados. Se basa en poder identificar con precisión a los usuarios autorizados y luego administrar su capacidad para hacerlo. Acceda a los servicios según sea necesario para su función organizativa o función de trabajo específica. La gestión de acceso también se ha denominado gestión de identidad o derechos en algunas organizaciones.

2.5.5.1.Gestión de eventos

De acuerdo con ITIL v3, un evento se define como la ocurrencia detectable de un cambio de estado y tiene importancia para la administración de la Infraestructura de TI o la prestación de servicios de TI.

El objetivo principal del Proceso de esta gestión es garantizar que los CI y los servicios se supervisen constantemente. Este proceso apunta a filtrar y clasificar los eventos para que se puedan tomar las acciones apropiadas si es necesario. El propósito y el alcance del proceso de este se enumeran a continuación:

- Detectar e investigar cualquier cambio de estado que tenga importancia para la administración de un CI o servicios de TI.
- Proporcionar un medio para la detección temprana de incidentes.
- Decida las acciones apropiadas para los eventos y asegúrese de que se comuniquen a las funciones apropiadas.
- Proporcione el desencadenante, o punto de entrada, para la ejecución de muchas actividades de administración de servicios.
- Proporcionar un mecanismo para comparar el rendimiento operativo real con los estándares de diseño y los SLA.
- Proporcionar una base para la garantía del servicio, la generación de informes y la mejora del servicio.

La Gestión de eventos tiene cuatro subprocesos que operan dentro de esta, las descripciones breves de esos subprocesos se presentan a continuación, seguidos de un diagrama que describe el flujo del proceso de gestión de eventos de ITIL y las actividades:

1. **Monitoreo y Notificación de Eventos**: Se utiliza para configurar y mantener los mecanismos para monitorear eventos, notificar a las partes interesadas y determinar las reglas para el filtrado y la correlación de eventos.
2. **Filtrado de eventos y correlación de 1er nivel**: Se usa para filtrar eventos que son simplemente informativos y se pueden ignorar. También comunica cualquier evento de advertencia y excepción al siguiente nivel.
3. **Correlación de segundo nivel y selección de respuesta**: Este es el subproceso más vital de la Gestión de Eventos. Es responsable de interpretar la gravedad y la categoría de un evento y, a continuación, selecciona una respuesta adecuada si es necesario. Por lo general, implica transferir eventos registrados a otros equipos de soporte de primer nivel.
4. **Revisión del evento y cierre**: Este subproceso se utiliza para verificar si los eventos se han manejado de manera adecuada y garantiza el cierre del evento. También se asegura de que los registros de eventos se analicen para identificar tendencias o patrones, y luego sugiere acciones correctivas si es necesario.

Todos estos procesos para un mejor entendimiento se los muestra en la Figura 6.

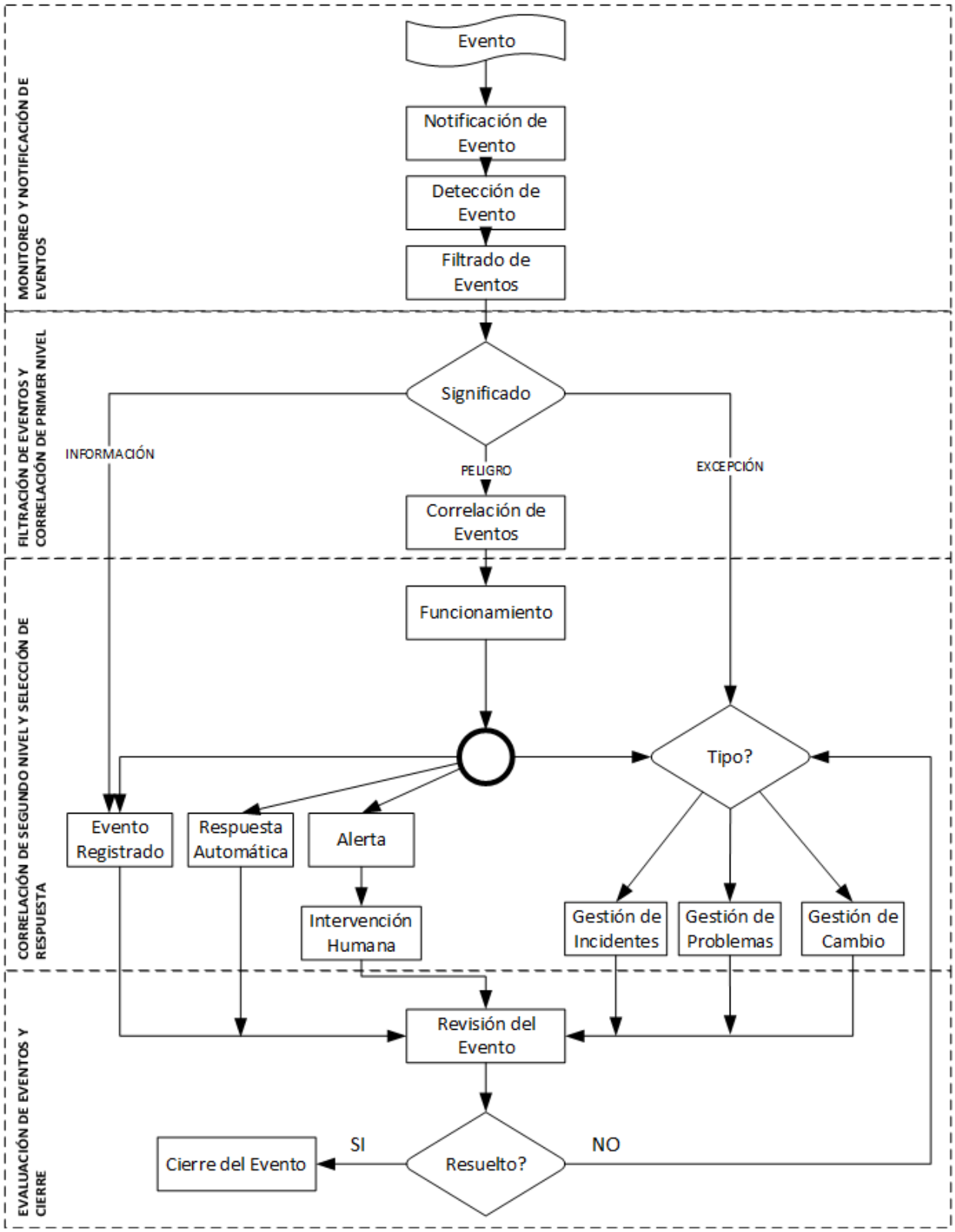


Figura 6. Proceso de gestión de eventos ITIL Flujo y actividades

Fuente: Adaptado de (CERTGUIDANCE, 2018)

2.5.5.2.Gestión de incidencias

Un 'incidente' se define como una interrupción no planificada de un servicio de TI, o una reducción en la calidad de un servicio de TI, o una falla de un CI que aún no ha afectado un servicio de TI (por ejemplo, la falla de un disco de un disco que afecte a un servicio de los implementados en la empresa).

Los incidentes pueden ser reconocidos por el personal técnico, detectados y reportados por las herramientas de monitoreo de eventos, las comunicaciones de los usuarios generalmente a través de una llamada telefónica a la mesa de servicio, o reportadas por proveedores y socios externos. El propósito de la gestión de incidentes es restablecer la operación normal del servicio [10] lo más rápido posible y minimizar el impacto adverso en las operaciones comerciales. Por lo tanto, garantizar que se mantienen los niveles acordados de calidad de servicio.

La gestión de incidentes incluye cualquier evento que interrumpa, o que pueda interrumpir, un servicio. Esto incluye eventos que son comunicados directamente por los usuarios, ya sea a través de la mesa de servicio o a través de una interfaz desde la administración de eventos hasta las herramientas de administración de incidentes. Los incidentes también pueden ser reportados y / o registrados por personal técnico. Por ejemplo, notan algo desfavorable con un componente de hardware o de red que pueden reportar o registrar un incidente y remitirlo a la mesa de servicio.

- Los objetivos que persigue el proceso la gestión de incidencias son:

---

[10] Operación Normal del Servicio: se define como un estado operacional, donde los servicios y los IC se desempeñan dentro de sus niveles de servicio y operacionales acordados con el cliente.

- Asegurar que los métodos y procedimientos estandarizados para una respuesta, análisis, documentación, gestión continua y notificación de incidentes eficientes y rápidos.
- Aumentar la visibilidad y la comunicación de incidentes a las empresas y al personal de soporte de TI.
- Mejorar la percepción empresarial de TI para resolver y comunicar incidentes rápidamente cuando se producen.
- Alinear las actividades y prioridades de gestión de incidentes con las de la empresa.
- Mantener la satisfacción del usuario con la calidad de los servicios de TI.

La priorización de incidentes es el proceso de separar incidentes en función del impacto y la urgencia, una organización puede dividir la prioridad en varios niveles como Alto, Medio, Bajo, etc.

- **Incidente de alta prioridad:** afecta a un gran número de usuarios o clientes, interrumpe el negocio, afecta la entrega del servicio y, por lo general, tiene un impacto financiero.
- **Incidente de prioridad media:** afecta a algunos miembros del personal (o grupo) e interrumpe el trabajo hasta cierto punto. Los clientes pueden verse ligeramente afectados o incomodados.
- **Incidente de baja prioridad:** incidentes menores que no tienen impacto o tienen poco impacto en el usuario individual y tienen soluciones instantáneas.

Cuando pasa por el Ciclo de vida del incidente, el estado del incidente cambia continuamente. A continuación, se muestran los estados y sus breves descripciones que se definen en las pautas de mejores prácticas de gestión de incidentes de ITIL:

Tabla 4. Ciclo de vida del incidente

ESTADO	DESCRIPCIÓN
Nuevo	Este estado indica que la mesa de servicio ha recibido el incidente, pero no lo ha asignado a ningún agente de la mesa de servicio.
Asignado	Este estado indica que el incidente se ha asignado a un agente de la mesa de servicio indi vidual.
En progreso	Significa que un incidente ha sido asignado a un agente y él está trabajando activamente para diagnosticar y resolver el incidente.
En espera	indica que el incidente requiere más información o respuesta del usuario o de un tercero. En este estado, se detiene el conteo de SLA.
Resuelto	Significa que la mesa de servicio ha confirmado que se proporcionó una solución al incidente y que el servicio del usuario se restauró a los niveles de SLA.
Bajo observación	Esto significa que se ha proporcionado una solución a un incidente desde el extremo de la mesa de servicio, y aún están observando la efectividad de la solución. Esto se hace generalmente según la solicitud del usuario, caso por caso.
Cerrado	Este es el estado final, lo que significa que el incidente se resuelve completamente y que no se pueden tomar más acciones.

Fuente: Adaptado de (CHERWELL, 2018)

El marco ITIL describe un proceso de nueve pasos para gestionar incidentes. También llamado ciclo de vida de gestión de incidentes. Esas actividades o pasos se enumeran a continuación en la Figura 7 y generalmente se siguen en el orden secuencial como lo mostrado en la Figura 8:

Figura 7. Detalle del proceso de gestión de incidentes

Fuente: Adaptado de (CHERWELL, 2018)

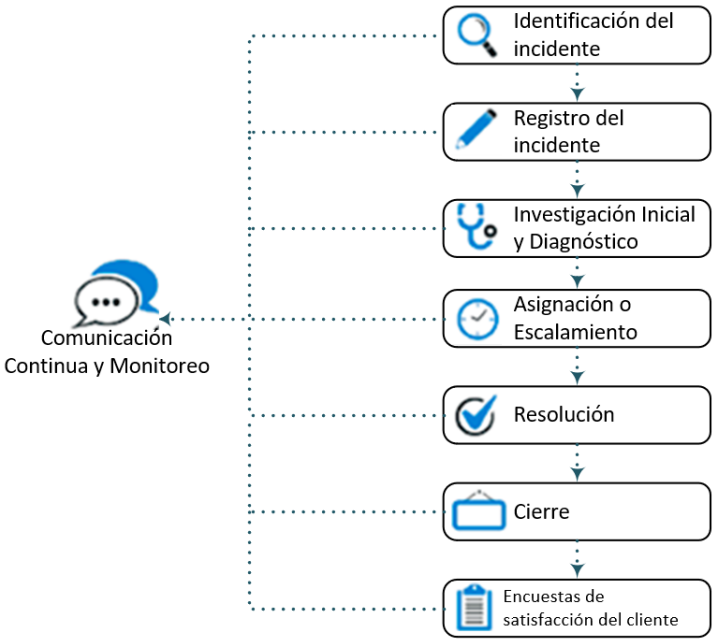


Figura 8. Proceso de Gestión de incidentes

Fuente: Adaptado de (Cherwell, 2018)

2.5.5.3.Gestión de problemas

Para definir principalmente el problema ITIL lo menciona como el origen de uno o más incidentes cuya causa es desconocida. Por lo tanto, la gestión de problemas es el proceso responsable de gestionar el ciclo de vida de un problema.

Los principales objetivos de la Gestión de Problemas son:

- Eliminar incidencias recurrentes.
- Minimiza el impacto de los incidentes que no se pueden prevenir.
- Prevenir los problemas e incidentes derivados de los mismos.

La gestión de problemas trabaja junto con la gestión de incidentes y la gestión de cambios para aumentar la calidad y disponibilidad del servicio.

ITIL en su versión 3 define dos tipos de Tipos de gestión de problemas

1. **Proactivo**: Guiado por el proceso de mejora continua, supervisa el Servicio para detectar problemas antes de que se conviertan en incidentes.
2. **Reactivo**: analiza incidentes y brinda soluciones

La gestión del problema tiene un ciclo de vida basado en siete subprocesos los cuales de los cuales se tiene:

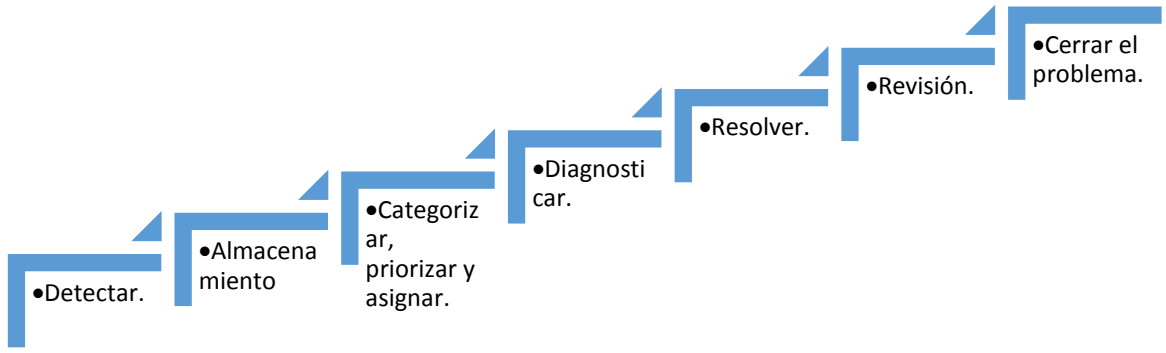


Figura 9. Ciclo de vida de la gestión de problemas

Fuente: Adaptado de (CERTGUIDANCE, 2018)

2.5.5.4.Gestión de acceso

Es el proceso de otorgar a los usuarios autorizados el derecho de usar un servicio mientras se evita el acceso a usuarios no autorizados. El proceso de administración de acceso de ITIL también se conoce como la administración de acceso de usuarios de ITIL o el proceso de administración de identidad.

El objetivo principal es otorgar a los usuarios autorizados el derecho a utilizar un servicio y, al mismo tiempo, evitar el acceso a usuarios no autorizados. Algunos otros objetivos importantes de este proceso de administración de acceso de usuarios son los siguientes:

- Administrar el acceso a los servicios según las políticas y acciones definidas en Information Security Management.

- Procesar cualquier solicitud para otorgar acceso a los servicios, cambiar los derechos de acceso, restringir el acceso y garantizar que los derechos que se proporcionan o modifican se otorgan correctamente.
- Conceder acceso a servicios, datos o funciones, solo si están autorizados para obtener ese acceso.
- Administrar el acceso a los servicios, evite el uso indebido de los derechos de acceso y elimine el acceso cuando las personas cambian de roles o trabajos.
- Ayudar a proteger la confidencialidad, integridad y disponibilidad de los servicios, activos, instalaciones e información de la organización.

ITIL v3 define muy claramente la jerarquía de procesos para el control de acceso, indicando que el acceso debe otorgarse de acuerdo con las reglas establecidas por la Política de seguridad de la información. El proceso de ITIL Access Management no define ni modifica ninguna política; Simplemente sigue la política existente.

La gestión de acceso del usuario define seis pasos o actividades que se enumeran a continuación y, por lo general, se siguen de forma secuencial:

Figura 10. Ciclo de vida de la gestión de acceso

Fuente: Adaptado de (CERTGUIDANCE, 2018)

2.5.6. Mejora continua del servicio (CSI).

La mejora continua del servicio es la quinta y última etapa del ciclo de vida de ITIL. Esta ayuda a identificar las oportunidades de mejora al vigilar las diversas aplicaciones y procesos de servicio introducidos durante las diferentes fases del ciclo de vida de ITIL. Una vez que el servicio de TI se selecciona, diseña, construye y mantiene, el trabajo de perfeccionamiento continuo del servicio, es apoyar y mejorar los servicios y procesos.

CSI se centra en aumentar la eficiencia y la rentabilidad de los servicios de TI entregados al cliente. Supervisa y mide el rendimiento del proveedor de servicios de TI. Confirma que los servicios de TI están alineados con las necesidades cambiantes del negocio al identificar e implementar formas de mejora del servicio que respalden los procesos del negocio.

El plan de mejora continua del servicio incluye un proceso de siete pasos en el que las actividades se llevan a cabo en varias etapas del ciclo de vida del servicio, este proceso se sigue secuencialmente como se indica a continuación:

1.Identifique y defina la strategia de mejora:	•Identifica la visión general, los requisitos del negocio, la estrategia y los objetivos.
1.Definir qué medir:	•La estrategia de servicio de ITIL y el diseño del servicio identifican y definen los puntos de referencia de rendimiento para procesos o servicios.
1.Recopilar los datos:	•Recopila datos sin procesar del entorno real (es decir, la fase de operación del servicio) para el procesamiento y análisis.
1.Procesar los datos	•Se procesa los datos recopilados para darle un contexto (conversión a información) para que esos datos puedan ser analizados.
1.Analizar los datos recopilados	•Análisis de la información para obtener información lógica sobre la tendencia de la operación comercial y responder a la pregunta "¿Dónde queremos estar?".
1.Presente y utilice la información:	•Se busca la respuesta a "¿Cómo llegamos allí?" Y se comunica información sobre las distintas partes interesadas.
1.Implementar mejoras	•Responsable de la implementación real del plan de mejoras. Este paso aplica el cambio requerido, la optimización y las acciones correctivas en los procesos o servicios identificados.

Figura 11. Proceso del CSI

Fuente: Adaptado de (CERTGUIDANCE, 2018)

Además, este proceso muestra también un “Ciclo Deming” (planificar-hacer-verificar-actuar), el cual es un método de administración iterativo de cuatro pasos que se utiliza en los negocios para el control de calidad y la mejora continua de procesos y producto.

Basándonos en los siete pasos de la mejora continua podemos definir el ciclo Deming de la siguiente manera:

- Con los pasos 1 y 2 se proporciona la respuesta a la primera pregunta del enfoque de CSI "¿Qué es la visión?". Y estos pasos están alineados con la etapa del "Planificar" del Ciclo Deming.
- Para complementar la etapa "Hacer" del ciclo de Deming se necesitan los pasos 3 y 4 para responder la pregunta "¿Dónde estamos ahora?".
- La etapa de “verificación” se la realiza con los pasos 5 y 6.

- Finalmente, la etapa “Actuar” se complementa con el paso numero 7 el cual proporciona la respuesta a las preguntas "¿Llegamos allí?" Y "¿Cómo mantenemos el impulso?".

En la Figura 12 se muestran los siete pasos de CSI y su mapeo con los “Enfoques de CSI” y las etapas de “Ciclo Deming” (Planificar-Hacer-Verificar-Actuar).

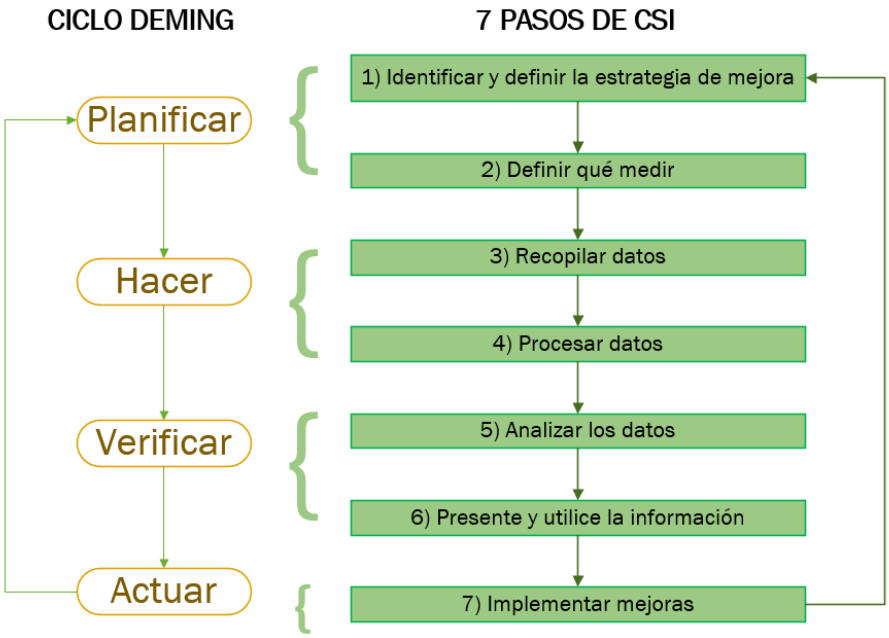


Figura 12. Los 7 pasos de CSI, y ciclo Deming

Fuente: Adaptado de (CERTGUIDANCE, 2018)

2.6.Relación de ITIL y el modelo funcional FCAPS

ITIL en su versión 3 muestra un “manual de buenas prácticas” el cual a su vez tiene relación con el modelo funcional de la ISO (FCAPS), para su mejor entendimiento se realiza un análisis de las FCAPS desde una perspectiva de ITIL, como se muestra en la Tabla 5.

Tabla 5. Relación FCAPS e ITIL

FCAPS	Función de ITIL
Gestión de Fallos Incluye la detección, aislamiento y resolución de problemas de red Ayuda a asegurar una óptima experiencia de usuario, reducir el tiempo de inactividad, degradaciones de rendimiento inaceptables y el tiempo medio para resolver la avería.	Dentro de ITIL se define la fase **Operación de servicios y los procesos de Gestión de Eventos y Gestión de incidentes**. El proceso de **Gestión de eventos** permite detectar y dar sentido a los fallos existentes, permite determinar la acción de control apropiada, además permite actuar como base para el aseguramiento del servicio, la presentación de informes y la mejora del servicio. El proceso de **Gestión de incidentes** ayuda a identificar cualquier interrupción en un servicio normal con el objetivo de restablecer el servicio lo antes posible, incluyendo la priorización de in incidente, la asignación y su resolución o escalamiento a otro nivel.
Gestión de Configuración Esta gestión tiene las funciones de: Recolectar y almacenar la información de red y la configuración del sistema. La información de configuración incluye elementos de hardware, software y programación. Ejemplo: Un enrutador Cisco, IOS y la puesta en marcha y configuración en ejecución. Se hace referencia como elemento de configuración (CI) en ITIL	Dentro de ITIL se define la fase **Transición de servicio** y en sus procesos: **Gestión de cambio y Gestión de activos y configuración de servicios**, dentro de los cuales se define el proceso desde la adquisición de las unidades, su configuración inicial, y mejora de los servicios durante las fases de Operación del Servicio y Mejora Continua,
Gestión de Contabilidad Facilita una mejor distribución de los recursos Mide el uso de recursos Ayuda a reducir los costes de explotación y Establece un mejor control de red	Se define en la fase de **Estrategia del servicio** en el proceso de **Gestión financiera** donde se realiza un análisis financiero En la fase de **Diseño de servicio** dentro del proceso **Gestión de Nivel de Servicio** en el cual se define el nivel de uso del equipo es decir si un servicio es utilizado sólo por un equipo en particular.

	En la fase **Operación de servicio** y en el proceso **Administración de aplicaciones**, se define si estos servicios están disponibles para todos los usuarios de toda empresa. Por ejemplo, el servicio de correo electrónico
Gestión de Rendimiento Área definida para entender el estado de la red actual y la eficiencia, ayuda a preparar la red para el futuro, incluye la medición de diversos parámetros de rendimiento y asegura la disponibilidad del servicio y el rendimiento a un nivel óptimo	Dentro de ITIL en la fase de **Diseño de servicio** se define la **Gestión de capacidad y disponibilidad**. En la fase **Operación de servicio** se habla de una gestión técnica y de aplicaciones. La fase de **Mejora continua del servicio** ayuda a mejorar la calidad del servicio, incluyendo la estandarización y análisis del rendimiento alcanzado por la red.
Gestión de Seguridad: Mantiene la confidencialidad de la información de usuario y de negocio. Incluye la protección de la red de usuarios no autorizados, controla las actividades generales y asegura la seguridad de los datos a través de la autenticación y cifrado	En la fase de **Diseño de servicio** el proceso de **Gestión de la seguridad** protege la disponibilidad, confidencialidad e integridad de la información. Dentro de la **Operación de servicio** el proceso **Gestión de acceso** controla el nivel y grado de funcionalidad o datos que un usuario tiene derecho a utilizar.

Fuente: Adaptado de (ITIL, 2014), (ISO, 2015), (Rouse, 2007), (Padmavathy Sankaran, 2017), y (Rizos, Introduction to FCAPS – Fault, Configuration, Accounting, Performance, Security, 2016)

2.7.Sistemas de gestión de configuración.

En la actualidad se pueden encontrar diferentes sistemas que permiten realizar el registro de activos y un registro de tickets, muchos de ellos se enfocan en solventar una de las dos características, entre los que proporcionan soporte para gestión de configuración en cuanto a la gestión de activos y de tickets podemos hablar de tres grandes herramientas como son OCS Inventory, ITOP y GLPI.

2.7.1. OCS Inventory

Fuente: (OCS Inventory, 2019)

Su nombre proviene de las siglas en ingles de Open Computers and Software Inventory que en su traducción al español es Inventario de Computadoras y Software Abierto, siendo ésta una herramienta creada con la finalidad de brindar una gestión de manera técnica para equipos informáticos. Desde sus inicios OCS Inventory se ha enfocado en el inventario tanto de software como de hardware.

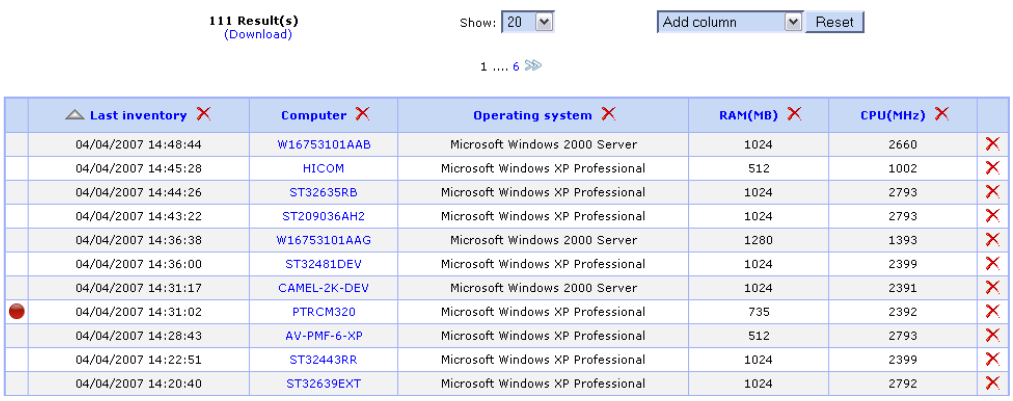
OCS Inventory cuenta con agentes que envían información de software y hardware al servidor, en intervalos de tiempo, también sondean la red en busca de nuevos elementos activos que no pueden aceptar agentes usando el escaneo mediante SNMP.

El objetivo principal que persigue esta herramienta es recopilación completa de datos por Ipdiscover. El escaneo mediante protocolo SNMP permite la recopilación de información de todo tipo de equipamiento que soporte este protocolo, como son: computadores, impresoras,

Routers, Switch, Acces Point, entre otros. Los escaneos mediante una red SNMP se los realiza mediante escaneos IP.

Entre las funcionalidades principales que se puede destacar de la herramienta se tienen:

Funcionalidad de inventario: OCS permite una comunicación cliente servidor de tal manera que el agente envía la información al hacia el gestor, para ser almacenada esta información, mientras que mediante una interfaz web el usuario puede ver estos resultados de inventario de hardware y software detectado.



111 Result(s) (Download) Show: 20 Add column Reset 1 6

Last inventory	Computer	Operating system	RAM(MB)	CPU(MHz)
04/04/2007 14:48:44	W16753101AAB	Microsoft Windows 2000 Server	1024	2660
04/04/2007 14:45:28	HICOM	Microsoft Windows XP Professional	512	1002
04/04/2007 14:44:26	ST32635RB	Microsoft Windows XP Professional	1024	2793
04/04/2007 14:43:22	ST209036AH2	Microsoft Windows XP Professional	1024	2793
04/04/2007 14:36:38	W16753101AAG	Microsoft Windows 2000 Server	1280	1393
04/04/2007 14:36:00	ST32481DEV	Microsoft Windows XP Professional	1024	2399
04/04/2007 14:31:17	CAMEL-2K-DEV	Microsoft Windows 2000 Server	1024	2391
04/04/2007 14:31:02	PTRCM320	Microsoft Windows XP Professional	735	2392
04/04/2007 14:28:43	AV-PMF-6-XP	Microsoft Windows XP Professional	512	2793
04/04/2007 14:22:51	ST32443RR	Microsoft Windows XP Professional	1024	2399
04/04/2007 14:20:40	ST32639EXT	Microsoft Windows XP Professional	1024	2792

Figura 13. Inventario realizado en OCS Inventory

Fuente: (OCS Inventory, 2019)

Extensiones de inventario OCS: permite que se ejecuten nuevos scripts de Windows o de Unix para la recuperación de información, y enviarla al servidor el cual de igual manera puede crear nuevas extensiones que le permitan almacenar información útil dentro de su base de datos, usando un código en lenguaje Perl integrado para la comunicación y mostrando está en una interfaz basada en PHP.

El descubrimiento de la red y sus materiales se la realiza en dos etapas primero el módulo de búsqueda por IP detecta un hardware en la red, identifica la red a la que se debe analizar, luego mediante el protocolo de resoluciones de direcciones ARP, y almacena todas estas IP correspondientes al segmento de red dentro de un archivo de inventario, el cual es

enviado al servidor: Posteriormente la exploración mediante SNMP para recuperar información diversa de los dispositivos de red conectados.

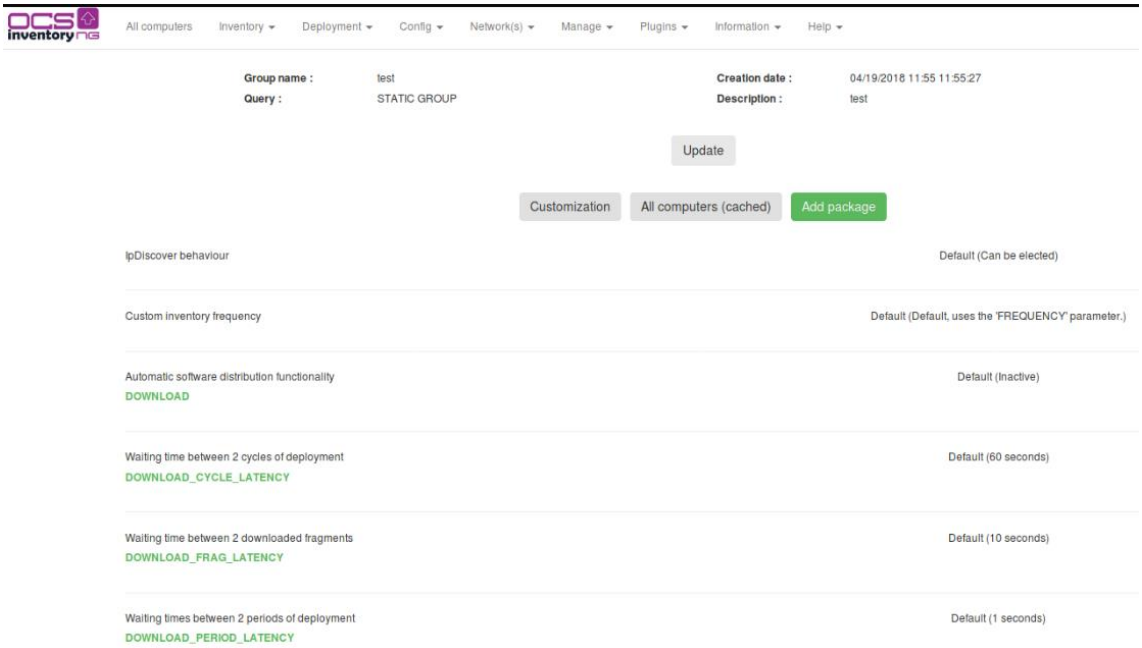


Figura 14. Descubrimiento automático con OCS Inventory

Fuente: (OCS Inventory, 2019)

Este es un software es multiplataforma por lo cual se puede instalar en un computador con Windows 95 o superior, en cualquier distribución de Linux e inclusive MacOS X

2.7.2. iTop

Fuente: (iTop, 2018)

iTop proviene del término en ingles IT Operational Portal que significa Portal Operacional de TI, siendo esta una aplicación de código abierto diseñada para las operaciones en servicios de TI. Esta herramienta se diseñó basado en los procesos de ITIL por lo cual es una herramienta muy adaptable a sus procesos.

La base de iTop es una CMDB por lo que la herramienta se enfoca en el registro de equipamiento activo de TI, aunque también tiene incorporado la gestión de tickets y varios procesos derivados estos no son su fuerte y son muy limitados (iTop & Combodo, 2019).

Entre sus principales características se mencionan las siguientes:

Documentar la infraestructura de TI y toda la infraestructura relacionada como es el caso de servidores, aplicaciones, dispositivos de red, máquinas virtuales, ubicaciones, entre otros.

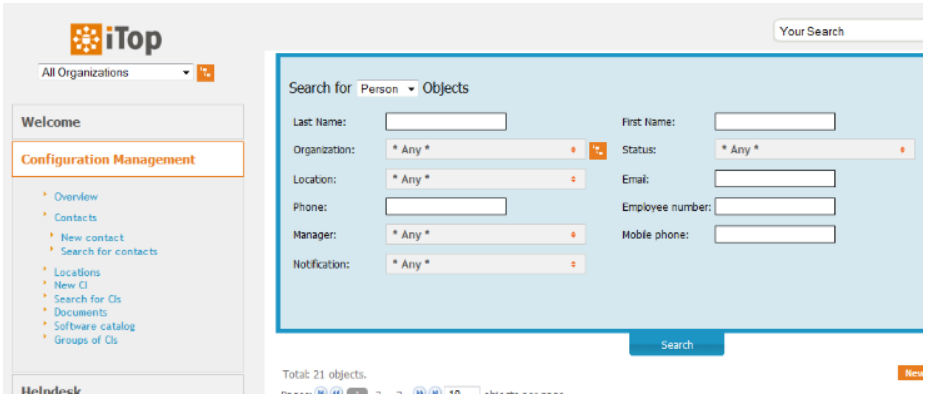


Figura 15. Registro de activos iTop

Fuente: (iTop, 2018)

iTop permite además la gestión de incidencias, peticiones de usuarios y paradas planificadas.

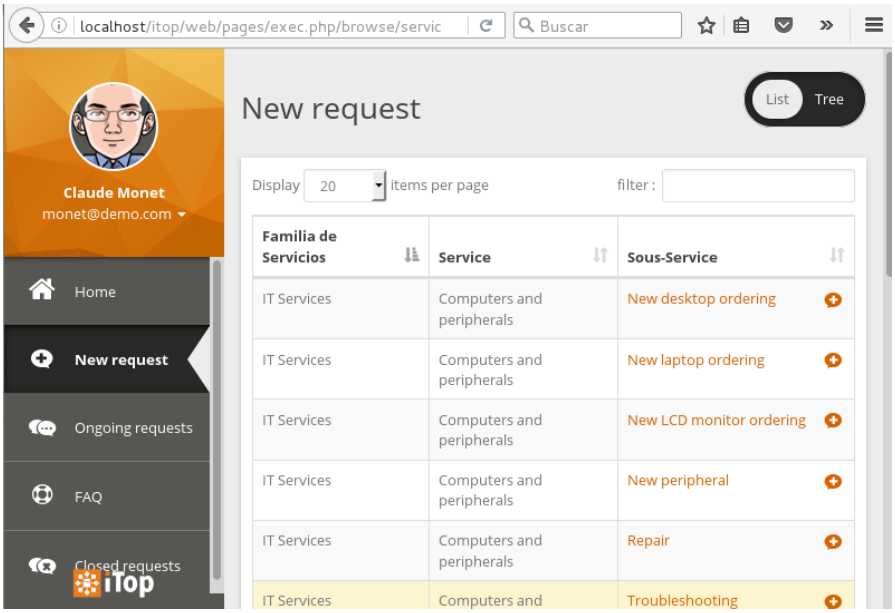


Figura 16. Registro de tickets iTop

Fuente: (iTop, 2018)

La documentación de los servicios de TI y contratos con los proveedores externos y sus condiciones a nivel de servicio.

La importación y exportación de información de forma manual o usando scripts es posible con esta herramienta (iTop & Combodo, 2019).

iTop puede ser utilizado por ingenieros de soporte, gerentes de servicio e incluso por los usuarios finales gracias a la interfaz web que permite realizar y responder solicitudes.

iTop tiene cuatro versiones, la versión gratuita que no permite la creación y actualización de tickets de manera libre, sino más bien está restringido a una cantidad de 4 cambios y generación de 8 tickets por semana y dependiendo el tipo de producto de iTop se obtendrán mejores beneficios los mismos se los puede encontrar en su web oficial de iTop. (iTop & Combodo, 2019).

iTop para su instalación necesita algunos recursos de software previamente instalados y como es el caso de Apache / IIS, MySQL y PHP.

En cuanto a sistema operativo, iTop se ejecuta en cualquiera que soporte dichas aplicaciones. Esta aplicación permite su instalación en Windows, Linux (Debian, Ubuntu y Redhat), Solaris y MacOS X.

2.7.3. GLPI (Gestionnaire Libre de Parc Informatiqué)

Fuente: (GLPI Project, 2018)

GLPI es una herramienta de software libre que permite una gestión de inventario informático y además permite un soporte técnico (Help Desk). Este sistema muestra una interfaz web que permite abarcar los principales problemas en la gestión de inventarios informáticos:

Entre sus principales funciones se encuentran:

Compatibilidad con ITIL: de tal manera que permite una escalabilidad, categorización, calcular priorización, además de tener una validación en varios niveles y la implementación de trabajos automatizados basados en las políticas de la organización (GLPI Project, 2018).

Manejo de activos e inventario automático de TI: permite además de su registro un inventario de bienes computadores, equipos de red, impresoras dispositivos e incluso teléfonos, además de una vista detallada de cada elemento registrado sus conexiones y la ubicación de red de cada componente, además permite obtener un historial completo de las modificaciones de cada modificación realizada, (GLPI Project, 2019)así también incluye un inventario de componentes de red de manera detallada en cuanto a conexiones remotas incluyendo

información como IP, MAC, Vlans , entre otras, a través de protocolo local o a través de detección por las redes usando plugin FusionInventory u OCS Inventory.

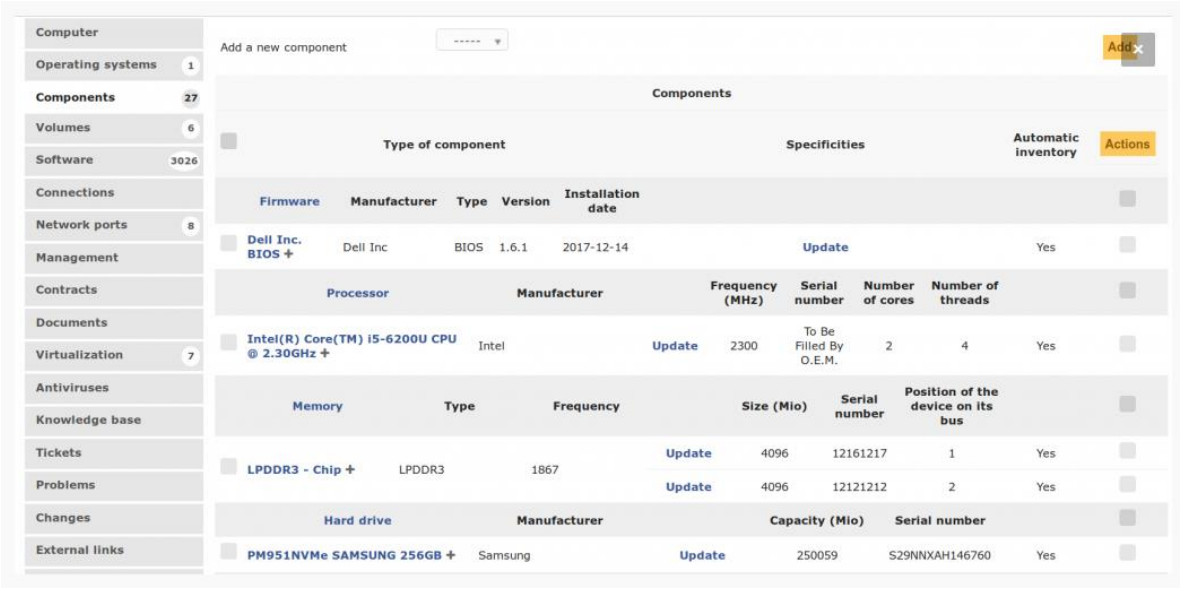


Figura 17. Registro de equipamiento activo con GLPI

Fuente: (GLPI Project, 2018)

Inteligencia para control de calidad de la información: GLPI permite mejorar la labor de los gerentes al momento de realizar estadísticas, permitiendo declarar reglas de control que permitan demostrar que los bienes son únicos, para evitar actualización de dato e incluso la duplicidad de los mismos.

Manejo administrativo y financiero de los activos de TI: el sistema permite el ingreso de fechas correspondientes al ciclo de vida de un bien de tal manera que se puedan tomar acciones previas o posteriores a la culminación de la misma, además se permite llenar información de garantías de los dispositivos mostrando alertas cuando estas estén caducadas, así también información requerida para el manejo de bienes en cuanto a proveedores y contratos realizados, e incluso permite almacenar documentos que sean asociados a estos como es el caso de facturas, notas de entrega y documentación técnica necesaria.

Figura 18. Registro de garantías en GLPI

Fuente: (GLPI Project, 2018)

Inventario automatizado y administración de licencias: combinando GLPI con las herramientas FusionInventory u OCS Inventory se puede compactar como una herramienta muy robusta para la obtención de información de hardware y de software e incluso de licencias.

Figura 19. Registro e inventario de software en GLPI

Fuente: (GLPI Project, 2018)

Estadísticas y reportes: GLPI provee estadísticas de inventarios, y de mesa de ayuda de manera gráfica para tener estadísticas del funcionamiento e incluso del reporte de peticiones que se han realizado en cuanto a los fallos, actualizaciones o incluso de registro de equipamiento.

Figura 20. Reporte estadístico generado en GLPI

Fuente: (GLPI Project, 2018)

Integración profunda: GLPI proporciona un control de acceso y autenticación, mediante servidores LDAP, servidores de correo electrónico e inclusive directorios activos. Esta integración permite crear reglas para el acceso de los usuarios, y mostrar cierta información dependiendo el tipo de usuario.

Inventario: permite realizar un inventario automatizado de los sistemas operativos, de máquinas físicas, virtualización y contenedores, siendo este inventario mediante descubrimiento o mediante inclusión de información de manera manual.

GLPI cuenta con una versión completamente libre y código abierto, en caso de necesitar soporte directo con GLPI Project en cuanto a la utilización de la herramienta y la instalación de nuevos plugin para complementar la herramienta se puede acceder a una versión de suscripción anual, dependiendo las características que se deseen contratar. Cabe recalcar que GLPI en su versión libre no cuenta con ninguna limitante para su uso, así como también se puede acceder al soporte por medio de la comunidad.

2.7.3.1.Elementos necesarios para su instalación

En cuanto a hardware es necesario contar con las siguientes características para una instalación mínima (GLPI Project, 2019):

- 250 MBs de memoria RAM
- 5 GB de Disco Duro libres (luego de instalación del sistema operativo)
- Procesador 1 GHz (Pentium individual) como mínimo

Al tratarse de Software GLPI necesita los siguientes elementos (GLPI Project, 2019):

- Sistema operativo: cualquier distribución de software libre, de preferencia Debian 4.1 o superior.
- Al tratarse de GLPI como una aplicación web, es necesario tener previamente instalado un servidor web como es el caso de Apache 2 o una versión más reciente o Nginx, además PHP 5.6 o su versión más reciente.
- Para su almacenamiento de información es necesario una base de datos como: MySQL 5.6 o superior, o MariaDB 10.0 o su versión más actual.
- Para un control remoto es necesario habilitar SSH, FTP, y protocolos que permitan esta conectividad.

2.7.4. Relación de los sistemas de configuración

En la Tabla 6, se observa una comparativa de las principales características y elementos necesarios de los sistemas mencionados anteriormente.

Tabla 6. Comparativa de sistemas de configuración

Detalle	**OCS Inventory**	**ITop**	**GLPI**
Ultima Versión	2.3 lanzada el 12 de enero del 2017	2.6.1lanzada el 10 de abril del 2019	9.5.4 lanzada el 18 de diciembre del 2019
Licencia	Libre y de pago	Libre y de pago	Libre
Versión de PHP necesaria	Mínimo 5.0 o más reciente	Mínimo 5.6. Recomendado 7.0, 7.1 o 7.2 No funciona con 7.3	Mínimo PHP 5.6. Recomendado la versión 7.0 o superior
Base de datos	MySQL 5.4 o MariaDB 10	Mínimo MySQL 5.6 o MariaDB 10.1. Recomendado MySQL 5.7 o MariaDB 10.2. No funciona con MySQL 8	MySQL 5.6, o MariaDB 10 o versiones más recientes
Servidor web necesario	Apache 2	Apache 2	Apache 2
Sistema operativo compatible	Multiplataforma (GNU/Linux, Unices, Windows, otros)	Windows, Linux	Windws, Linux
Soporte	Directo bajo suscripción	Blogs comunitarios y soporte directo bajo suscripción	Blogs comunitarios y soporte directo bajo suscripción

Fuente: Adaptado de (GLPI Project, 2018), (iTop, 2018), (OCS Inventory, 2019)

CAPÍTULO III. SITUACIÓN ACTUAL

En este capítulo se muestra información referente a la red que maneja Yachay E.P. dando una vista general de la denominada Ciudad del conocimiento "Yachay", se muestra información referente al registro de equipamiento de red que la UOTSHPC maneja en la actualidad, así como también del registro de tickets y todo el proceso a seguir para dar solución a los eventos e incidencias registrados. Por otra parte, se muestra además información de la red física y también de la red lógica que maneja la DOTSHPC en específico la UOTSHPC enfocado en la red Data Center e incluyendo además el área de networking del Super Computador, mismas que sirven como referencia para la implementación del sistema.

3.1. Ubicación

La Empresa Pública Yachay E.P. se encuentra ubicada en el cantón San Miguel de Urcuquí, perteneciente a la Región zonal 1 (Imbabura, Carchi, Pichincha Norte, Esmeraldas y Sucumbíos), localizado al noroccidente de la provincia de Imbabura de la Republica del Ecuador. (Yachay, 2018)

Yachay E.P., es una Empresa Pública ecuatoriana, creada el 13 de marzo del 2013, y legalmente encargada del proyecto denominado "Ciudad del Conocimiento Yachay", misma que persigue la misión de "generar un ecosistema para impulsar la conversión del Ecuador hacia una economía basada en la generación de conocimientos e innovación",

3.2.Ciudad del conocimiento Yachay

Esta es la primera ciudad planificada del Ecuador, esta ciudad fue creada con la finalidad de potenciar el desarrollo de investigación y aplicativos tecnológicos que impulsen de mejor manera el buen vivir de todos los habitantes tanto de la ciudad como del país.

Figura 21. "Ciudad del Conocimiento" Yachay

Fuente: Yachay.gob.ec

Yachay es un ecosistema de innovación para generar y potenciar los emprendimientos de base tecnológica y los negocios intensivos en conocimiento. La nueva ciudad combina las mejores ideas, talento humano e infraestructura de punta. La denominada “Ciudad del Conocimiento Yachay” está conformada por diferentes sectores como son:

- Data Center
- Centro de Emprendimiento
- Hacienda San Eloy
- Instituto Superior 17 de Julio
- Universidad Yachay Tech,
- Bloques de residencias

- Hoja Blanca
- Mercado las Manuelas
- Centro Infantil del Buen Vivir.
- El Rosario
- Ingenio San José

3.3. Estructura orgánica de Yachay E.P.

La Empresa Pública Yachay E.P. en su estructura organizacional cuenta diferentes gerencias entre las que podemos destacar la Gerencia Técnica, misma que se encarga de: gestionar, monitorizar, controlar y dirigir todos los procesos relacionados con la infraestructura física y lógica de la empresa, esta cuenta con diferente subgerencias, direcciones y unidades para el cumplimiento de sus actividades.

En la Figura 22, se observa la estructura en cuanto a la parte organizacional de la Empresa pública Yachay E.P. dentro de la cual nos centraremos principalmente en la Dirección de Operaciones Tecnológicas y Servicios HPC (DOTSHPC), que está comprendida dentro de la gerencia técnica.

La DOTSHPC cuenta con la Unidad de Operaciones Tecnológicas y Servicios HPC (UOTSHPC), misma que es la encargada de monitorizar, controlar, dirigir, y solventar todas las necesidades referentes al servicio del super computador (HPC) y del servicio de Internet e intranet en la Empresa Pública y en sus diferentes sectores que la conforman.

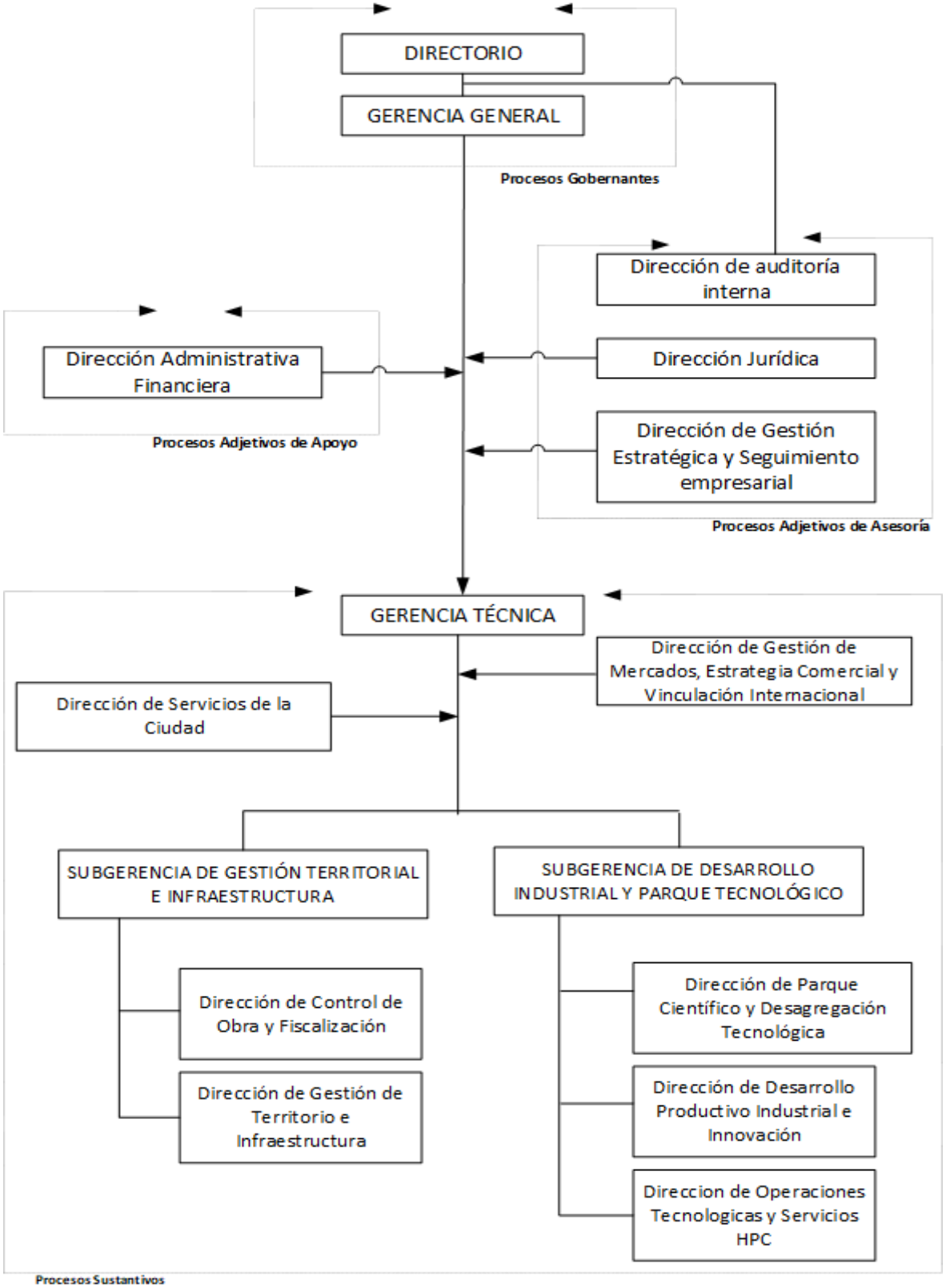


Figura 22. Estructura Orgánica de la Empresa Pública Yachay E.P.

Fuente: (Yachay E.P., 2019)

3.4.Portafolio de servicios

La DOTSHPC tiene como portafolio los servicios y sub servicios a su cargo mismos que son mostrados en la Tabla 7, los cuales cuentan con un operador propietario y un operador de backup, para la gestión necesaria que se realice en cada sub servicio. Todos estos servicios están disponibles para los funcionarios de la empresa dependiendo su área y cargo.

Tabla 7. Portafolio de Servicios de Yachay E.P.

SERVICIOS	SUBSERVICIOS
DATA CENTER	Incendios Control de accesos Ventilación y aire acondicionado Energía Video seguridad
RED	WAN, MAN, LAN, MPLS, etc. Wlan Internet (enlaces de Internet y datos) DHCP DNS
SEGURIDAD	Seguridad perimetral Antivirus Antispam Acceso remoto Certificados SSL Proxy web
INFRAESTRUCTURA	Virtualización de servidores - Cloud Computing Storage
BACKUP Y STORAGE	File server Cloud box
PRODUCTIVIDAD Y COLABORACIÓN	Mail Active Directory Telefonía IP / cisco jabber

SISTEMAS ADMINISTRATIVOS	Sistema financiero Intranet Content management OTRS
HPC	LAN Infiniband SCF LSF GPFS Aplicaciones WEB (hpc.yachay.gob.ec)
WEB	Quipux Inventario Sistema de viajes Sistema del IESS Sistema Ruter
SUBSISTEMAS ELECTRÓNICOS	Biométricos. Video seguridad
SOPORTE	Impresoras Equipos tecnológicos Mantenimiento equipos tecnológicos
SISTEMAS DE INFORMACIÓN	Yauth Yforms Ysigmapas Ytthh Base de datos Giltab Wildfly Regece Integración continua Aplicaciones móviles Desarrollo de software Despliegue de aplicaciones en contenedores Gestor de proyectos ágiles (Taiga) Gestor de proyectos de la Empresa (Y monitor)

Fuente: DOTSHPC

3.5.Registro de equipamiento de red

Yachay E.P. al ser una Empresa Pública está sujeta al ejercicio de diferentes normas gubernamentales, entre ellas se encuentra la "Normativa de control interno de la contraloría general del estado" (Contraloria General del Estado, 2009) vigente hasta la actualidad, en la que se trata sobre normas para el control interno la cual está dirigida a entidades y organismos del sector público y además para personas del sector público o privado que dispongan de recursos públicos.

De acuerdo con el art. 410-09 del Reglamento Administración y Control de Bienes del Sector Público, sobre el "mantenimiento y control de la infraestructura tecnológica" en los literales 6 y 7 se menciona:

"6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad." (Contraloria General del Estado, 2009)

"7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables." (Contraloria General del Estado, 2009)

Donde, haciendo uso del literal 7, la Empresa Pública Yachay E.P. se ve en la obligación de mantener un inventario informático detallado ayudando a cumplir las funciones detalladas en el literal 6, sobre el mantenimiento de la infraestructura.

Además de esta normativa Yachay E.P. haciendo ejercicio del artículo 4 del reglamento general para la administración y control de bienes y existencias del sector público, modificado el 06 de julio del 2016; ha implementado su propia reglamentación relativa a la administración, uso y control de los bienes mueves e inmuebles que constituyen el patrimonio de la Empresa Pública "Yachay E.P." (Yachay E.P., 2016).

En el reglamento interno para la administración, utilización y control de bienes existentes de la Empresa Pública "Yachay E.P.", sección dos, capitulo tres sobre el registro de los bienes en el artículo 18, dice que el guardalmacén llevara un registro administrativo y contable.

Así también en el mismo reglamento interno en la sección tres capitulo uno de los equipos informáticos, en el artículo 29 de las obligaciones de la dirección de soporte y operaciones tecnológicas literal b "Mantener una lista actualizada e inventario propio del conjunto de equipos informáticos de la institución. El registro deberá contener las especificaciones técnicas del equipo." (Yachay E.P., 2016).

Actualmente la Empresa Pública Yachay E.P. a pesar de contar con estas normativas, cuenta con el registro administrativo y contable, pero dentro de la UOTSHPC se cuenta únicamente con un registro manual del equipamiento realizado en hojas de cálculo de Excel, mismo que no incluye toda la información necesaria para el cumplimiento de esta reglamentación, un ejemplo de este registro se muestra en la Figura 23, donde los parámetros que se incluyen en estas hojas de registros son: número de ítem, sector de ubicación, tipo de dispositivo, modelo, marca, cantidad, descripción, hostname, número de serie, versión, IOS, MAC, modulo / puerto, ubicación actual, estado de funcionamiento, numero de

contrato / proyecto, observaciones de contrato / proyecto, observaciones del equipo, código del registro en Yachay E.P. y la IP

Estos parámetros pueden ser fácilmente manipulados, pudiendo incluso ser desactualizados en caso de algún cambio no registrado en estas hojas de Excel, además el registro no cuenta con el parámetro de técnico responsable ni de una completa información de los parámetros previamente mencionados. Esta información se puede validar en una hoja detallada en el ANEXO 1.

ÍTEM	SECTOR	DISPOSITIVO	MODELO	MARCA	CANT.	DESCRIPCIÓN
11	DCU	Switch de Core	CISCO C6807-XL	CISCO	1	Catalyst 6807-XL 7-slot chassis, 10RU
12	DCU	Módulo 16 Puertos	WS-X6816-10G-2TXL	CISCO	1	16 Port 10G with DFC4XL (Slot 1)
13	DCU	Card	WS-F6K-DFC4-EXL	CISCO	1	Catalyst 6500 Dist Fwd Card DFC4XL
14	DCU	Módulo SFP	X2-10GB-LR	CISCO	1	10GBASE-LR Module

HOSTNAME	SERIAL NUMBER	VERSION	IOS
CSW-UCQ-YACHAY-DC-01	SM 05R	15.1(2)SY4a	s2t54-ADVIPSERVICESK9-M
S/N	SA 3DZ		
S/N	SA J54		
S/N	SP 2G7		

MAC	MODULO / PUERTO	UBICACIÓN ACTUAL	ESTADO	CONTRATO / PROYECTO
		DATA CENTER URCUQUÍ - YACHAY 2 IT02 - RACK 13	Operativo	Contrato Yachay EP No. 0147-2014 Proyecto DataCenter/ Canje de deuda
		DATA CENTER URCUQUÍ - YACHAY 2 IT02 - RACK 13 (Insertado en Switch 6807-XL)	Operativo	Contrato Yachay EP No. 0147-2014 Proyecto DataCenter/ Canje de deuda
		DATA CENTER URCUQUÍ - YACHAY 2 IT02 - RACK 13 (Insertado en Switch 6807-XL)	Operativo	Contrato Yachay EP No. 0147-2014 Proyecto DataCenter/ Canje de deuda
	Te1/1	DATA CENTER URCUQUÍ - YACHAY 2 IT02 - RACK 13 (Insertado en Switch 6807-XL)	Operativo	Contrato Yachay EP No. 0147-2014 Proyecto DataCenter/ Canje de deuda

Figura 23. Registro de equipos de telecomunicación

Fuente: DOTSHPC

3.6.Registro de eventos e incidencias

Para el registro de incidencias Yachay E.P. tiene dentro de su reglamentación el procedimiento denominado Atención de requerimientos de soporte tecnológico en su versión 2.0, con fecha 31 de marzo del 2017, vigente en la actualidad. Donde se señala el

funcionamiento y todo el procedimiento a seguir en cuanto al funcionamiento del sistema OTRS (Open-source Ticket Request System o Sistema de Tickets de Código Abierto)

Dentro de las responsabilidades para el registro de incidentes se han designado diferentes elementos entre los elementos técnicos necesarios se detallan los siguientes:

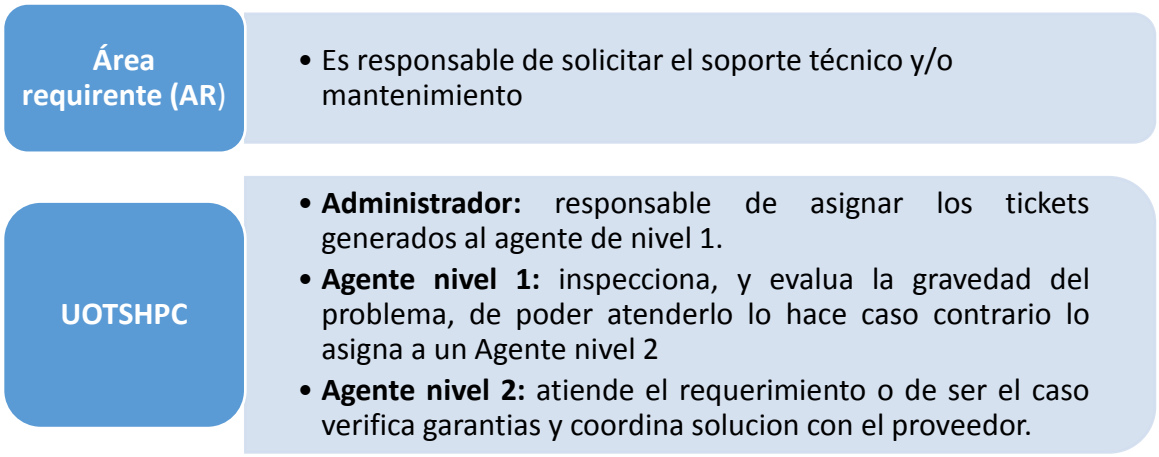


Figura 24. Responsabilidades del registro y solución de tickets

Fuente: (Yachay E.P., 2017)

3.6.1. Procedimiento para el registro de eventos e incidencias

El proceso para dar seguimiento y solventar un evento o incidencia por parte de la DOTSHPC de manera técnica, teniendo en cuenta que en este proceso se ha omitido los procesos administrativos internos, se detalla a continuación el siguiente procedimiento:

- El AR realiza el requerimiento de soporte tecnológico a través de correo electrónico a soporte@yachay.gob.ec o con una llamada telefónica a las ext. 3030, 3031, 3032, los incidentes reportados ingresan al sistema OTRS
- El administrador asigna ticket, una vez conocida la disponibilidad de personal y el responsable que atenderá el requerimiento.

- El agente nivel 1 realiza la inspección y evaluación inicial, aplicando manuales e instructivos.
- Si el agente nivel 1 puede atender al requerimiento, lo solventa.
- Si el agente nivel 1 no puede solventar dicho requerimiento puede reasignarse a un Agente nivel 2 por parte del Agente nivel 1 o del Administrador.
- Si el agente nivel 2 puede resolver el requerimiento realizara la atención de acuerdo a la gravedad y complejidad que amerite.
- De no ser así la DOTSHPC verifica la aplicación de garantías o disponibilidad de horas de soporte.
- Dado el caso de que cuente con estas garantías o disponibilidad de horas de soporte el agente nivel 2 coordina la ejecución con el proveedor y valida la solución del requerimiento,
- El en caso de no contar con garantías ni horas de soporte el agente de nivel 2 realiza un informe técnico de diagnóstico para la contratación del servicio, y coordina todo este proceso hasta la adquisición del mismo.
- Una vez adquiridas las partes o piezas de repuesto o contratación de servicio para cubrir el requerimiento, el agente nivel 2 realiza un informe de satisfacción con respecto al contrato realizado, mismo que debe ser revisado y aprobado por el director de la DOTSHPC.
- Una vez solventada la incidencia ya sea por un Agente nivel 1, Agente nivel 2, por garantías o adquisición de quipos se remite una notificación por medio de correo electrónico conforme al sistema OTRS al AR mencionando que el requerimiento ha sido atendido.
- El AR recibe la notificación de que el requerimiento ha sido atendido, si el servicio está de acuerdo a conformidad el funcionario que atendió el requerimiento en el

sistema OTRS cierra el ticket y finaliza el procedimiento, caso contrario el AR debe realizar nuevamente el requerimiento de soporte tecnológico.

Este proceso se lo demuestra de manera gráfica en un diagrama de flujos en la Figura 25 y 26.

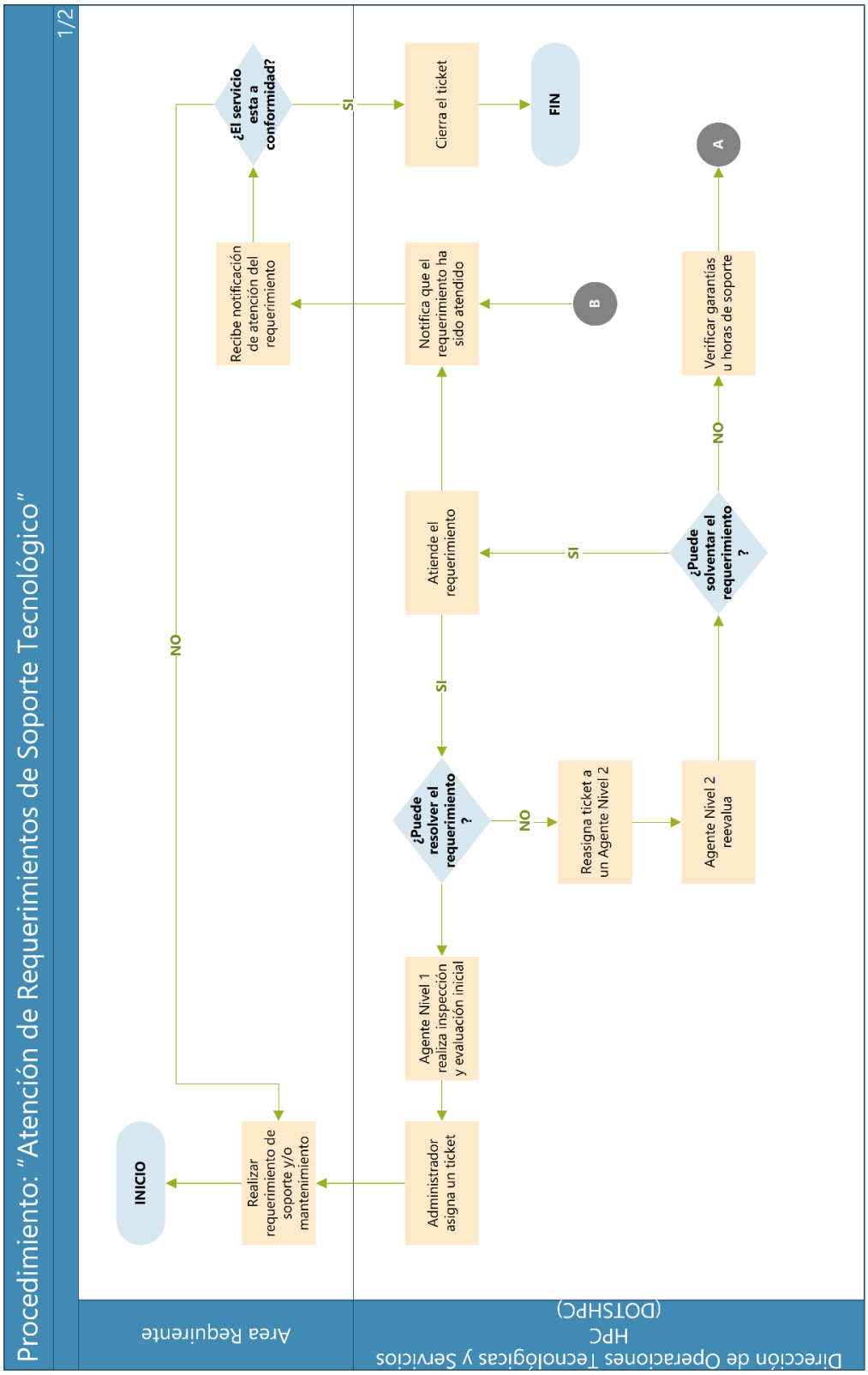


Figura 25. Proceso de Atención de requerimientos de Soporte Tecnológico (1 de 2)

Fuente: DOTSHPC

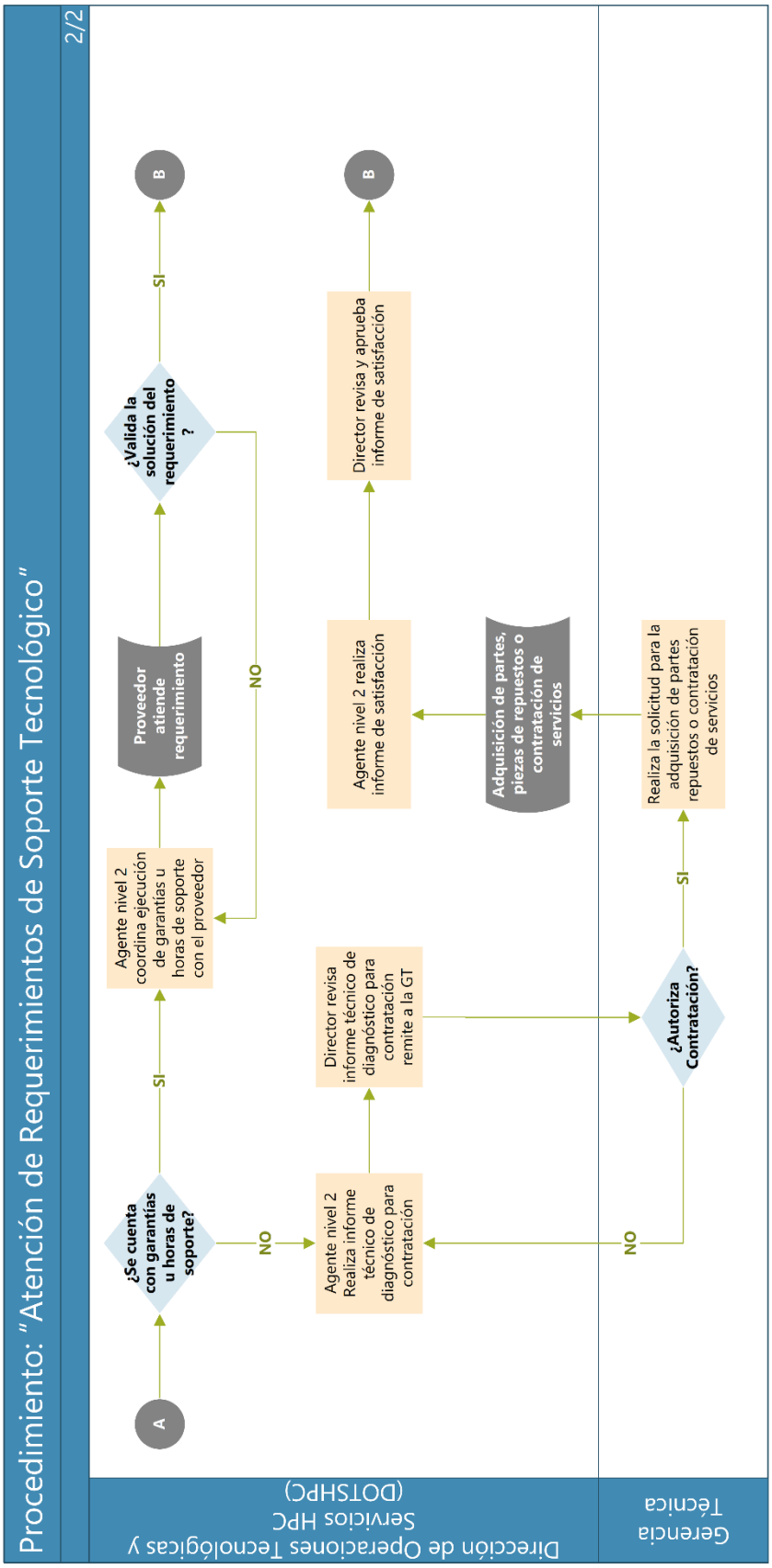


Figura 26. Proceso de Atención de requerimientos de Soporte Tecnológico (2 de 2)

Fuente: DOTSHPC

3.7.Topología física de red.

La UOTSHPC al ser la encargada del buen funcionamiento de la red de la “Ciudad del conocimiento Yachay”, cuenta con una red distribuida en diferentes sectores como se muestra en la Figura 27, siendo estos: Data Center (DC), Mercado las Manuelas (MM), Universidad Yachay Tech, Bloques de residencias (BR), El Rosario (RS), Instituto Tecnológico 17 de Julio (ITS), Centro Infantil del Buen Vivir (CIBV), Hoja blanca (HB), Centro de Emprendimiento (CE).

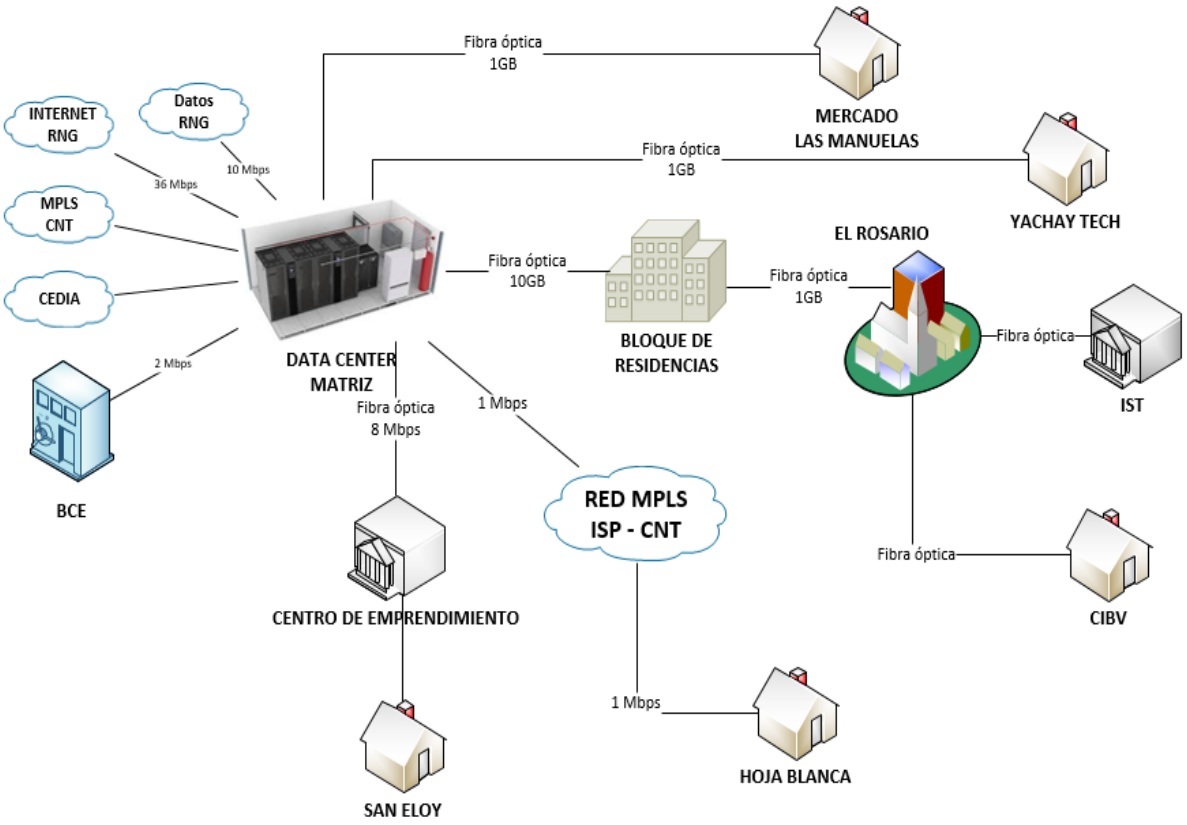


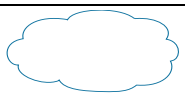
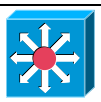
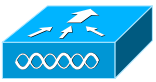
Figura 27. Diagrama de conectividad de la ciudad del Conocimiento Yachay

Fuente: DOTSHPC

En la Figura 28 se muestra la topología de red que conecta con el Data Center de Yachay, de manera que se puede apreciar los enlaces principales que a esta red se conectan

como son: el enlace principal de la red de CNT, misma que brinda a Yachay un ancho de banda de 10 Gbps, además se conecta a un enlace de datos y de Internet con la red gubernamental (RNG) mismas que tienen una capacidad de 10 Mbps y 30 Mbps respectivamente, además se conecta con un enlace directo hacia el Banco Central del Ecuador (BCE) con un ancho de banda de 2 Mbps, y también con una red interna denominada Invitados CE que brinda conectividad a los visitantes del Centro de Emprendimiento con un enlace de 8Mbps, y así también se tiene un enlace dedicado hacia la red de CEDIA, además de las redes mencionadas el Data Center se conecta con la red del super computador (HPC). La topología mostrada en la Figura 28 utiliza la simbología de la Tabla 8.

Tabla 8. Simbología de red Utilizada

Simbología	Descripción	Simbología	Descripción
	Cable para conexión		Red externa
	Ether Channel		Switch de Core Capa 3
	Switch de Acceso Capa 2		Switch de Core, para la red del HPC
	Firewall		Switch de Acceso, para la red del HPC
	Controladora para la red Wireless		Servidores Virtualizados

Fuente: DOTSHPC

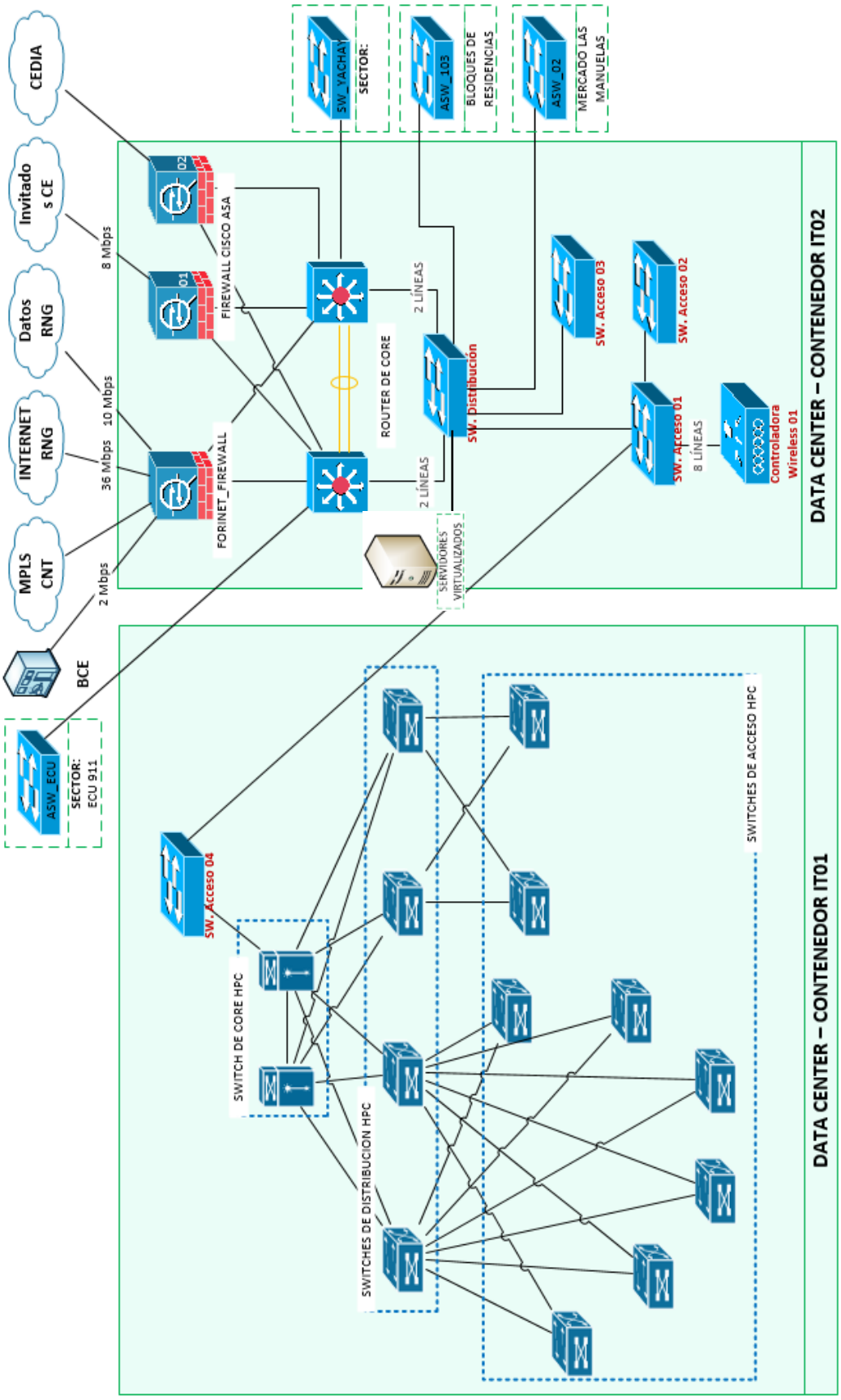


Figura 28. Topología General de la red de Yachay

Fuente: DOTSHPC

3.7.1. Topología de red Data Center

En el 2014 se realiza una contratación pública para la adquisición dos contenedores para la puesta en funcionamiento del Data Center, mismo que cumple los requerimientos para establecerse como TIER III. A estos contenedores se los ha denominado IT01 e IT02 respectivamente, teniendo en cuenta que en estos contenedores además de incluir el equipamiento de Networking se encuentra todo el equipamiento que conforma el super computador (HPC).

Esta es la principal red de la cual se conectan los diferentes servicios y en la que se concentran todos los equipos que conforman el núcleo de la red, razón por la cual la UOTSHPC brinda mayor prioridad a este sector. Su nomenclatura para distinción en la red es DC. La red DC cuenta con las tres capas de la arquitectura de una red de nueva generación, es decir núcleo, distribución y acceso, siendo sus enlaces principales redundantes para evitar caídas de conectividad y fallos de comunicación.

En el IT01 se encuentra el equipamiento de Networking mostrado en la Figura 29, mismo que se brinda conectividad desde el IT02 hacia el HPC y su red de Networking conectando cada uno de sus enlaces por medio de fibra óptica, además se aprecia la red de Networking del HPC, que al igual que la red DC cumple con la arquitectura de una red de nueva generación.

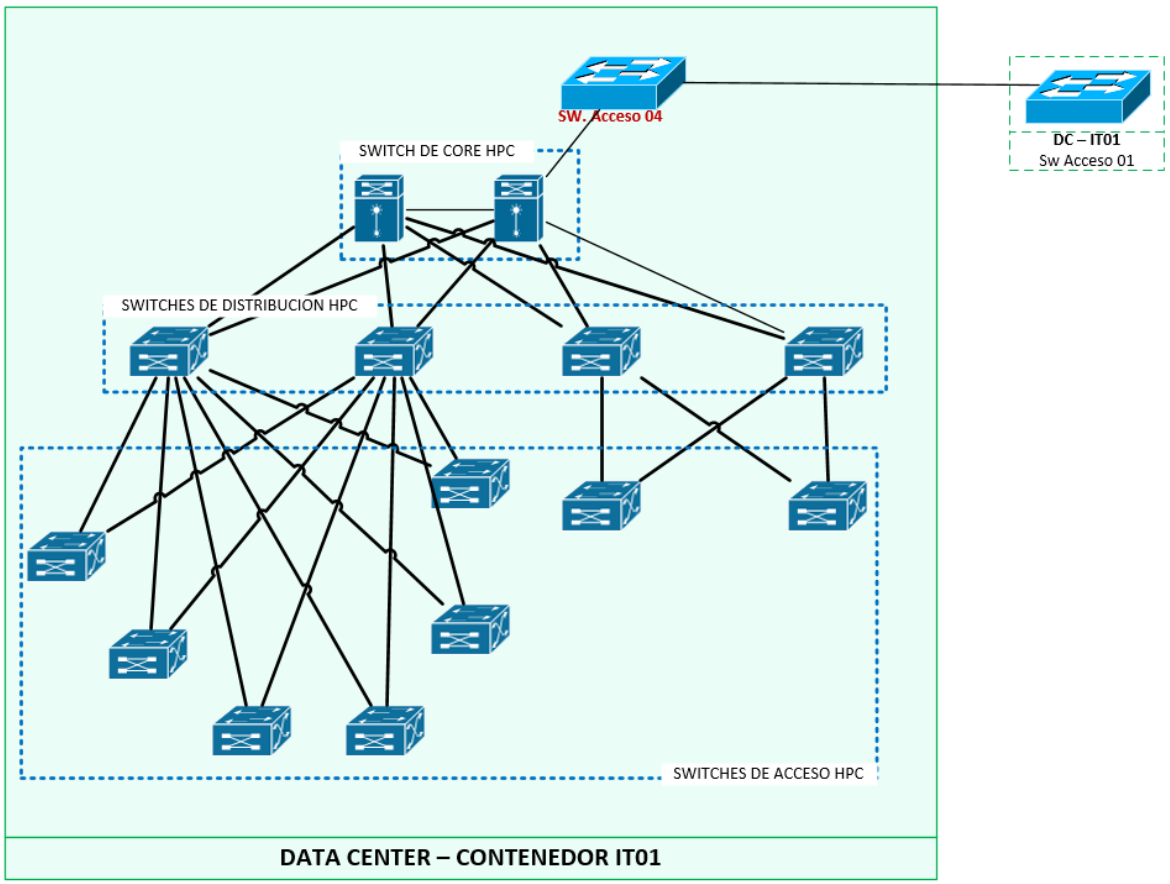


Figura 29. Topología Data center IT01

Fuente: DOTSHPC

La Figura 30 muestra el diagrama de conectividad del IT02 de la red Data Center, su conectividad con las diferentes redes cercanas y sus nodos de conectividad principales que se mencionaron previamente entre estos: enlace con el BCE, enlace backbone CNT, enlace de Internet y Datos RNG, enlace invitados CE y el enlace CEDIA. La red del IT02 conecta a los sectores de toda la Ciudad del Conocimiento Yachay; siendo sus redes directamente conectadas: la red denominada ECU911, el Bloque de Residencias, el Mercado Las Manuelas y el IT01.

Dentro del IT02 al tener los enlaces principales cuenta también con seguridad perimetral para el acceso a la información, siendo estos un firewall Fortinet el encargado principalmente de estos accesos, pero también se cuenta con dos firewalls Cisco ASA conectados en alta disponibilidad con balanceo de carga, para evitar caídas y fallos del servicio.

Dentro de esta red también se concentran los Switch de núcleo (core), de acceso y de distribución, principales de toda la red, así como también se concentran los servidores virtualizados, donde se alojan todos los servicios que se brindan a toda la Ciudad del Conocimiento “Yachay”.

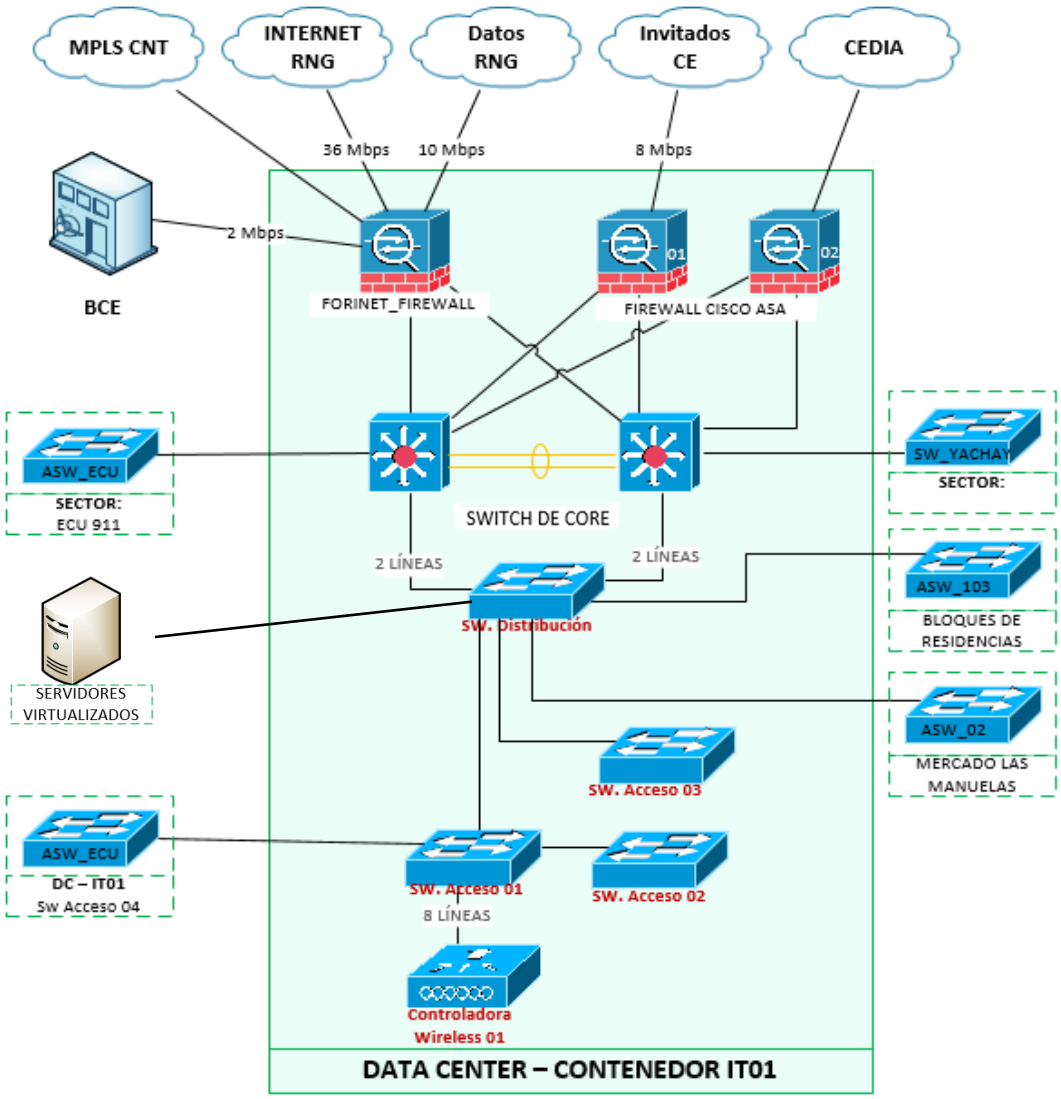


Figura 30. Topología Data Center IT02

Fuente: DOTSHPC

En resumen, de las topologías mostradas previamente y con base del registro de activos proporcionado por la DOTSHPC, se muestra la Tabla 9 con la información de cada uno de los elementos que conforman la red Data Center.

Tabla 9. Equipos de red alojados en la red Data Center

EQUIPO	MARCA/MODELO	CARACTERÍSTICAS	CANTIDAD
Switch de Core	Cisco Catalyst 6800	32 puertos Características de Capa 3 administrable	2
Switch de Distribución	Cisco Catalyst 4500X-16 SFP+	24 puertos	1
Switch de Acceso	Cisco Catalyst 2900	48 puertos	3
Controladora de Wireless	Cisco 5508	8 puertos Soporte hasta 500 access Points	1
Firewall	Cisco ASA 5510	4 puertos	2
Firewall	FORTINET FORTIGATE 1000D	8 puertos	1

Fuente: Recolección de información proporcionada por la DOTSHPC

3.8.Topología lógica de red.

Dentro de la red de Yachay se cuenta con la red 80.0.0.0 /8, siendo esta una red clase A, de la cual la UOTSHPC distribuye esta red, de manera que ésta sea segmentada en diferentes sectores permitiendo que cada sector tenga acceso a ciertos servicios. La UOTSHPC distribuye las subredes creadas en todos los equipos de la red Data Center, es decir en sus Switch de core, distribución y acceso.

La red lógica se divide en dos segmentos principales que no se intercomunican, la red de invitados y red corporativos, donde, los usuarios de la red invitados son todas las personas interna y externas que quieran acceder a una red de en la cual se tenga el único servicio de conectividad a Internet, por el contrario, a la red corporativos se conectan todos los usuarios

autorizados , que necesitan acceder a los diferentes servicios internos de la empresa e incluso tener acceso a la configuración interna del equipamiento de red, dentro de la red corporativos se cuenta con diferentes segmentos de red que permiten distinguir áreas específicas de la red. Todas estas distribuciones lógicas se las realiza mediante una distribución por VLANS, mismas que se muestran en la Tabla 10.

Tabla 10. Direccionamiento de Red

RED	**VLANS**	**VLAN ID**	**Dirección de subred**	**Mascara de subred**	
Invitados	Invitados	43	80.2.0.0	/22	255.255.252.0
Corporativos	Gestion_DC	22	80.0.0.0	/24	255.255.255.0
	Gestion_SW	23	80.0.1.0	/24	255.255.255.0
	Gestion_APs	24	80.0.2.0	/24	255.255.255.0
	Corporativo_CE	30	80.0.3.0	/22	255.255.252.0
	Servidores	10	80.1.0.0	/24	255.255.255.0
	VozIP	40	80.1.0.0	/24	255.255.255.0
	Impresoras	41	80.1.1.0	/26	255.255.255.192
	Streaming	42	80.1.2.0	/24	255.255.255.0
	Telepresencia	47	80.1.3.0	/24	255.255.255.0
	CCTV	48	80.1.4.0	/26	255.255.255.192
	Control_Acceso	49	80.1.5.0	/26	255.255.255.192
	HPC_USER	20	80.0.10.0	/27	255.255.255.224
	HPC_ADMIN	21	80.0.11.0	/27	255.255.255.224

Fuente: Información proporcionada por la UOTSHPC

Hay que tomar en cuenta que todo servicio virtualizado se encuentra dentro de la red de Corporativos dentro de la VLAN de Servidores, es decir la VLAN 10, en la red 80.1.0.X/24, dentro de estos servicios virtualizados se encuentra el DNS mismo que tiene la dirección IP 80.1.0.34.

CAPÍTULO IV. PROPUESTA E IMPLEMENTACIÓN DEL MODELO DE GESTIÓN

Se realiza la propuesta para la gestión de tickets basado en los procesos que la UOTSHPC lleva actualmente, luego de lo cual se enlistan los elementos principales que la unidad necesita para el registro de equipamiento de red y del registro de eventos e incidencias a modo de tickets; con estos requerimientos mínimos se analizan las herramientas que permitan estos registros y se realiza una comparativa de los sistemas de gestión de configuración mencionados en el capítulo dos, basado en el estándar ISO/IEC/IEEE 29148:2011 para la selección del software más apropiado para la implementación. Todo lo mencionado anteriormente, así como también el dimensionamiento y la implementación de la herramienta se lo realiza dentro de este capítulo.

4.1. Propuesta de normalización de eventos e incidencias.

El modelo de propuesta realizado se basa en las buenas prácticas de ITIL v3, con el que la Empresa Pública Yachay E. P. basa sus procesos de servicios de TI.

4.1.1. Clasificación de eventos e incidencias

Tomando en cuenta la Tabla 7 categorización por servicios que tiene actualmente la empresa y haciendo un análisis con la UOTSHPC se ha denotado cada una de las actividades generadas por cada uno de sus servicios y subservicios.

Las actividades que se realizan en cada uno de los subservicios se las ha clasificado por su dificultad de resolución en dos niveles, siendo el primer nivel actividades que se pueden resolver de manera rápida y que no necesitan un proceso de configuración complejo, siendo

estas actividades en su mayoría directamente coordinadas con los usuarios finales; en el segundo nivel se encuentran actividades más complejas que meritan de un conocimiento más extenso de los servicios y subservicios, como es la configuración de equipos de red, servidores, plataformas e incluso la gestión de garantías y procesos con entes externos a la empresa.

Estas actividades para una gestión de nivel uno y nivel dos se las mencionan a continuación por cada uno de los servicios y subservicios.

Servicio: Backup Y Storage

Tabla 11. Actividades para el servicio "Backup Y Storage"

Subservicios	**Actividades para nivel 1**	**Actividades para nivel 2**
File Server	• Validar conexión al file server desde el equipo del usuario. • Creación de accesos directos de carpetas compartidas y unidades de red hacia el File Server.	• Asignar permisos de acceso a las carpetas compartidas a los funcionarios. • Mantenimiento de la estructura de archivos en el File Server. • Gestión monitoreo y mantenimiento del servidor de File Server. • Incremento de espacios de disco en el File Server. • Respaldo de configuraciones y datos del file server. • Movimiento de archivos dentro del File Server. • Garantizar el espacio suficiente para almacenamiento de la información.
Cloud Box	• Instalación de cliente YachayBox en terminal del usuario. • Verificar problemas de conectividad. • Capacitación de uso del cliente YachayBox al usuario final.	• Activad/desactivar usuarios. • Asignar Quota y permisos al usuario. • Gestión y mantenimiento del servidor.

Servicio: Data Center

Dentro del servicio Data Center se encuentran los subservicios: Incendios, Control de Accesos, Ventilación y aire acondicionado, Energía, y Video seguridad.

Las actividades que se realizan en un evento o incidente nivel 1 para todos los subservicios son:

- Revisión de conectividad de los elementos.
- Revisión del estado de los equipos, solventar eventos generados por los sistemas electrónicos.

Las actividades que se realizan para los incidentes de nivel 2 en todos los subservicios son:

- Resolver incidencias generadas en los sistemas electrónicos.
- Instalación, configuración, monitoreo y mantenimiento de los sistemas electrónicos.

Servicio: HPC

Dentro de este servicio se encuentran los subservicios: LAN, Infiniband, SCF, LSF, GPFS, Aplicaciones y WEB (hpc.yachay.gob.ec).

Las actividades que se realizan para la solución de un evento o incidencia de nivel 1 son las siguientes:

- Revisión de cables de red.

- Revisión de puntos de red.
- Conectividad física entre equipos de red.
- Estado físico de tarjetas de red

Las actividades que se realizan para la solución de un evento o incidencia nivel 2 son:

- Instalación, configuración, monitoreo y mantenimiento de equipos.
- Configuración de VLAN's, enrutamientos, puertos y puertos troncales.
- Gestión de usuario y contraseña a los equipos.

Servicio: Infraestructura

Tabla 12. Actividades para el servicio "Infraestructura"

Subservicios	**Actividades para nivel 1**	**Actividades para nivel 2**
Virtualización de servidores - Cloud Computing	• Validar conexión a la máquina virtual desde el equipo remoto.	• Creación, mantenimiento y monitoreo de máquinas virtuales. • Configuración del entorno de virtualización.
Storage	• Monitoreo de la capacidad de almacenamiento del storage para que no sobre pase los límites permitidos. • Asignación de espacio para creación de nuevas máquinas virtuales.	• Reconexión de la infraestructura de almacenamiento con la infraestructura de virtualización. • Soporte y garantía técnica de los equipos y componentes con los proveedores.

Servicio: Productividad y Colaboración

Tabla 13. Actividades para el servicio "Productividad y Colaboración"

Subservicios	Actividades para nivel 1	Actividades para nivel 2
Mail	• Respaldar/archivar buzones de correo electrónico en el terminal del usuario, por límite de espacio. • Respaldar/archivar buzones de correo electrónico de usuarios que salen de la institución. • Instalar y configurar el cliente de correo electrónico en el terminal del usuario. • Revisar la configuración del cliente del servicio de correo electrónico en el terminal del usuario.	• Dar alta/baja el buzón del servicio de correo electrónico. • Gestionar grupos de distribución de correo electrónico. • Gestionar flujos de correo electrónico. • Respaldar/archivar buzones de correo electrónico de usuarios dados de baja. • Ampliar/reducir tamaño de buzón de correo electrónico del usuario. • Mantenimiento del servidor de correo electrónico. • Brindar el espacio de almacenamiento para los respaldos de correo electrónico.
Active Directory	• Pruebas de acceso con credenciales del usuario. • Prueba de conectividad al servicio	• Configuración de credenciales de usuarios. • Brindar permisos a los usuarios. • Configuración, mantenimiento del servidor
Telefonía IP / Cisco Jabber	• Revisión del estado de los equipos • Revisión del estado de los elementos de conexión (cables, puertos de red) • Instalación del equipo final. • Restablecer configuración del equipo. • Capacitación para el uso del servicio al usuario	• Dar alta/baja extensión telefónica. • Configuración y asociación del teléfono y extensión en el call manager. • Asignación de líneas directas a extensiones telefónicas • Mantenimiento del servidor call manager

Servicio: Red

Tabla 14. Actividades para el servicio "Red"

Subservicios	Actividades para nivel 1	Actividades para nivel 2
WAN, MAN, LAN, MPLS, etc.	• Revisión de cables de red. • Revisión de punto de red. • Conectividad física entre switch y dispositivo final. • Estado físico de tarjeta de red del dispositivo final.	• Instalación y configuración de equipos de red. • Configuración de VLAN's, enrutamientos, puertos y puertos troncales
WLAN	• Configuración de terminales de usuario a la red. • Verificación de conectividad de las terminales de usuario	• Instalación, configuración, monitoreo y mantenimiento de equipos WLAN. • Gestión de usuario y contraseña en la controladora WLC. • Bloqueo y desbloqueo de dispositivos. Agregación de nuevos puntos de acceso, configuración de interfaces y VLANS
INTERNET (Enlaces de Internet y Datos)	• Revisión de conectividad a Internet. • Test de velocidad. • Revisión física de cables de red y estado de equipos de frontera. • Escaneo de equipos con problemas/amenazas en la red.	• Configuración de equipos para conectividad a Internet. • Emisión de tickets a Soporte corporativo de CNT
DHCP	• Prueba de conectividad a Internet. • Revisión y configuración de direcciones IP en dispositivos finales. • Prueba de conectividad hacia el servidor desde el dispositivo final	• Configuración, mantenimiento y actualización del servidor DHCP.

DNS	• Prueba de conectividad a Internet. • Revisión y configuración de direcciones DNS en dispositivos finales. • Prueba de conectividad hacia el servidor desde el dispositivo final	• Configuración, mantenimiento y actualización del servidor DNS

Servicio Seguridad

Tabla 15. Actividades para el servicio "Seguridad"

Subservicios	**Actividades para nivel 1**	**Actividades para nivel 2**
Seguridad Perimetral	• Verificación de conectividad. • Verificación de permisos asignados a los usuarios • Prueba de funcionamiento de políticas de seguridad.	• Configuración de políticas de seguridad. • Creación de redes. • Configuración de interfaces. • Configuración de SNAT y DNAT
Antivirus	• Verificación de la instalación única del antivirus de la empresa. • Actualización de bases y definiciones de antivirus. • Limpieza de virus en quipos de usuarios	• Conectividad al servidor. • Eliminación de malware a nivel avanzado. • Instalación de endpoint. • Monitoreo de equipos clientes instalados con el antivirus.
Antispam	• Reportar correos maliciosos que ingresa a los buzones de equipos clientes.	• Administración de Black List y White List. • Monitoreo del buzón de cuarentena. • Configuración y mantenimiento del servidor. • Identificación de problemas por rebotes.
Acceso Remoto	• Validar conexión al equipo desde el equipo del usuario. • Verifica conectividad a la red (LAN/WAN).	• Configuración de equipos de red o máquinas virtuales para el acceso remoto.
Certificados Ssl	• Verificación de páginas WEB.	• Configuración de certificados en los servidores.

Proxy Web	• Verificar conectividad al Proxy. • Prueba de funcionamiento de bloqueo de servicios y aplicaciones.	• Configuración del servicio y del servidor. • Detección de problemas a nivel de servicios en el servidor.

Servicio: Sistemas Administrativos

Tabla 16. Actividades para el servicio "Sistemas Administrativos"

Subservicios	**Actividades para nivel 1**	**Actividades para nivel 2**
Sistema Financiero	• Creación y desactivación de usuarios • Actualización del sistema en equipo del cliente. • Asignación de permisos de acceso a los módulos dentro del sistema. • Instalación de software. • Asignación de claves de edición de campos dentro del sistema.	• Administración del plan de contingencia. • Administración del servidor del sistema y servidor Backup. • Administración de respaldo de bases de datos en el servidor. • Soporte y actualización del sistema en el servidor.
Intranet	• Conectividad del equipo del usuario. • Validación de usuario y contraseña para el acceso al servicio	
Content Management	• Creación de usuarios • Cambio de contraseñas y roles de usuarios.	• Instalación de plugins para WordPress. • Cambios en la interfaz gráfica de los sitios web.
OTRS Y GLPI	• Asignación de tickets nivel 1. • Informar los tickets de primer nivel de atención de	• Gestión, monitoreo y mantenimiento del servidor.

	incidencias o requerimientos de usuario. • Reasignación de tickets a nivel 2.	• Información de tickets de segundo nivel de atención de requerimientos/incidencias.

Servicio: Soporte

Tabla 17. Actividades para el servicio "Soporte"

Subservicios	Actividades para nivel 1	Actividades para nivel 2
Impresoras	• Conectividad del equipo Disponibilidad y gestión de suministros. • Inspección física del equipo. • Mantenimiento preventivo y correctivo de los equipos de impresión. • Evaluar y reportar el estado del equipo. • Cambio de suministros y kit de limpieza	• Reparación de la impresora (cambio de fusores y/o repuestos). • Evaluar y reportar el estado del equipo posterior a una reparación.
Equipos Tecnológicos	• Revisión de software y hardware. • Realización de informes técnicos de ser necesario. • Adquisición de accesorios o repuestos para los equipos	• Revisión de software y hardware de equipos de TI. • Compra accesorios o repuestos para los equipos de TI.
Mantenimiento Equipos Tecnológicos	• Seguimiento y supervisión del plan de mantenimiento preventivo y correctivo de equipos tecnológicos e infraestructura de TI	• Elaboración del Plan anual de mantenimiento preventivo/correctivo de equipos. tecnológicos e infraestructura de TI. • Gestión con proveedores

Servicio: Sistemas Electrónicos

Tabla 18. Actividades para el servicio "Sistemas Electrónicos"

Subservicios	Actividades para nivel 1	Actividades para nivel 2
Biométricos E.P.	• Revisión de conectividad. • Revisión del estado físico del equipo.	• Gestión de daño físico que merita reparación o cambio. • Gestión de soporte externo.

Video Seguridad	• Validar el funcionamiento de quipos de CCTV instalados en la empresa. • Instalación y reubicación de equipos de video-vigilancia. • Identificación de problemas y resolución de eventos menores de la infraestructura de CCTV. • Respaldo y gestión de datos de video-vigilancia. • Instalación de software de monitoreo de los equipos instalados dentro de la empresa (DOTSHPC).	• Servicios para respaldo y gestión de datos de video-vigilancia. • Configuración de puertos para conectividad al servicio. • Gestión, monitoreo y factibilidad de los servicios habilitantes del servicio de CCTV

Servicio: Web

Tabla 19. Actividades para el servicio "Web"

Subservicios	**Actividades para nivel 1**	**Actividades para nivel 2**
Quipux	• Creación y desactivación de cuentas de usuarios. • Verificar el funcionamiento y carga de la página. • Instalación de firmas electrónicas.	• Detección de problemas de enrutamiento
Inventario	• Activar y desactivar de usuarios para el acceso al servicio. • Ingreso de nueva información al registro de inventarios. • Verificar la asignación y descarga de equipos informáticos a usuarios finales. • Actualización constante del inventario de quipos informáticos/impresoras/software de terminal de usuario asignados a usuarios finales. • Creación y edición de áreas y cargos.	• Inventario de infraestructura critica de TI, equipamiento y licenciamiento de activo de red, HPC, Cloud Computing • Soluciones de Datacenter centralizados y servidores.

Sistema De Viajes	• Actualización de información	• Consultas técnicas con Presidencia
Sistema Del IESS	• Revisión de conexión con la VPN • Gestión de usuarios para el sistema AS400	• Consultas técnicas con equipo de soporte del IESS
Sistema Ruter	• Creación y eliminación de usuarios	• Consultas técnicas con equipo de soporte del MINTEL

Servicio: Sistemas de Información

Para este servicio se ha detectado una sola actividad dentro de todos los subservicios, misma que puede darse por indisponibilidad, modificación y despliegue del servicio, esta es la de realización de correctivos, todos estos correctivos se los resuelve directamente en nivel uno, por lo que no se escala a nivel dos.

4.1.2. Priorización de eventos e incidencias

Yachay tiene varios servicios internos, mismos que se muestran en la Tabla 20, donde cada servicio es denotado por un código identificativo para el servicio. Cada problema encontrado o registrado recae directamente en un servicio.

Tabla 20. Códigos de servicios

Código	Servicio
SRV_DC	Data center
SRV_RED	Red
SRV_SEG	Seguridad
SRV_INF	Infraestructura
SRV_BACk	Backup y Storage
SRV_PROD	Productividad y colaboración
SRV_ADM	Sistemas administrativos
SRV_HPC	HPC (Super Computador)
SRV_WEB	Web
SRV_ELEC	Subsistemas electrónicos
SRV_SOP	Soporte
SRV_INF	Sistemas de información

ITIL propone la clasificación de tickets por prioridad la cual esta lindada directamente con el impacto y la urgencia, donde el impacto se refiere al daño que presenta para el negocio y sus operaciones dicho incidente, por otra parte, la urgencia se refiere al tiempo en el que este problema podría tener un impacto significativo para la empresa.

Tabla 21. Prioridad en base al impacto y la urgencia

	IMPACTO ALTO	IMPACTO MEDIO	IMPACTO BAJO
URGENCIA ALTA	1	2	3
URGENCIA MEDIA	2	3	4
URGENCIA BAJA	3	4	5

Fuente: Adaptado De (Cherwell, 2018)

Para ser un poco más específicos, el impacto alto se habla de una afección a toda la empresa o su gran mayoría, al hablar de un impacto medio se trata de una afección a un sector o grupo de la empresa y por último al tratarse de un impacto bajo estamos hablando de una afección mínima de usuarios pudiendo ser uno o dos.

En cuanto a los tres niveles de urgencia se tiene: alta cuando el servicio afectado o problema encontrado necesita una solución inmediata, si el problema encontrado tiene una solución controlada o es programada se encuentra en la urgencia media, y por otro lado si la

solución puede esperar o está dentro de un tiempo planificado se encuentra en una urgencia baja.

De los cinco niveles de prioridad obtenidos mediante la intersección del impacto y la urgencia se puede distinguir una incidencia y un evento, como se muestra en la Tabla 22 donde se encuentra ordenada de mayor a menor prioridad.

Tabla 22. Códigos de prioridad de eventos e incidencias

Código	Prioridad	Evento / Incidencia	Descripción
PR1	1	Incidencia	Muy alta (Critico resolucion imediata)
PR2	2	Incidencia	Alta
PR3	3	Evento o Incidencia	Media
PR4	4	Evento	Baja
PR5	5	Evento	Muy Baja (Planificado)

En el caso de las prioridades 1 y 2 se considera como un incidente, al tratarse de una prioridad 4 o 5 se trata de un evento, pero al ser una prioridad 3 el técnico responsable de verificar la falla debe considerar si éste se considera un evento o incidencia dependiendo de la gravedad de la falla presentada.

Los criterios para que un problema registrado entre en cada nivel de prioridad se encuentran mencionadas en la Tabla 23, en base a la reunión realizada con la UOTSHPC (revisar el ANEXO1).

Tabla 23. Criterios para priorizar un evento o incidencia

Código	Criterio
PR1	El incidente es de alto impacto en las funciones críticas de la empresa. Se presenta una indisponibilidad o degradación excesiva del desempeño de las aplicaciones o servicios. Al ser de urgencia alta requiere una solución inmediata.

PR2 El incidente presenta un impacto significativo en alguna de las funciones del negocio, por indisponibilidad o degradación del desempeño en las aplicaciones o servicios.
La solucion del inconveniente debe realizarse a la brevedad posible

PR3 El evento o incidente presenta un impacto moderado en alguna de las funciones del negocio, por degradación leve de desempeño de las aplicaciones o servicios.
El incidente está controlado dado que existe una solicion premeditada y requiere una solucion pronta.
Los usuarios pueden esperar la restauración del servicio.
La solución definitiva debe estar programada.

PR4 El evento presenta un impacto en las funciones no críticas del negocio, el usuario puede esperar por una fecha determinada para la solución definitiva.
El evento implica un número reducido de usuarios o clientes afectados y es de poca visibilidad.
Existe un plan alternativo de solución y se puede esperar la solución definitiva.

PR5 El usuario puede esperar para la resolucion del inconveniente, este puede deberse a una para del servicio planificada previanmente.
El usuario puede continuar con sus tareas críticas de operación, se mantiene la funcionalidad y el desempeño de las aplicaciones o servicios.

El procedimiento a seguir para cada uno de los niveles y dependiendo de las competencias de cada servicio el procedimiento a seguir es el siguiente:

Tabla 24. Procedimiento para resolución de un evento o incidencia por prioridad

Código	Procedimiento
PR5	• Revisión de la conectividad física del equipo del usuario • Revisión del estado físico de cables de red • Revisión del estado físico del punto de red • Revisión del estado físico de la tarjeta de red del dispositivo final • Revisión de la conectividad con las credenciales del usuario al servicio con el que se tiene el inconveniente. • Realizar pruebas de conectividad con el servicio del inconveniente • Capacitación para el uso del servicio al usuario
PR4	• Instalación de equipos finales. • Configuración del equipo del usuario final • Instalación de aplicaciones necesarias para la conectividad al servicio • Restablecer configuración del equipo.

PR3	• Gestión de usuarios y contraseñas • Respaldar/archivar información de usuario. • Respaldar/archivar información de equipos y servicios gestionados. • Instalación, configuración, monitoreo y mantenimiento de equipos de red. • Configuración de VLAN's, enrutamientos, puertos y puertos troncales • Mantenimiento físico de equipos de usuarios finales • Adquisición de suministros
PR2	• Configuración, mantenimiento y actualización de los servidores. • Gestión para adquisición de repuestos para equipos del usuario final. • Gestionar soporte y garantía de equipos y componentes con los proveedores. • Gestión de contratos. • Gestión de soporte con proveedores o entidades externas a la empresa.
PR1	• Se realizan las actividades de prioridad 3 y 2 que meriten una solución inmediata.

Para la solución de eventos o incidencias dentro de la UOTSHPC se asignan un agente nivel 1 y un agente nivel 2.

Luego de generado un ticket por cualquier usuario o área requirente, el agente de nivel 1 realiza la inspección principal del evento o incidente generado, de no tener una prioridad se toma el problema como un evento de prioridad 5, y se aplica el procedimiento, si con las actividades realizadas el problema se ha resuelto se cierra el ticket, caso contrario realiza las actividades de un evento con prioridad 2 e intenta resolver el problema, de no haber resuelto el problema con las actividades de un evento de prioridad 2 y dependiendo de su competencia realiza las actividades de un evento de prioridad 3, si con este proceso se resuelve el evento se realiza un informe técnico que contenga el problema encontrado y la solución aplicada y se cierra el ticket, caso contrario el agente nivel 1 realiza el mismo informe técnico y lo reasigna a un agente nivel 2, el cual dependiendo del informe técnico del agente nivel 1 prioriza el

evento o incidencia, y aplica el procedimiento necesario para la solución del ticket, al solucionarse el agente nivel 2 realiza un informe técnico con la información pertinente.

El informe técnico debe constar del código de servicio, el código de prioridad, y si el evento o incidencia fue originado por software (SW) o por una afección en el hardware (HW), además debe incluir la información completa de la afección encontrada.

Por ejemplo, un usuario reporta que no puede acceder a Internet. El agente nivel 1 se dirige a la ubicación del equipo que no tiene Internet y aplica las actividades de un ticket de prioridad 5 y observa que el cable de red esta desconectado, el agente procede a conectarlo y verifica el acceso a Internet. Al terminar genera un informe con el cogido SRV_RED-PR5-HW y detallando que el problema encontrado se ha generado por la desconexión del cable de red.

En el caso de que al generarse un ticket el agente nivel 1 está en condiciones de priorizar el evento lo hace, de igual manera con un informe técnico con el código de incidencia y detallando el motivo de la prioridad brindada.

Por ejemplo, un usuario registra que no puede imprimir una de las impresoras de la empresa, el agente nivel 1 realiza la inspección necesaria con la realización de las actividades de un ticket de prioridad 5 y verifica que existe un daño del tóner de la impresora y merita un cambio, el agente nivel 1 hace el informe técnico con el código SRV_SOP-PR3-HW debido a que el subservicio de impresoras se encuentra dentro del servicio soporte, necesita la adquisición de suministros por lo tanto es una prioridad 3 y el problema fue por hardware.

4.2.Parámetros necesarios para la implementación del Modelo de Gestión.

En base a las reuniones establecidas con la UOTSHPC se han definido algunos de los elementos necesarios que se deben incluir dentro del registro de equipamiento y también dentro del registro de eventos e incidencias, estos requerimientos son tomados en cuenta para la selección de la herramienta a ser implementada dentro de los servidores lógicos de la Empresa Pública. Para constancia se muestra el ANEXO 2 las actas de reuniones realizadas.

4.2.1. Parámetros necesarios para el registro de equipamiento

Según lo mencionado anteriormente la UOTSHPC requiere un sistema el cual permita la inclusión de información detallada como la que se muestra en la Tabla 25.

Tabla 25. Parámetros necesarios para el registro de equipamiento

Ítem	Descripción
Nombre	Nombre descriptivo del equipo.
Estado	Equipo esta activo o inactivo.
Marca	Marca del equipo de red.
Modelo	Modelo del equipo de red.
Direccion IP	Direccion IP de gestion configurada en el equipo de red.
Hostname	Nombre del equipod dentro de la red.
Numero de puertos	Cantidad de puertos con los que cuenta el equipo de red.
MAC	Numero de serie descriptiva unica del equipo de red.
Ubicación	Lugar fisico de ubicación del equipo de red.
Tecnico(s) responsable(s)	Nombre de el o los responsables del equipo.
Gestion de cambios	Registro de incidentes y eventos genrados con el equipo.

Dentro de estos parámetros se establece que la información puede ser incluida de forma manual, como es el caso de la ubicación, técnicos responsables y la gestión de cambios.

4.2.2. Parámetros necesarios para el registro de eventos e incidencias

Dentro de los eventos e incidencias que la UOTSHPC es encargada de brindar una solución, se encuentran como parámetros principales el registro de los parámetros mencionados en la Tabla 26.

Tabla 26. Parámetros necesarios para el registro de eventos e incidencias

Ítem	Descripción
Numero de Ticket	Numero identificativo de evento o incidencia
Avería	Cual es el daño encontrado
Ubicación	Lugar fisico de ubicación donde se tiene el fallo
Técnico(s) responsable(s)	Nombre de el o los responsables encagado(s) de brindar soporte
Tipo de Ticket	Ticket Nivel 1 o Nivel 2
Dirección IP	Direccion IP de gestion configurada en el equipo de red.
Hostname	Nombre del equipo dentro de la red.
Gestión de cambios	Permitir registrar el o los cambios generados para solventar el fallo registrado

Esta información debe ser incluida por el administrador de manera manual luego de haber recibido una llamada o un correo electrónico por parte de un área requirente.

4.3.Estándar para selección de software ISO/IEC/IEEE 29148:2011

Dentro del estándar ISO/IEC/IEEE 29148 publicada en el año 2011 se encuentran disposiciones que permiten la selección de software mediante la utilización de parámetros, requisito, características y atributos. Este estándar permitirá la elección del sistema a implementarse en la Empresa Pública Yachay E. P., la norma se la adjunta en el ANEXO 3.

4.3.1. Propósito de la norma

El propósito del uso de la norma es que la implementación del sistema de gestión de configuración que cumpla con los parámetros establecidos previamente en el alcance del

presente proyecto, de tal manera que la UOTSHPC pueda realizar el registro de equipamiento de red y también registrar eventos e incidencias como tickets.

4.3.2. Alcance

Seleccionar la plataforma que permita el registro de activos y tickets, el cual se adapte de mejor manera a los requerimientos del proyecto.

4.3.3. Perspectiva del producto

La implementación del sistema debe permitir a la UOTSHPC tener una plataforma basada en software libre, que permita el registro y almacenamiento de información del equipamiento de red implementada en el Data Center, tanto de manera automática como inclusión de información adicional de manera manual, el mismo debe permitir generar tickets para registro seguimiento y resolución de eventos e incidencias

4.3.4. Funciones del producto

La implementación del sistema debe cumplir el siguiente listado de funcionalidades:

- Permitir el acceso únicamente a personal autorizado, enlazado a un directorio activo de la empresa.
- Registrar información del equipamiento de red instalado en el Data Center de manera automática usando SNMP v2 y de manera manual en caso de ser necesario.
- Tener un inventario del equipamiento de red implementado en la red del Data Center.
- Registro de tickets de nivel dos, de eventos e incidencias especificando información técnica que ayude al técnico responsable realizar el seguimiento y solución del mismo.

4.3.5. Características de los usuarios

El sistema al brindar una solución tecnológica a nivel técnico debe ser usado por personal con nivel de educación superior con experiencia en el uso y configuración de redes de comunicación, para el registro de equipamiento y de tickets, así como también para brindar un seguimiento y solución de tickets.

4.3.6. Limitaciones

Como limitantes para la implementación del sistema se han considerado las siguientes:

- No utilizará una plataforma que esté basada en software de pago.
- El sistema no debe consumir una excesiva cantidad de ancho de banda, debido a que dentro de esta red se brindan más servicios.
- El proceso para la generación, asignación y resolución de tickets debe estar basada en las buenas prácticas de ITIL, para dar continuidad a los procesos que se llevan a cabo en la empresa.

4.3.7. Requerimientos específicos del sistema

Se detallan los requerimientos detallados por la UOTSHPC con respecto a la funcionalidad y manejo del mismo, aspectos que son relacionados con el software del sistema a implementarse.

4.3.7.1.Interfaces de usuario

REQ1: **Administración:** el sistema debe contar con una interfaz gráfica que permita acceder a la información tanto para el administrador del sistema como para el área

técnica en función, de tal manera que se pueda verificar e incluir información técnica sobre los equipos de red conectados y la generación asignación y cierre de tickets

4.3.7.2.Interfaces de software

REQ2: Registro de equipamiento: el sistema debe permitir registrar información de equipamiento de red de manera automática y manual, como mínimo de los elementos requeridos por la UOTSHPC.

REQ3: Procesos de ITIL: para el registro y resolución de tickets es necesario que la herramienta base su proceso en la operación de servicios de las buenas prácticas de ITIL.

REQ4: Registro de Tickets: el sistema debe permitir registrar, asignar, modificar y cerrar tickets para la solución de eventos e incidencias, permitiendo el registro de los elementos requeridos por la UOTSHPC.

4.3.7.3.Interfaces de comunicación

REQ5: Conectividad: el sistema deberá permitir la administración de un gran número de equipos de red para poder realizar su registro.

REQ6: Soporte de protocolos: el software debe permitir la comunicación mediante SNMP v2 para la obtención de información del equipamiento de red implementado en el Data Center.

4.3.7.4.Requisitos no funcionales

REQ7: Licencia: el sistema debe ser implementado en software con licenciamiento libre.

4.3.7.5.Modo de operación

REQ8: Gestión de usuarios: el sistema debe permitir crear modificar y/o eliminar usuarios locales y sus contraseñas,

REQ9: Gestión con el directorio activo: el sistema debe permitir enlazarse con el directorio activo de la empresa para poder acceder al sistema con las credenciales brindada por la institución.

REQ10: Gestionar permisos de usuarios: el sistema debe permitir la asignación y modificación de permisos de acceso a la información, de tal manera que el administrador pueda gestionar todo el sistema, y dependiendo el sector y las funciones de los técnicos, se permita el acceso a toda o parte de la información según sus funciones y requerimientos

4.3.8. Valoración de los requerimientos

Con un listado de los requerimientos obtenidos para la implementación del sistema, se detalla en la Tabla 27 los puntajes que permitirá la selección de selección de la herramienta que mejor se adapte a dichos parámetros

Tabla 27. Requerimientos del sistema de gestión de configuración

REQUERIMIENTO	VALOR	DESCRIPCIÓN
REQ1: Administración	0	El sistema no cuenta con una interfaz web para administración.
	1	El sistema cuenta con una interfaz web para administración.
REQ2: Registro de equipamiento	0	El sistema no permite el registro de equipos de manera automática y/o de manera manual
	1	El sistema permite el registro de equipos de manera automatica y/o de manera manual

	2	El sistema permite el registro de los elementos necesarios por la UOTSHPC de manera manual y/o automática. Mostrados en la Tabla 25
REQ3: Procesos de ITIL	0	Los procesos a seguir no son adaptables al proceso de ITIL
	1	Los procesos a seguir son adaptables o son basados al proceso de ITIL
REQ4: Registro de Tickets	0	No se permite una completa gestión y solución de tickets
	1	Si se permite el registro, seguimiento y solución de tickets
	2	Permite el registro de los elementos requeridos por la UOTSHPC en la Tabla 26
REQ5: Conectividad	0	Tiene una cantidad limite muy pequeña para el registro equipos.
	1	No una cantidad limite o su cantidad limitante es muy alta para el registro equipos.
REQ6: Soporte de protocolos	0	No es compatible o no recolecta información con SNMv2
	1	Si es compatible y recolecta informacion a través de SNMPv2
REQ7: Licencia	0	No tiene licencia de software libre
	1	Tiene licencia de software libre
REQ8: Gestión de usuarios	0	No se permite crear, modificar, eliminar, o modificar usuarios y/o sus contraseñas, locales del sistema
	1	Se permite crear, modificar, eliminar, o modificar usuarios y/o sus contraseñas locales del sistema.
REQ9: Gestión con el directorio activo	0	No se permite el enlace con directorios activos para autenticación de usuarios
	1	Se permite el enlace con directorios activos para autenticación de usuarios
REQ10: Gestionar permisos de usuarios	0	No se puede dar privilegios a usuarios específicos para acceder modificar o agregar información.
	1	Se puede dar privilegios a usuarios específicos para acceder modificar o agregar información.

4.3.9. Calificación del sistema de gestión de configuración

En base a los parámetros establecidos gracias a la aplicación del estándar IEEE-29148, se establecieron valores para cada uno de estos parámetros necesarios para la implementación

del sistema, tomando en cuenta estos valores se realizara la selección de una de las tres herramientas presentadas en el titulo 2.7 “ Sistemas de gestión de configuración”, la herramienta que se selecciona será la que se adapte de mejor manera a las necesidades presentadas y la cual será implementada, por lo tanto dependiendo se sus características se ha llenado la Tabla 28.

Tabla 28. Calificación de los sistemas de gestión

REQUERIMIENTOS	OCS Inventory	ITOP	GLPI
REQ1: Administración	1	1	1
REQ2: Registro de equipamiento	1	2	2
REQ3: Procesos de ITIL	0	1	1
REQ4: Registro de Tickets	0	1	2
REQ5: Conectividad	1	1	1
REQ6: Soporte de protocolos	1	1	1
REQ7: Licencia	1	1	1
REQ8: Gestión de usuarios	0	0	1
REQ9: Gestión con el directorio activo	1	0	1
REQ10: Gestionar permisos de usuarios	1	1	1
Valoración total	**9**	**9**	**12**

En base a la Tabla 28 y el análisis previamente obtenido de las herramientas que permiten la gestión de configuración en cuanto al registro de equipamiento activo y gestión de tickets, se selecciona GLPI a ser implementado ya que cumple con todos los requerimientos brindados por la DOTSHPC en específico de la UOTSHPC, además de que GLPI pude incluir funcionalidades de FusionInventory u OCS Inventory a manera de plugin para hacerla mucho más robusta.

4.4.Dimensionamiento del sistema de gestión de configuración.

La UOTSHPC al manejar un servicio virtualizado de servidores no hace falta hacer la adquisición de elementos físicos, pero si es necesario un dimensionamiento que permita saber

los recursos que esta máquina virtual debe contener para su buen funcionamiento, haciendo un enfoque en cuanto a memoria RAM y Disco Duro.

En cuanto a vida útil del servidor se ha propuesto por la UOTSHPC de 10 años de funcionamiento, así también la unidad ha provisto la implementación en el sistema operativo Debian gracias a sus funcionalidades y compatibilidad con el sistema a implementar.

4.4.1. Memoria RAM

El sistema operativo Debian para su implementación en un entorno grafico se necesita como mínimo 256 Mb y 1 Gb recomendado, así también de un disco duro de 5 Gb como mínimo y 10 Gb recomendablemente (Debian, 2019).

En cuanto a la herramienta a implementarse necesita 250 Mb de memoria RAM y 5 Gb de Disco duro como mínimo. (GLPI Project, 2019)

En base a lo mencionado tenemos la Tabla 29 donde se muestra la capacidad máxima de consumo de memoria RAM, para estos servicios.

Tabla 29. Requerimiento de Memoria RAM

Memoria RAM	Recomendado
Sistema operativo	1024 Mb
GLPI	250 Mb
Conexión web y base de datos	30 Mb

Fuente: (GLPI Project, 2019)

Para tener un mejor rendimiento en todos sus procesos según las buenas prácticas de Microsoft y según el análisis realizado para el servicio de virtualización realizado Ramírez Indacochea & Robalino Cárdenas (2014), se recomienda que el proceso de trabajo de un servidor no debe exceder el 80% de la capacidad de procesamiento en memoria RAM, para

que el o los servicios y procesos no se saturen brindando un mejor rendimiento en condiciones de máximo rendimiento (Microsoft, 2019), por lo tanto se debería brindar un 20% adicional al valor total de memoria RAM recomendada, pero adicional a Microsoft brinda una fórmula para el cálculo de conexiones simultaneas en un servidor SQL, misma que puede ser aplicada para este cálculo ya que GLPI también utiliza un servidor web, conexiones simultaneas al servicio y una gestión en una mase de datos, por lo tanto:

$$Maximo\ Clientes = \frac{RAM\ Total - RAM\ otros\ procesos}{RAM\ por\ conexion\ (servicio\ web\ y\ base\ de\ datos)} \quad (1)$$

Donde:

RAM Total = (RAM por conexión x Máximo de clientes) + RAM otros procesos

Para lo cual se tuvo una reunión con la UOTSHPC y se definió que el servicio estaría disponible solo para esta unidad, por lo que el número máximo de conexiones simultaneas no excedería de 10, por lo tanto, el cálculo quedaría de la siguiente manera:

RAM Total = (30 x 10) + (1024+250)

RAM Total = 1574 Mb

Este es un valor de consume de Memoria RAM en un estado de máximo uso del servidor, pero como se mencionó previamente a este valor se le adicionará un 20% para que no se sature y el proceso máximo del servidor en cuanto a memoria RAM sea del 80% en el caso más crítico.

$$20\% = \text{RAM Total x } 20\%$$

$$20\ \% = 1574\ x\ 20\% = 314.8\ \text{Mb}$$

Memoria RAM Requerida = RAM Total + 20%

Memoria RAM Requerida = 1888,8 Mb

Por lo cual se ha destinado un total de **2 GB** para la máquina virtual.

4.4.2. Disco Duro

En cuanto a Disco Duro necesario como se menciona en la Tabla 30, donde se muestran no los parámetros mínimos de instalación sino más bien la capacidad que ocupa el sistema operativo instalado y la herramienta.

Tabla 30. Uso de Disco Duro tras instalacion minima

Disco Duro	Capacidad de uso al instalarse
Debian actualizado	5,6 Gb
GLPI y complementos (Apache, PHP, MariaDB)	897 Mb
Total	6,48 GB

Fuente: Adaptado de (GLPI Project, 2019), (GLPI Project, 2018) y (Debian, 2019)

El Sistema Operativo actualizado y GLPI instalado con sus complementos tienen un peso total de 4.89 GB, y teniendo en cuenta que cada registro generado ocupa 789 Bytes (GLPI Project, 2019). La empresa requiere que se dimensione la capacidad de almacenamiento para posteriores registros de todo su equipamiento, teniendo en cuenta que actualmente cuenta con un máximo de 2500 equipos de red (valor proporcionado por la UOTSHPC), tenemos:

Capacidad requerida = # equipos de red * espacio de registro unitario

Capacidad requerida = 2500 * 789 Bytes

Capacidad requerida = 1972500 Bytes = 1926,27 Mb = **1,88 GB**

Esto en el caso de que se registren solo esta cantidad de equipos de red, al ser este un servidor con una vida útil de 10 años, se tiene entonces que, por un valor proporcionado por la UOTSHPC la empresa tiene un crecimiento del 3% anual dentro de 10 años la empresa contaría con:

$$\#\text{Equipamiento en 10 años} = \text{Cantidad actual} * (\%\ \text{crecimiento anual})^{\#\ de\ años}$$

$$\#\text{Equipamiento en 10 años} = 2500 * (1.05)^{10}$$

#Equipamiento en 10 años = 3359,8 ≈ **3360**

En cuanto al registro de equipamiento total dentro de los diez años se tiene:

Capacidad registros = # equipos de red * espacio de registro unitario

Capacidad registros = 3360 * 789 Bytes

Capacidad registros = 2651040 Bytes = 2588,91 Mb = 2,53 GB

En cuanto a los tickets generados se ha provisto por la UOTSHPC que anualmente se han registrado una cantidad máxima de 900 tickets por falla de equipamiento de red, por lo tanto en dentro de 10 años se tendrá generado una cantidad aproximada de 9000 tickets, y teniendo en cuenta que el registro de cada ticket ocupa un máximo de 645 Bytes (GLPI Project, 2019) se tiene:

Capacidad Tickets = cantidad de tickets * espacio de registro unitario

Capacidad Tickets = 9000 * 645 Bytes

Capacidad Tickets = 5805000 Bytes = 5.668,95 Mb = **5,54 GB**

GLPI además tiene la opción de almacenar información relevante como scripts y otra documentación importante dentro de cada registro, siendo este ticket o registro de equipamiento, con una capacidad máxima de archivo de 2 Mb., por lo que se calcula con la cantidad total de registros dentro de los siguientes 10 años.

Capacidad Información Adicional = # Registros totales * 2 Mb

Capacidad Información Adicional = (3360+9000) * 2 Mb

Capacidad Información Adicional = 12360 * 2 Mb

Capacidad Información Adicional = 24720 Mb = **24,14 Gb**

Por lo tanto, el tamaño de disco duro para el almacenamiento de toda esta información es de:

Capacidad Total = Instalación de Sistema + Capacidad registros + Capacidad Tickets + Capacidad Informacion Adicional

Capacidad Total = 6,48 GB + 2,53 GB + 5,54 GB + 24,14 Gb

Capacidad Total = 38,68 GB

Ramírez Indacochea & Robalino Cárdenas (2014) menciona que para el dimensionamiento de disco duro al igual que en Memoria RAM, de un servicio virtualizado

debe trabajar en un umbral máximo del 80%, es decir que el servidor debe contar con un sobredimensionamiento de 20%, para lo cual en una de las reuniones realizadas con la UOTSHPC se estableció un sobre dimensionamiento del 30%, ya que el servidor va a almacenar información y archivos que no tienen una cantidad establecida, es decir que algunos registros pueden no haberse cargado un archivo, mientras que otros registros pueden almacenar dos o más archivos, por lo tanto por lo cual la capacidad de almacenamiento se ha estimado en: **50,248 GB ≈ 51 Gb**.

4.5. Implementación del sistema de gestión de configuración.

La UOTSHPC cuenta con un servidor de virtualización ubicado en el IT02, lugar donde se encuentran almacenados todos los servicios con los que cuenta la ciudad del conocimiento Yachay, por lo que este servidor no será una excepción y se alojará en el mismo lugar señalado en la Figura 31.

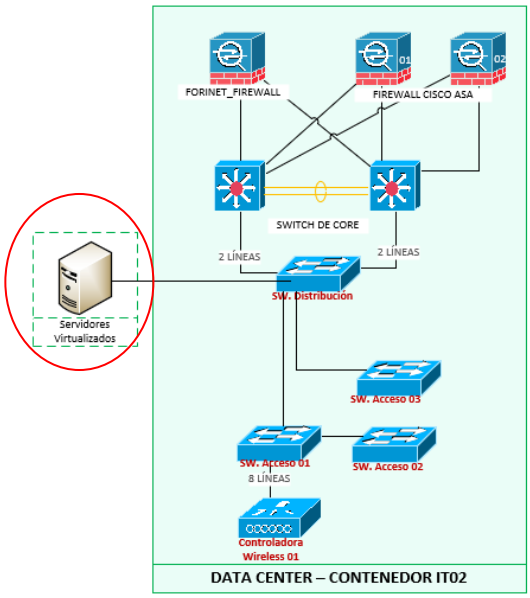


Figura 31. Ubicación física del Servidor

Fuente: DOTSHPC

La UOTSHPC es la encargada de proporcionar la máquina virtual con las características mencionadas previamente, mismas que se muestran en la Tabla 31, la unidad se encarga además de la instalación básica del sistema operativo.

Tabla 31. Elementos de máquina virtual proporcionada por la UOTSHPC

Elemento	Tamaño / Versión
Disco Duro	51 GB
Memoria RAM	2GB
Sistema Operativo Debian	Versión 9.4
Direccion IPv4 (Red Servidores)	80.1.0.247

4.5.1. Configuración de interfaz de red

Principalmente se debe realizar la configuración de la dirección IP de la máquina virtual, dentro del rango permitido para los servidores, esta dirección IP fue brindada por la UOTSHPC, misma que se muestra en la Tabla 32.

Tabla 32. Elementos para la configuración de red de la máquina virtual

Elemento	Direccion IP	Mascara de Sub Red
IP maquina virtual	80.1.0.247	255.255.255.0
Puerta de enlace predeterminada	80.1.0.1	
DNS	80.1.0.34	

Al terminar de configurar la dirección IP de manera correcta, el servidor debe poder ingresar a Internet sin problemas, lo cual permitirá la instalación de los paquetes necesarios para la instalación del sistema, la configuración relacionada con la configuración se puede observar en el ANEXO 4 APARTADO A, se aprecia la configuración de la tarjeta de red de la máquina virtual.

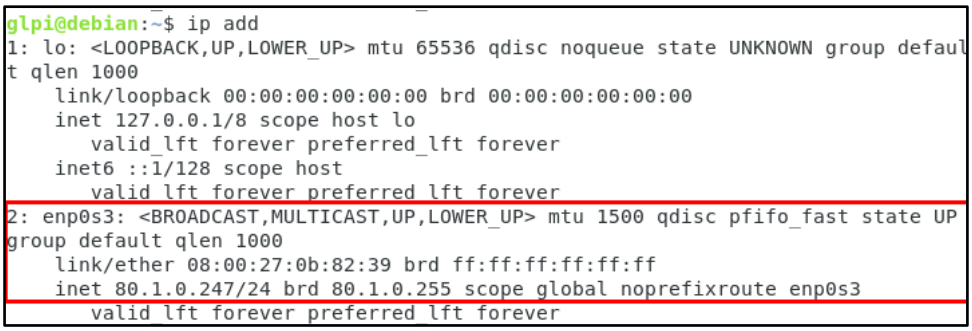


Figura 32. Configuración de red en máquina virtual

Fuente: Terminal Debian

4.5.2. Prerrequisitos de GLPI

Para la instalación de GLPI en su última versión hasta la actualidad la 9.4, se necesita la instalación de varios complementos como se han mencionado en el título 2.7.3.1. "Elementos necesarios para su instalación", mismos que se resumen en la Tabla 33.

Tabla 33. Prerrequisitos para instalación de GLPI

Servicio / Aplicacion	Version
Servidor web - Apache	2 o superior
PHP	5.6 o mas reciente
Base de Datos – MySQL	5.6 o mas reciente
O Base de datos – MariaDB	10.0 o mas reciente

Adicional a este proceso para una configuración remota y mayor facilidad de configuración e instalación del servicio se instala y configura principalmente SSH como se muestra en el ANEXO 4 apartado B, una vez habilitado SSH en el servidor se instalan los elementos necesarios mencionados en la Tabla 33 siguiendo el proceso mencionado en el ANEXO 4 desde el apartado C hasta el apartado F de manera secuencial, de tal manera que al terminar el proceso mencionado se tendrá configurado un servidor web, PHP con las extensiones necesarias para el uso de GLPI y además una base de datos configurada para el uso de la herramienta configurada en el gestor de base de datos MariaDB.

4.5.3. Instalación y configuración de GLPI

Para la instalación de GLPI desde la página oficial se debe descargar el paquete de instalación, descomprimirlo y ejecutarlo, luego de este proceso se debe restaurar el servicio de apache y el servicio de base de datos, para que GLPI reconozca estos como servicios internos del sistema, al terminar este proceso desde un computador conectado en la misma red lógica se accede a un navegador apuntando a la dirección IP del servidor con la dirección a la carpeta de GLPI, en este caso 80.1.0.247/glpi, mediante este servicio web se completará todo el proceso de instalación de GLPI.

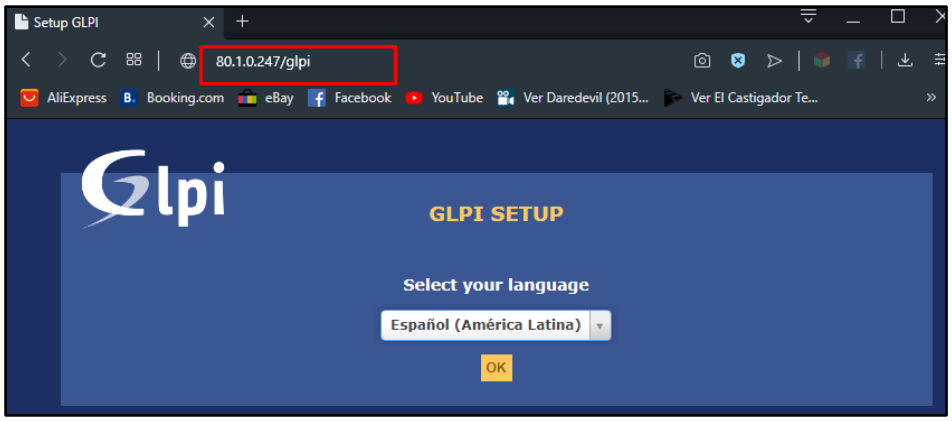


Figura 33. Página principal de instalación de GLPI

Fuente: Interfaz GLPI

Al terminar con la instalación de GLPI, se puede acceder al servicio con el usuario y contraseña por defecto “glpi”, mismo que por recomendaciones de seguridad es recomendable eliminar o a su vez cambiar de contraseña, estas credenciales se pueden ingresar en la pantalla principal de GLPI que se muestran en la Figura 34.

Figura 34. Inicio de Sesión en GLPI

Fuente: Interfaz GLPI

El proceso completo para la instalación y configuración de GLPI, se lo muestra en el ANEXO 4 apartado G.

4.5.4. Vinculación de GLPI con active directory.

Yachay E. P. cuenta con un servicio de registro de usuarios centralizado, este servicio denominado Active Directory también llamado AD o Directorio Activo, consiste en una base de datos LDAP, que permite crear, administrar y mantener de manera centralizada los usuarios y sus permisos dentro de la red LAN de la ciudad del conocimiento (Paessler , 2019).

Por lo cual, para mantener la gestión de usuarios centralizada se debe asociar el AD con GLPI, como se muestra en el ANEXO 5 y obteniendo como resultado la importación de los usuarios que van a utilizar esta herramienta, que son los técnicos de la UOTSHPC.

Figura 35. Usuarios importados desde el Active Directory.

Fuente: Interfaz GLPI

4.5.5. FusionInventory para GLPI

FusionInventory es una herramienta creada para hacer inventarios del equipamiento de red, tales como, servidores, switches, access point, impresoras, computadores, entre otros (FusionInventory, 2019), este plugin permite la incorporación de la función de escaneo automático de red para poder realizar un inventario automatizado.

El plugin de FusionInventory se lo instala en el servidor que en este caso es la máquina virtual de Debian, el proceso detallado de su instalación se encuentra en el ANEXO 6 apartado A, luego del cual se obtiene dentro de la misma interfaz web de GLPI las funciones del plugin FusionInventory, pero el plugin no funciona solo, FusionInventory recolecta la información de los equipos de red mediante SNMP, haciendo uso de un agente, el cual puede estar en cualquier parte de la red con acceso al servidor, es decir puede estar ubicado físicamente en otra ubicación de la red, pero que tenga conectividad lógica con el servidor.

Para la instalación del agente, se necesita tener un computador que esté disponible las 24 horas del día, los 7 días de la semana, para que las tareas se ejecuten en cualquier momento que el administrador configure los procesos, por lo cual a UOTSHPC, brinda acceso a una de

las máquinas virtuales para la instalación del agente de FusionInventory, misma que tiene un sistema operativo Windows server 2008 y previamente instalado SNMP en el mismo.

FusionInventory necesita una comunidad SNMP para su funcionamiento, por lo cual la UOTSHPC, ha destinado la comunidad denominada “YachaySNMP” para el transporte de la información que será enviada desde el o los equipos de la red Data Center hacia el agente, esta comunidad SNMP debe ser configurada en cada uno de los equipos de red con permisos de solo lectura, ya que GLPI necesita únicamente acceder a la información mas no modificarla.

GLPI al instalarse el plugin FusionInventory se lo toma como un gestor de red permitiendo que este almacene y gestione algunas funciones de red como es la verificación del estado de los enlaces, por lo tanto, éste hace la petición hacia el agente mediante el protocolo SNMP para la obtención de la información de los equipos de un rango especifico de red.

En este caso el gestor (GLPI), hace una petición al agente para obtener la información del segmento de la red Data Center, el agente hace las peticiones a los equipos de esta red que comparten la misma comunidad SNMP y los almacena, el agente envía esta información almacenada hacia el gestor (GLPI), para que lo almacene y lo muestre en una interfaz gráfica a manera que pueda ser visual por el usuario.

Para la instalación del plugin y del agente de FusionInventory revise el ANEXO 6 y para la configuración de GLPI y del agente para el inventario automático de equipamiento revise el ANEXO 7.

4.6. Procedimiento para el registro de equipamiento de un segmento de red.

Para el registro de equipamiento nuevo o equipamiento no registrado en el sistema GLPI, se propone el siguiente proceso que permitirá a la UOTSHPC realizar el registro de nuevo equipamiento dentro del inventario de GLPI, me manera que se mantenga el proceso de mejora continua como se lo menciona en las buenas prácticas de ITIL.

El procedimiento para el registro del equipamiento son parte de actividades que se deben realizar dentro de GLPI, mismas que se encuentran a modo de manual de inventario automático de equipamiento en el ANEXO 7. Este procedimiento se lo muestra en la Figura 36 mismo que se lo detalla a continuación:

1. Para la inclusión de nuevo equipamiento dentro del inventario de GLPI, es necesario configurar una comunidad SNMP v2 dentro del equipo o equipos de red.
2. Si la comunidad SNMP para este(s) equipos no inventariados es una comunidad nueva misma que no está registrada dentro de GLPI ni del agente FusionInventory se procede con la actividad 3, caso contrario se procede con la actividad 4.

Nota: Se recomienda utilizar una sola comunidad SNMP para todo el tráfico de registro de equipamiento dentro de GLPI.

3. Asociar la nueva comunidad SNMP en GLPI, dentro de las credenciales SNMP, revise el apartado A. el administrador además debe configurar la nueva comunidad SNMP en el agente, revise el apartado B.

4. Configurar el o los rangos de IP en los cuales se encuentra el/los nuevo(s) equipo(s), si necesita ayuda revise el apartado C.
5. Asocie una o varias credenciales SNMP con el rango o rangos de IP, utilice el apartado D.
6. Si el tiempo de ejecución de escaneo de red para nuevos equipos se ha establecido previamente se procede con la actividad 8, caso contrario se ejecuta la actividad 7.
7. Dentro de un horario de menor uso de la red y sus servicios se debe definir un horario de un rango de una hora para la ejecución de escaneo de red y obtención de la información de los equipos conectados, luego de haberlos definido debe configurar estos dentro de GLPI como se muestra en el apartado E.
8. Cree una nueva tarea dentro de GLPI para un descubrimiento de red IP, como se muestra en el apartado F.
9. Configure un trabajo dentro de la tarea de reconocimiento de red IP, para que GLPI almacene un registro de las IP utilizadas dentro del rango que se ha creado previamente, utilice el apartado G para cumplir con esta tarea.
10. Cree una tarea nueva para el descubrimiento de red mediante protocolo SNMP.

Nota: Realizar el procedimiento de la actividad 8, pero seleccionar el módulo Inventario de red (SNMP) en vez del módulo Descubrimiento de Red.

11. Configure un nuevo trabajo dentro de la tarea creada en la actividad 10, que permita obtener información mediante SNMP de los equipos encontrados en el escaneo de red IP.

Nota: Realizar el procedimiento de la actividad 9, pero seleccionar el módulo Inventario de red (SNMP) en vez del módulo Descubrimiento de Red.

12. Activar las tareas de descubrimiento IP y de inventario por SNMP, y esperar al horario establecido para que las actividades se ejecuten y obtener un inventario de los equipos de red conectados.
13. Si el/los equipo(s) de red conectados dentro de la red establecida no se han reconocido, revise cada una de las configuraciones realizadas desde la actividad 1.

Nota: Para una actualización automática de equipos dentro de la red configurada en el proceso descrito, se recomienda dejar la actividad en un estado activo para que la tarea vuelva a ejecutarse en los días y horarios establecidos.

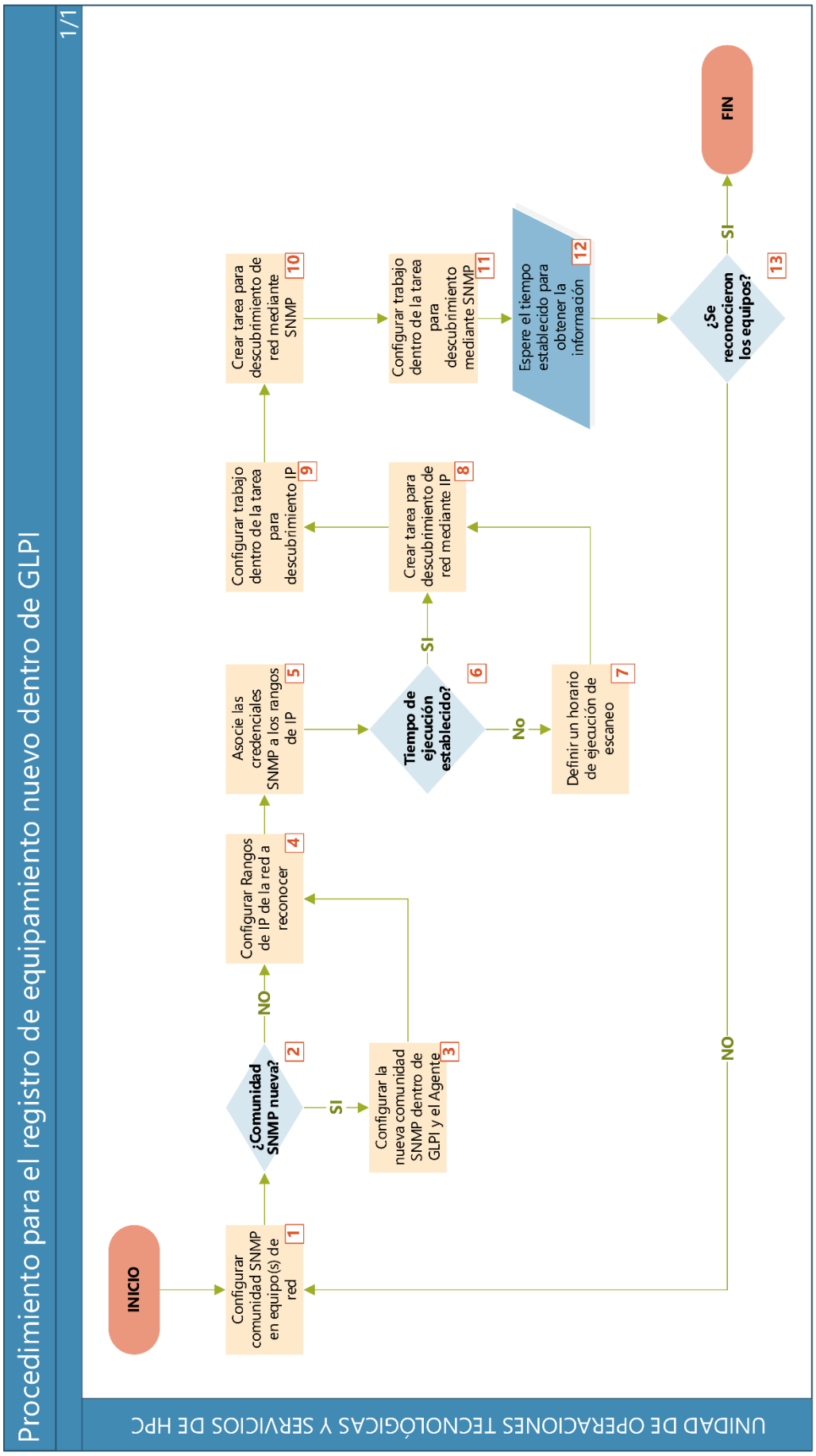


Figura 36. Procedimiento para el registro de equipamiento de un segmento de red

4.7.Procedimiento para la actualización de información de equipos de red

Se ha realizado el siguiente procedimiento para que la UOTSHPC actualice la información de los equipos de red. Este procedimiento se lo debe realizar dentro del sistema GLPI por el técnico responsable o el administrador a cargo.

El proceso de actualización se lo realiza únicamente cuando el equipo se encuentra registrado en GLPI, si éste no se encuentra registrado se debe ejecutar el Procedimiento para el registro de equipamiento de un segmento de red.

Las actividades que se numeran a continuación están incluidas en el manual de inventario automático de equipamiento en el ANEXO 7.

1. El usuario debe decidir si la actualización se la puede hacer mediante la obtención de información por SNMP de ser así se procede con la actividad 2, de lo contrario se debe actualizar esta información de manera manual por lo que debe seguir con la actividad 7.

   Nota: La actualización de información de usuarios, de técnicos responsables, información financiera, y configuración del equipo no se registran automáticamente, esta actualización debe hacerla de manera manual.

2. Dentro de GLPI se verifica si la actividad creada para el escaneo de la red dentro de la cual está el equipo está creada como se muestra en el apartado F, si ésta se encuentra creada se procede con la actividad 3 de lo contrario se procede con la actividad 9.

3. Revisar los parametros previamente configurados en la tarea, tales como el tiempo de ejecución, las redes configuradas, los trabajos dentro de la tarea, como se muestra en el apartado F y G.
4. Poner la tarea en estado activo y guardar.
5. Eesperar el tiempo establecido para que el escaneo de red se realice de manera automatica y recolecte la informacion de manera automática.
6. Revisar el/los equipo(s) que se necesitaba actualizar la información y revisar si esta información fue actualizada de manera automática por SNMP, si esta información se actualizo correctamente se termina el proceso, caso contrario se debe actualizar la información de manera manual, ejecutar la actividad 7.
7. Dentro de GLPI, en la pestaña Activos seleccionar el tipo de elemento (dispositivo de red, computadores, impresoras, etc.), en la parte superior se muestra una ventana de búsqueda ingresar el nombre del dispositivo registrado dentro de la red (Hostname), seleccionar el dispositivo.
8. Incluya la información que necesita actualizar dentro de la información del dispositivo seleccionado, al terminar con la con la actualización del dispositivo se debe guardar los cambios.
9. Ejecutar el Procedimiento para el registro de equipamiento de un segmento de red.

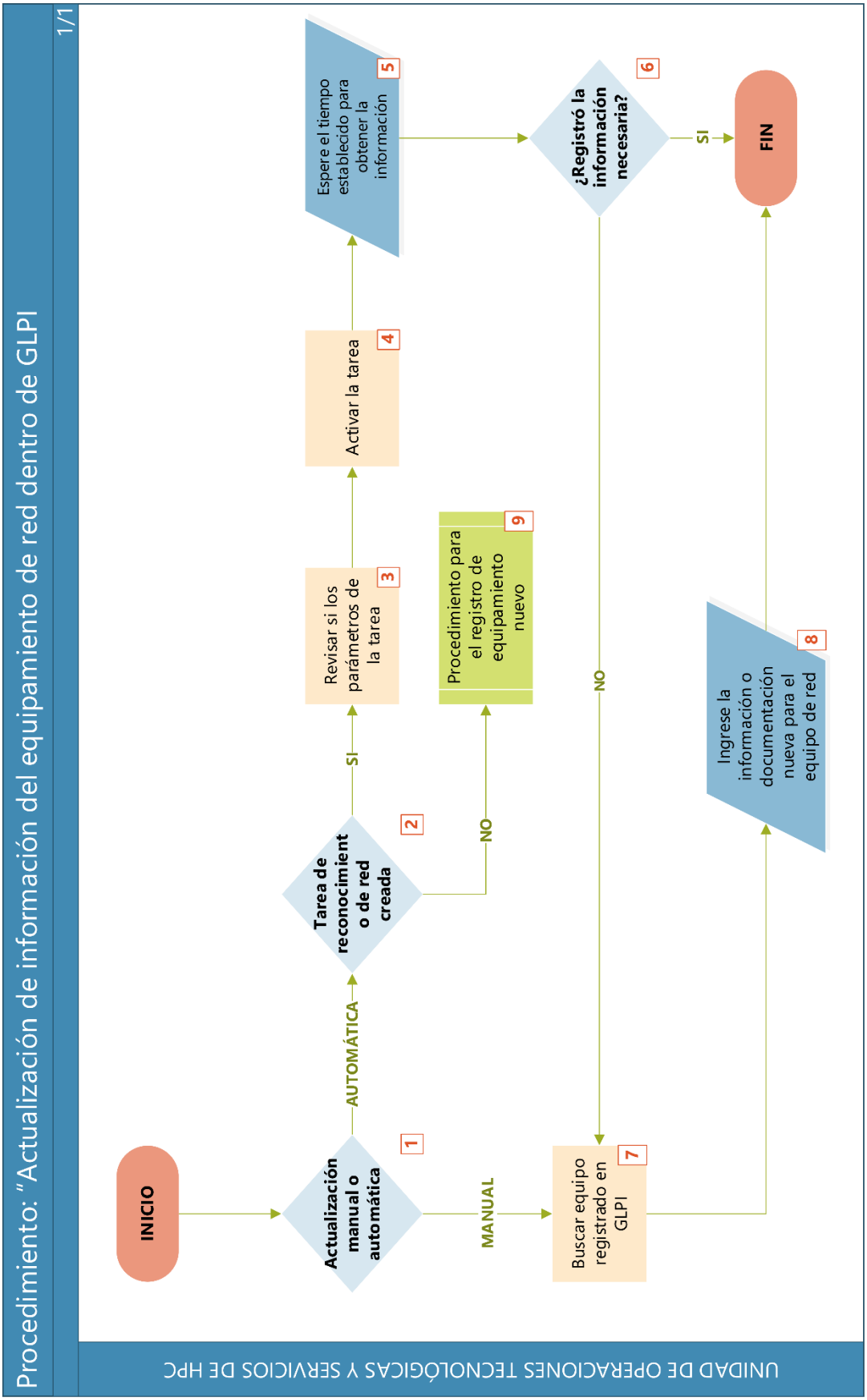


Figura 37. Procedimiento para la actualización de información de quipos de red

4.8.Registro de eventos e incidencias

GLPI se implementó principalmente para el registro de tickets de nivel dos, es decir eventos o incidencias de mayor gravedad que meritan de atención pronta, además de los que meritan un contacto con proveedores o entidades externas a la empresa.

En base a los procesos que maneja ITIL para el registro de eventos e incidencias y basados en el procedimiento para el registro de eventos e incidencias con el que cuenta Yachay, se puede resumir el escalado de un ticket de nivel uno a nivel dos en la Figura 38, donde el área requirente hace una petición mediante el registro del problema por medio de una llamada telefónica la UOTSHPC o mediante un correo electrónico a la dirección soporte@yachay.gob.ec,

El agente nivel 1 toma dicha solicitud analiza el problema, prioriza la solicitud y de estar en su competencia soluciona el evento o incidencia. En el caso que el agente nivel 1 no pueda resolver el problema envía un correo electrónico a la dirección soporten2@yachay.gob.ec, con el detalle de la inspección realizada y el problema encontrado, además si el agente puede priorizar el evento remite el correo electrónico con el código de evento o incidencia, para aplicar las acciones referentes a dicho nivel de prioridad.

El agente nivel 2 encargado del servicio o subservicio a quien se asignó el ticket, revisa en la plataforma GLPI el detalle del evento o incidencia encontrado y de estar en su competencia lo resuelve aplicando los procedimientos de acuerdo a su prioridad. En caso de que el agente nivel 2 encuentra una solicitud de n prioridad la cual merita una gestión con proveedores la realiza, e intenta resolver el incidente.

En el caso de que el evento o incidencia sea resuelto tanto el agente nivel 1 o el agente nivel 2 deben realizar el cierre del ticket con un informe técnico donde se detalle el proceso de solución aplicada.

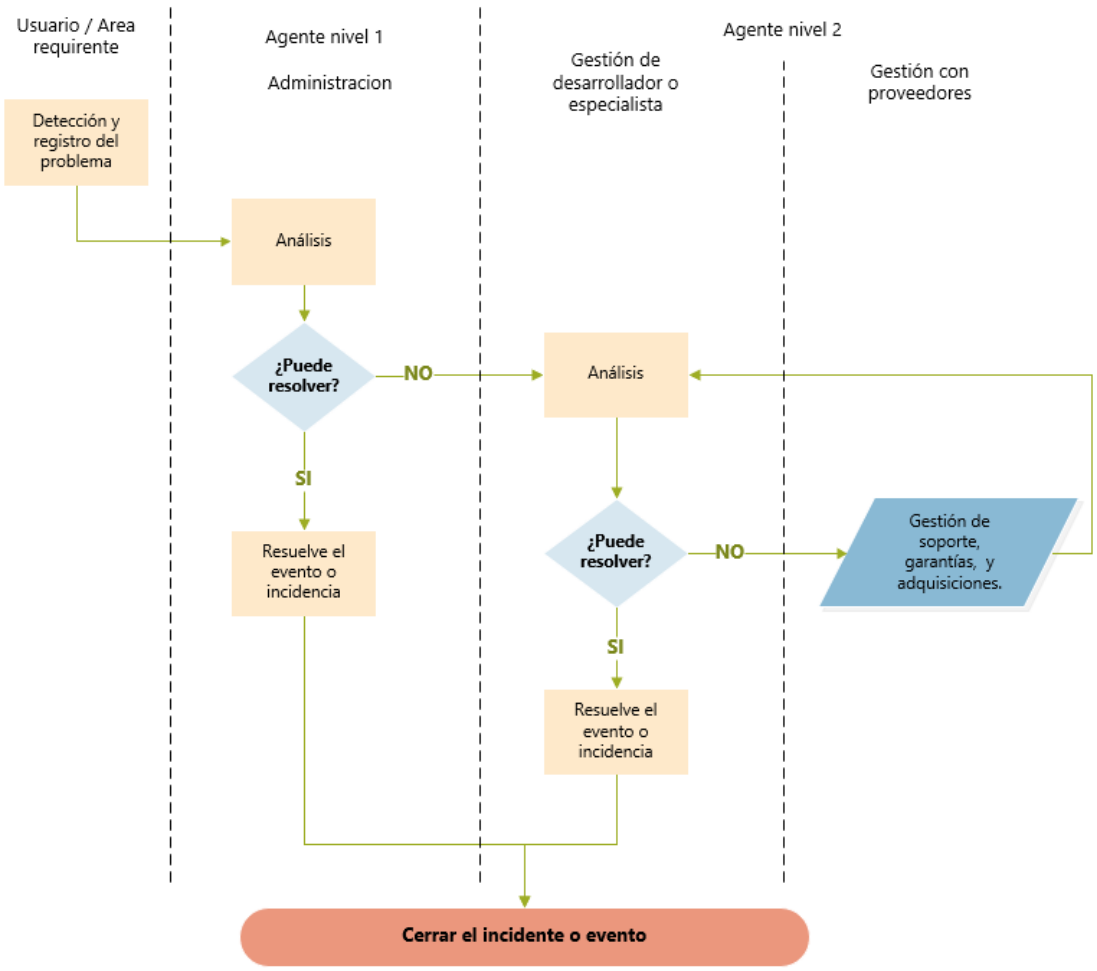


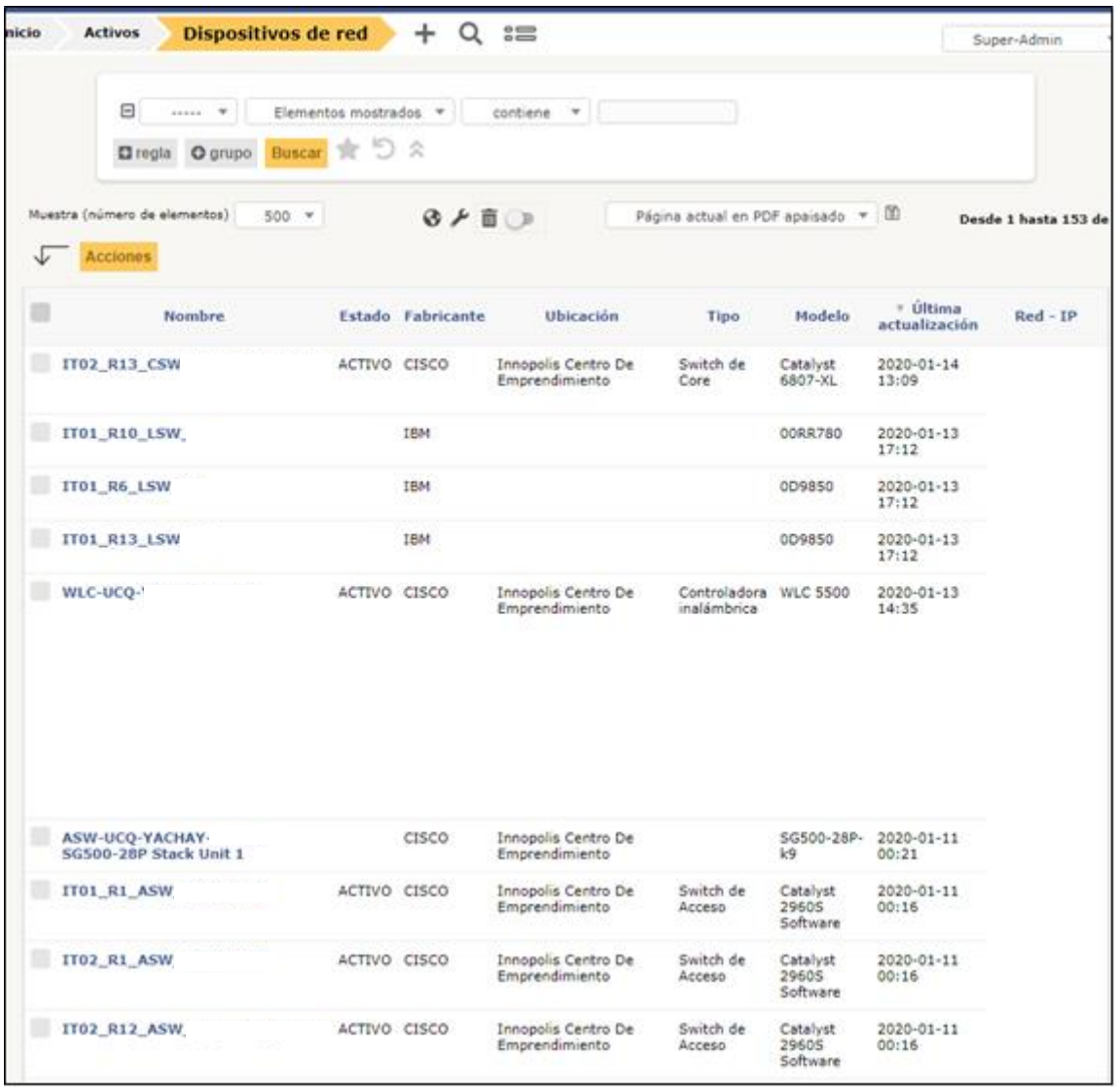
Figura 38. Escalado de eventos e incidencias

Fuente: Adaptado de (ITIL, 2014)

CAPITULO V. PRUEBAS DE FUNCIONAMIENTO Y RESULTADOS

5.1. Resultados del inventario automático

Al terminar con la ejecución de las tareas automáticas para el registro de equipamiento, dentro de GLPI se obtiene, de la información de los elementos de red encontrados al momento del escaneo del segmento de red como se lo aprecia en la Figura 39.



Nombre	Estado	Fabricante	Ubicación	Tipo	Modelo	Última actualización	Red - IP
IT02_R13_CSW	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Core	Catalyst 6807-XL	2020-01-14 13:09	
IT01_R10_LSW		IBM			00RR780	2020-01-13 17:12	
IT01_R6_LSW		IBM			0D9850	2020-01-13 17:12	
IT01_R13_LSW		IBM			0D9850	2020-01-13 17:12	
WLC-UCQ-'	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Controladora inalámbrica	WLC 5500	2020-01-13 14:35	
ASW-UCQ-YACHAY-SG500-28P Stack Unit 1		CISCO	Innopolis Centro De Emprendimiento		SG500-28P-k9	2020-01-11 00:21	
IT01_R1_ASW	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Acceso	Catalyst 2960S Software	2020-01-11 00:16	
IT02_R1_ASW	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Acceso	Catalyst 2960S Software	2020-01-11 00:16	
IT02_R12_ASW	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Acceso	Catalyst 2960S Software	2020-01-11 00:16	

Figura 39. Registro de Equipamiento de la red Data Center

Fuente: Interfaz GLPI

Al seleccionar un equipo de red de los que se han inventariado de manera automática se puede ver la información con la cual cuenta el dispositivo, esta información se la obtiene automáticamente mediante SNMP, en el caso de la información referente al usuario y técnicos responsables, el dominio, el grupo, contratos, costos, garantías y demás, debe ser incluida de manera manual.

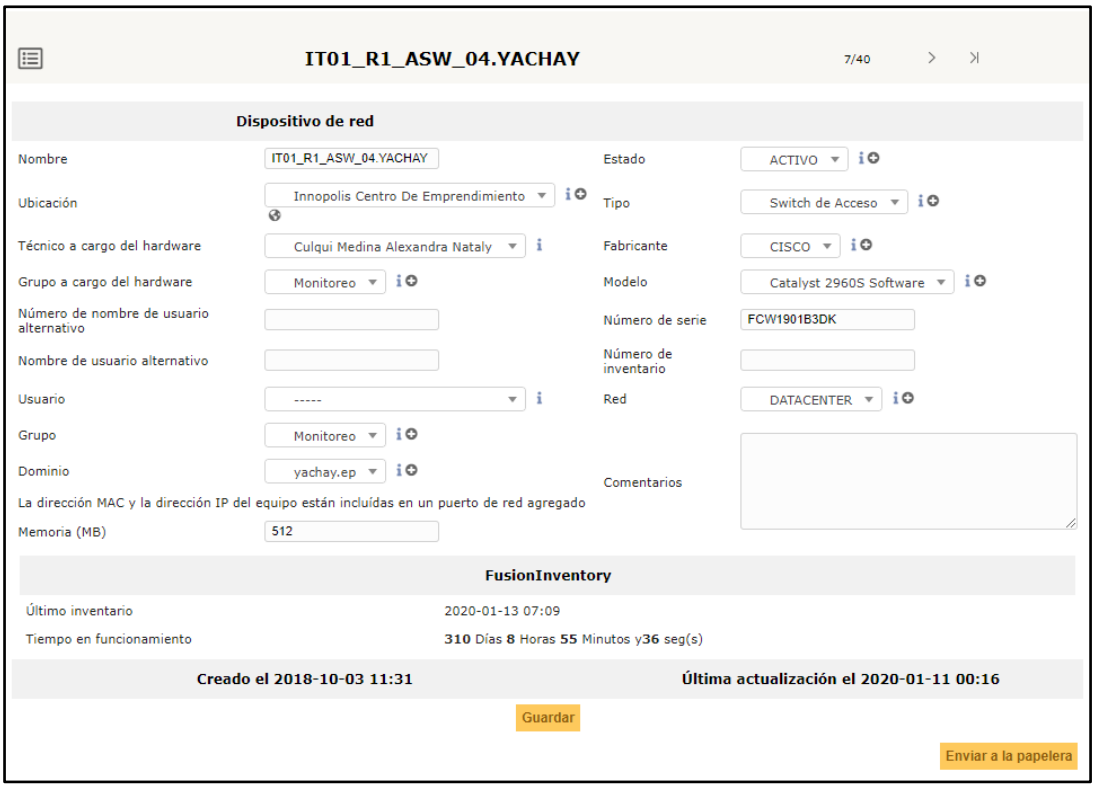


Figura 40. Información obtenida por SNMP del Switch 04 de la red Data Center.

Fuente: Interfaz GLPI

Nombre	MTU	Velocidad	Estado interno	Último Cambio	Tráfico recibido/enviado	Errores recividos/enviados	Duplex	Dirección MAC interna	VLAN
Fa0	1500	100 Mbps		1 minute, 31.32	- / -	- / -			
Gi1/0/1	1500	100 Mbps		230 days, 11:01:19.74	1 Go / 142 Mo	- / -	Completo		MONITOREO [46] U
Gi1/0/2	1500	100 Mbps		230 days, 11:01:42.30	1 Go / 142 Mo	- / -	Completo		MONITOREO [46] U
Gi1/0/3	1500	100 Mbps		230 days, 11:02:13.11	1 Go / 142 Mo	- / -	Completo		MONITOREO [46] U
Gi1/0/4	1500	100 Mbps		261 days, 13:35:46.46	1 Go / 142 Mo	- / -	Completo		MONITOREO [46] U
Gi1/0/5	1500	100 Mbps		310 days, 07:25:35.07	1 Go / 54 Mo	203 / -	Completo		MONITOREO [46] U
Gi1/0/6	1500	100 Mbps		270 days, 01:46:37.62	1 Go / 140 Mo	- / -	Completo		MONITOREO [46] U

Figura 41. Estado de los puertos de red del Switch 04 de la red Data Center.

Fuente: Interfaz GLPI

El registro de equipamiento de red ha permitido a la UOTSHPC tener un correcto registro de equipamiento dejando de lado los registros manuales y fácilmente manipulables, información como números de serie, modelos, fabricantes, módulos conectados dentro del dispositivo, las redes configuradas, tarjetas de red conectadas, redes directamente conectadas, software instalado e incluso el sistema operativo de los dispositivos (como se muestran en la Figura 40 y la Figura 41), son parámetros que se obtienen automáticamente mediante el escaneo SNMP, por lo que el registro actual y reportes que se obtienen depende de las necesidades y el nivel de detalle que el técnico responsable necesite.

Adicional al registro actual del equipamiento el técnico responsable o administrador del sistema pueden incluir información necesaria, ya sea documentación, fotos del estado del equipo, configuración o información que se crea relevante para ser almacenada y enlazada con el activo.

5.2. Gestión de tickets de nivel dos

Se ha realizado la gestión de tickets de nivel dos en el servidor GLPI, desde la generación de un ticket hasta brindar una solución completa, donde en primera instancia se envía un correo hacia la dirección soporten2@yachay.gob.ec, con el detalle de la inspección del agente nivel 1 y el código de procedimiento de la prioridad asignada por el agente nivel 1.

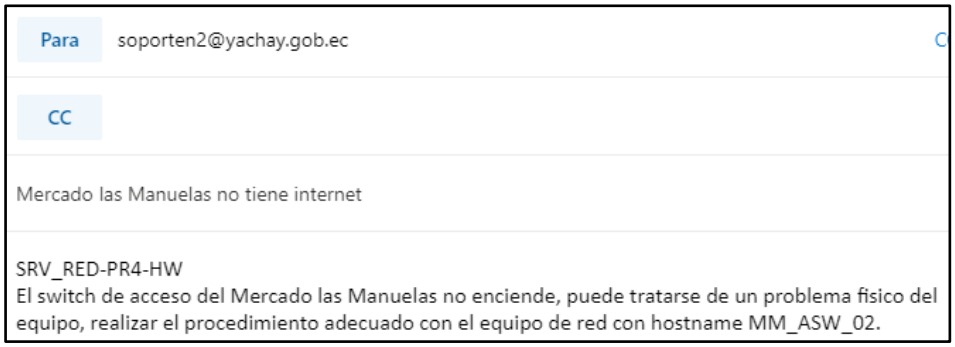


Figura 42. Envío de correo para generación de ticket

Fuente: Correo electrónico

Una vez que se ha enviado el correo, y para constatar que el ticket se creó de manera correcta se accede a la pestaña soporte en el menú peticiones, donde se puede verificar la creación del ticket.

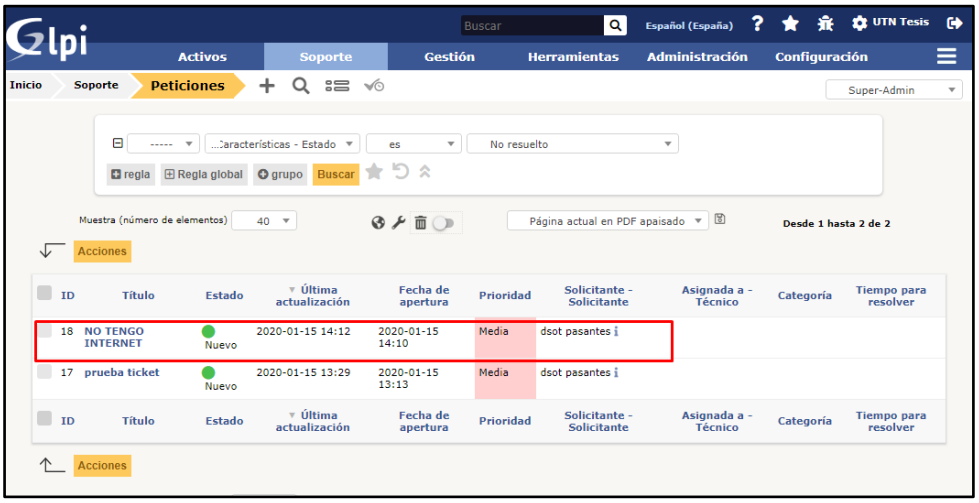


Figura 43. Creación automática de ticket basado en correo electrónico

Fuente: Interfaz GLPI

Al abrir el ticket de nivel 2 se llena la información principal que se muestra en la Figura 44, donde los parámetros que la UOTSHPC requiere se los detalla en la Tabla 34, esta información debe ser completada por el administrador del sistema, el gestor del ticket, o por el agente a cargo de la resolución del mismo.

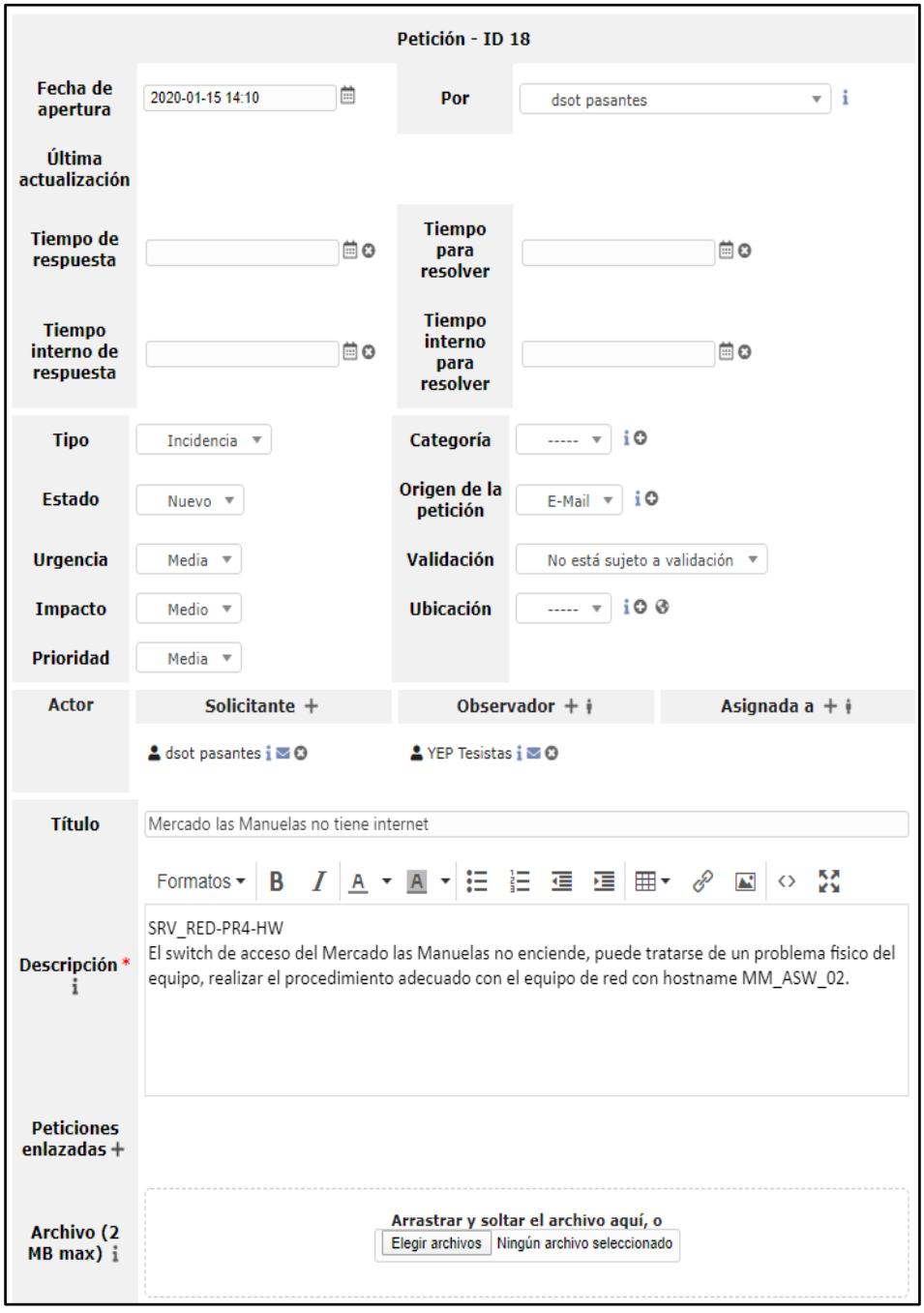


Figura 44. Registro de ticket.

Fuente: Interfaz GLPI

Tabla 34. Ítems para el registro de eventos o incidencias en GLPI

Item	DESCRIPCION
Fecha de apertura	Fecha en la cual se crea el ticket por parte del tecnico responsable o agente nivel 1.
Por	Nombre del usuario o tecnico solicitante.
Tiempo de respuesta	Se permite seleccionar un tiempo dentro del cual el agente nivel 2 debe revisar el problema a solucionar.
Tiempo para resolver	Se selecciona el tiempo maximo estimado para la solucion del ticket.
Tipo de ticket	Se selecciona si es una incidencia o es un evento
Categoría	Seleccionar dentro de este apartado el servicio o subservicio al cual ahce referencia este problema.
Actores	Permite el registro del Area Requirente o del agente nivel 1 como ente solicitante, el observador viene a ser el supervisor de la unidad o administrador encargado de la asignacion de tickets, y en la seccion “asignado a”, se selecciona el tecnico nivel 2 responsable de la solucion del ticket.
Estado	Permite seleccionar si el ticket esta activo, esta gestionando su solucion o si ya fue solucionado
Prioridad	Seleccione el nivel de prioridad del evento o incidencia registrado, si necesita puede hacer uso del campo urgencia e impacto para brindar una prioridad al problema.
Ubicacion	Seleccione el lugar geografico donde se presento la falla.
Titulo	Se registra el titulo que se le brinda al ticket generado en este caso el asunto del correo electronico enviado.
Descripción	Permite ingresar informacion que ayude al tecnico responsable a encontrar una solucion de la falla presentada en este caso el detalle del correo electronico enviado por el agente nivel 1
Archivo	De ser necesario se cargara adicionalmente uno o varios archivos de maximo 2MB que ayuden a describir la falla de manera mas detallada.
Submenu Elementos asociados	Este submenu permite el enlace directo con el elemento que presnta la falla pudiendo ser equipos de red o equipos de usuario previamente registrados.

Al gestionar un ticket de nivel 2 dentro de la plataforma, y al tener de manera centralizada la informacion, el agente nivel 2 puede tratar el evento o incidencia de forma mas detallada, de manera que el agente puede asociar al problema un elemento registrado en el cual

se ha originado la falla, ademas al tener informacion referente a contratos y garantias, se puede acceder a esta información sin necesidad de la busqueda de esta informacion en archivos de de excel o documentacion archivada en documentos virtuales, con esta centralizacion de informacion tanto el agente nivel 2 como el agente nivel 1 tienen un mejor seguimiento del proceso que permite la resolucion del evento o incidente.

5.3.Resultados obtenidos

Mediante la implementación del sistema de configuración se obtuvieron como beneficios para la Empresa Pública Yachay E.P. en especial para la UOTSHPC, los siguientes:

- El sistema permite el escaneo de red, para el registro del equipamiento, lo que hace que varios equipos instalados sean inventariados a detalle con sus componentes internos de hardware e incluso de software en el caso de ser necesario, dentro de una base de datos interna del sistema, evitando de esta manera que el técnico responsable realice el inventario detallado de manera manual en hojas de Excel u otro tipo de documentos el cual tomaba 15 a 20 minutos por cada equipo, reduciendo notablemente el tiempo de inventariado ya que con el sistema puede realizar el escaneo de un equipo de red en un lapso de 20 a 30 segundos y una red completa en un tiempo máximo de 120 minutos dependiendo de la cantidad de equipos conectados (254 equipos máximo por segmento de red), reduciendo su registro en un 95% del tiempo.
- La información del inventario automático del sistema puede ser agregada, modificada o borrada de manera manual según las necesidades del técnico responsable o del administrador del sistema, además el sistema permite la

actualización automática del inventario mediante el escaneo de red, permitiendo de esta manera tener un inventario actualizado.

- El sistema permite la gestión del activo, de manera que se puede registrar contratos, garantías e incluso contactos de proveedores y enlazarlos al equipamiento previamente registrados en el inventario, para que en el caso de suscitarse un problema que escale a nivel 2 el técnico responsable pueda gestionar su solución manteniendo la información centralizada en la plataforma, evitado de esta manera la pérdida de tiempo en la búsqueda de documentos físicos o digitales que contengan información referente al activo.
- El técnico responsable del equipamiento o del sistema pueden generar reportes de los problemas asociados con uno o varios equipos según sea necesario, ayudando de esta manera a la toma de decisiones en cuanto a la administración de la red.

CONCLUSIONES

Para las empresas que brindan diferentes servicios en una red es importante tener una buena gestión de inventarios centralizada, una buena gestión de eventos e incidencias, y una centralizada gestión de proveedores y SLAs, por lo que en este proyecto se ha enmarcado en la gestión de configuración del modelo FCAPS juntamente con las buenas prácticas de ITIL, para seleccionar la mejor herramienta que permita realizar estos procesos.

Una vez realizado el análisis sobre la red, los servicios y los procesos para el registro de equipamiento y para la gestión de tickets con la que cuenta Yachay E.P., se obtuvieron los requerimientos necesarios para la implementación del sistema, así como también parámetros necesarios para la generar una priorización de eventos e incidencias conforme a lo mencionado en las buenas prácticas de ITIL.

La implementación del sistema ha permitido a la empresa tener un registro completo del equipamiento de networking de la red Data Center de manera automática y complementando la información del activo o documentación referente al mismo de manera manual, de esta forma centralizando la información necesaria para la gestión de tickets de nivel 2, facilitando al técnico responsable la solución del mismo en el caso de tener que gestionar una solución con un ente externo.

El sistema presenta un beneficio para la UOTSHPC en cuanto al ahorro de tiempo al realizar un inventariado mediante el escaneo de la red, ya que presenta una reducción del 98% del tiempo para el registro del equipo, además evita los errores que pueden presentarse al tomar datos de los equipos de manera manual o digitarlos en hojas de cálculo de Excel, así también se reduce el tiempo de búsqueda de documentación referente a los equipos ya que esta información es registrada por el técnico responsable del activo y lo asocia al mismo.

RECOMENDACIONES

Se recomienda el uso de la herramienta GLPI a toda persona que sepa de criterios de redes y configuraciones, es decir a técnicos de soporte de redes ya que este sistema necesita de conocimientos puntuales en cuanto a configuración y rendimiento en redes.

El uso de la herramienta debe ser constante y nunca debe dejar de ser monitoreada debido a que puede incluir duplicidad de información, además dentro del marco de las buenas prácticas de ITIL se recomienda que siempre la empresa debe estar en un cambio constante adaptándose a las necesidades tanto de la empresa como del sector al que brinda el servicio, por lo cual se recomienda además que el registro de todo equipamiento en general de la empresa se incluya en este sistema (GLPI) para poder realizar cualquier gestión a nivel de red tanto de equipos finales de usuarios como equipos de red, que la empresa maneja.

Para que la información del equipamiento registrado en el sistema sea actualizada constantemente y de manera automática, se recomienda configurar tiempos de ejecución de escaneo de la red en horarios en los que esta se encuentre menos congestionada para que las tareas se ejecuten de manera más rápida.

La gestión de configuración de las FCAPS tiene una referencia directa con la conservación de la información del diseño y configuración actual, como ITIL lo hace en su gestión de activos y configuración de servicios, por lo cual se recomienda que las configuraciones realizadas mediante scrips, fotografías e información referente al estado actual del equipo se lo registre dentro de la plataforma.

Se recomienda a la UOTSHPC implementar un servidor de Backup, para que en el caso de presentarse un fallo inesperado del mismo la unidad pueda contar con la información necesaria hasta que se solucione el inconveniente presentado con el servidor principal, así también se recomienda a la unidad mantener un Backup de la base de datos de la herramienta para evitar daños o perdida de la información, todo esto se menciona en las buenas practicas de ITIL en cuanto a la mejora constante y seguridad de las herramientas implementadas dentro de la empresa.

BIBLIOGRAFÍA

Padmavathy Sankaran. (2017). *ITIL Change Management - A Beginner's Guide.*

Acosta Maza, B. (2017). *Implementación de un sistema de gestión de redes en RTVA.* España.

Agudelo, O. (2001). *Arquitectura de administración OSI*. Retrieved from http://www.arcesio.net/osinm/osinmfuncion.html

Alarcón Ávila, R. (2017). Gestion y administracion de redes como eje temático de investigación. *AVANCES Investigación en Ingeniería*, 109-111.

Ayala Yandun, V. E. (2015, Octubre 21). *Modelo de Gestión de Red Funcional en la Red Local de Datos del Gobierno Autónomo Descentralizado de San Miguel de Ibarra basado en el Estándar ISO.*

Bi-Tecing. (2014). *Servicios Basados en ITIL*. Retrieved from http://www.bi-tecing.com/bi-tecing/itil.php

Bosmediano Cárdenas, C. P. (2017). *Administración y gestión de usuarios para acceso a la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas basado en el protocolo 802.1x.* Ibarra.

CERTGUIDANCE. (2018). *ITIL Access Management Process Activities*. Retrieved from https://i1.wp.com/www.certguidance.com/wp-content/uploads/2017/11/SO050-ITIL-Access-Management-Process-Lifecycle-Activities.png?w=600&ssl=1

CERTGUIDANCE. (2018). *ITIL Continual Service Improvement* . Retrieved from https://i1.wp.com/www.certguidance.com/hiresimg/ITLF/CS001%20Seven%207%20Steps%20of%20CSI%20and%20Deming%20Cycle%20Mapping.jpg?ssl=1

CERTGUIDANCE. (2018, Marzo 22). *ITIL Event Management Process*. Retrieved from https://i2.wp.com/www.certguidance.com/hiresimg/ITLF/SO010-ITIL-Event-Management-Process-Flow.png?ssl=1

Cherwell. (2018). *The Essential Guide to ITIL Incident Management*. Retrieved from https://www.cherwell.com/library/essential-guides/essential-guide-to-itil-incident-management/

CHERWELL. (2018). *The Essential Guide to ITIL Incident Management*. Retrieved from https://www.cherwell.com/library/essential-guides/essential-guide-to-itil-incident-management/

Chiavenato, I. (2014). *Introducción a la Teoría General de la Administración* (Septima ed.). McGraw-Hill Interamericana.

CIC. (2019, Febrero 20). *¿Qué es Network Fault Management o la Gestión de fallos de red?* Retrieved from https://www.cic.es/que-es-network-fault-management-o-la-gestion-de-fallos-de-red/

CISCO. (2014, Mayo 29). *Introduction to Cisco IOS NetFlow*. Retrieved from https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

CISCO. (2014). *Simple Network Management Protocol.* Retrieved from https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/managed_services/8_6_1/cucm/managed_services/snmp.pdf

Contraloria General del Estado. (2009). *NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO.* Quito.

Debian. (2019). *Cumplir los requisitos mínimos de hardware*. Retrieved from https://www.debian.org/releases/jessie/i386/ch03s04.html.es

Foroughi , A. (2014). *Network Management.*

FusionInventory. (2019). *FusionInventory Overview*. Retrieved from http://fusioninventory.org/overview/

GLPI Project. (2018, 02). *GLPI.* Retrieved from https://glpi-project.org/es/manejo-de-activos-e-inventario-automatico-de-ti/

GLPI Project. (2019). *GLPI installation*. Retrieved from https://glpi-install.readthedocs.io/en/latest/index.html

Guzmán López, A. (2016). *Introducción a la Gestión de Redes.* Retrieved from https://docplayer.es/9434597-1-introduccion-a-la-gestion-de-redes.html

ISO. (2015). *Glosario* . Retrieved from Norma ISO 9001: http://www.normas9000.com/content/Glosario.aspx

ITIL. (2014). *ITIL® Foundation Handbook 3rd ed.* TSO.

ITIL. (2015). *ITIL V3 - Service Transition.* Londres: TSO.

iTop & Combodo. (2019, 01). *ITOP*. Retrieved from https://www.combodo.com/itop-193

iTop. (2018, 12). *iTop For ALL*. Retrieved from https://www.combodo.com/itop-193

iTop Hub. (2018, 12 19). *Installing iTop*. Retrieved from https://www.itophub.io/wiki/page?id=2_1_0%3Aadmin%3Ainstalling_itop

Kurose, J. (2016). *Redes de Computadoras.* Estados Unidos: Pearson.

Kurose, J., & Ross, K. (2016). *Computer Networking: A Top-Down Approach.* Pearson.

Lara Garcia, H. (2015). *Gestion de Redes.* Retrieved from https://slideplayer.es/slide/14480920/

M2M. (2016). Retrieved from https://www.m2maplicaciones.es/es/servicios/lectura-remoto-sensores-IoT/1/

McCloghrie, K. (1991). Concise MIB Definitions. *Request for Comments 1212*.

Microsoft. (2019, Julio 02). *Consideraciones sobre el uso de memoria para el ajuste del rendimiento*. Retrieved from https://docs.microsoft.com/es-es/windows-server/administration/performance-tuning/role/active-directory-server/memory-usage-considerations

OCS Inventory. (2019, 02). *A propos d'OCS Inventory*. Retrieved from https://ocsinventory-ng.org/?lang=fr

Oracle. (2016). *SNMP Agent MIB Reference.* Retrieved from https://docs.oracle.com/cd/E13203_01/tuxedo/tux81/snmpmref/1tmib.htm

Paessler , A. (2019). *IT Explained: Active Directory*. Retrieved from https://www.es.paessler.com/it-explained/active-directory

PAESSLER. (2019). *MIB browser.* Retrieved from PRTG Network Monitoring: https://www.es.paessler.com/mib-browser

Perle Systems. (2016). *Despliegues a Gran Escala. Conversores de Medio, Extensores Ethernet y Switches Industriales*. Retrieved from https://www.perlesystems.es/supportfiles/fcaps.shtml

Ramírez Indacochea, G. D., & Robalino Cárdenas, A. E. (2014). *Diseño e implementacion de servicios de virtualizacion de los servidores que operan en el centro de operaciones de la red (NOC) de la facultad de ingenieria en sistemas.* Quito.

Ren, J., & Li, T. (2016). *Network Management.* Michigan.

Rizos, C. (2013). *Security Management in the FCAPS model*. Retrieved from https://www.snmpcenter.com/security-management-fcaps/

Rizos, C. (2016). *Introduction to FCAPS – Fault, Configuration, Accounting, Performance, Security*. Retrieved from https://snmpcenter.com/fcaps-network-management/

Rouse, M. (2007). *FCAPS (gestión de fallos, configuración, contabilidad, rendimiento y seguridad)*. Retrieved from https://searchnetworking.techtarget.com/definition/FCAPS

Shingote, S., & Bagwe, S. (2018, 12). *Compare between SNMP v1, SNMP v2 and SNMP v3.* Retrieved from http://www.ques10.com/p/3301/compare-between-snmp-v1-snmp-v2-and-snmp-v3-1/

Significados.com. (2017, Marzo 09). *Significado de Gestión*. Retrieved Abril 3, 2019, from https://www.significados.com/gestion/

Techopedia. (2011). *What is Fault Configuration Accounting Performance Security (FCAPS).* Retrieved from https://www.techopedia.com/definition/24512/fault-configuration-accounting-performance-security-fcaps

Tucker, G. (2016, Enero 06). *Change Types*. Retrieved from https://www.itsminfo.com/change-types/

UIT-T X.680. (2015). *Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

Yachay. (2018). *Ubicacion Geografica - Empresa Pública Yachay EP*. Retrieved from www.yachay.gob.ec/ubicacion-geografica/

Yachay E.P. (2016). *Resolucion N0. YACHAY EP-GG-2016-0042.* Urcuquí.

Yachay E.P. (2017). *Atencion de Requerimientos de Soporte Tecnológico.* Urcuquí.

Yachay E.P. (2019). Estructura orgánica funcional. *Estatuto Orgánico de Gestión Organizacional por Procesos*.

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

CI elemento de configuración

CMDB: Base de datos de gestión de la configuración, es un repositorio que está diseñado para almacenar muchos de los componentes de un sistema de información.

CMS: Sistema de gestión de la configuración, incluye todas las herramientas para un buen proceso de Gestión de Configuración y Activos del Servicio una de estas herramientas es la CMDB

DML; Biblioteca Definitiva de Medios, repositorio seguro en el que las versiones autorizadas definitivas de todos los medios de comunicación, software, licencia de CIS están almacenados y protegidos

DOTSHPC: Dirección de Operaciones Tecnológicas y Servicios HPC.

HPC: High Performance Computing, comprende a un computador de alto rendimiento que permite la resolución de problemas complejos de manera más rápida.

IETF: Internet Engineering Task Force (en español, Grupo de Trabajo de Ingeniería de Internet1) es una organización internacional abierta de normalización.

ISO: (International Organization for Standarization) organización internacional para estandarización de tecnologías, procesos de pruebas científicas, condiciones de trabajo problemas sociales, entre otros

Mesa de Servicio: en inglés Desk Service, es un centro de comunicaciones que proporciona un único punto de contacto entre una empresa y sus clientes, empleados y socios comerciales

Operación Normal del Servicio: se define como un estado operacional, donde los servicios y los IC se desempeñan dentro de sus niveles de servicio y operacionales acordados con el cliente.

OSI: (Open Sysem Interconnection), es un modelo desarrollado por la ISO el cual divide las comunicaciones en siete capas y cada una cumple sus tareas específicas hasta completar la comunicación.

RFC: (Request For Coments) son documentos numerados que describen y definen protocolos, métodos, conceptos y programas de Internet, la gestión de estos documentos la realiza la IETF

Servicios de TI: se lo denomina al conjunto de actividades que tienen la finalidad de responder las necesidades de un cliente de tal manera que el valor de este servicio sea potenciado y sus costos de operación y riesgo reducidos

SNMP Traps: son mensajes enviados de forma remota desde los dispositivos SNMP activos hacia el agente SNMP, comunicando de esta manera eventos de la red.

SSH: protocolo de comunicación que permite el acceso remoto al dispositivo.

TI: Tecnologías de la Información, comprende a equipos de telecomunicaciones y ordenadores que permiten el procesamiento de información.

ANEXOS.

ANEXO 1: Registro de equipamiento previo a la implementación del sistema

ÍTEM	SECTOR	DISPOSITIVO	MODELO	MARCA	CANT.	DESCRIPCIÓN	HOSTNAME
11	DCU	Switch de Core	CISCO C6807-XL	CISCO	1	Catalyst 6807-XL 7-slot chassis, 10RU	S/N
53	DCU	Switch de Distribución	WS-C4500X-16SFP+	CISCO	1	Cisco ONE Catalyst 4500-X 16 Port 10G IP Base, Front-to-Back	DSW-UCQ-YACHAY-DC-01
76	DCU	Switch de Acceso	WS-C2960X-24PD-L	CISCO	1	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	ASW-UCQ-YACHAY-DC-01

ÍTEM	SERIAL NUMBER	VERSION	IOS	MAC	MODULO / PUERTO	UBICACIÓN ACTUAL
11	SERIE-DEL-EQUIPO	15.1	s2t54-ADVIPSERVICESK9-M			DATA CENTER URCUQUÍ - YACHAY IT02 - RACK N
53	JAE194700W8					DATA CENTER URCUQUÍ - YACHAY 2 IT02 - RACK N
76	FOC1943Y14G	15.0(2a)EX5	C2960X-UNIVERSALK9-M			DATA CENTER URCUQUÍ - YACHAY 2 IT02 - RACK N

ÍTEM	ESTADO	CONTRATO / PROYECTO	OBSERVACIONES CONTRATO / PROYECTO	OBSERVACIONES EQUIPO	CÓDIGO YACHAY E.P.	IP
11	Operativo	Contrato Yachay EP No. 0147-2014 Proyecto DataCenter/ Canje de deuda				IP
53	Operativo	CEIEC. CONTRATO NRO. 0047-2015 PROTOCOLIZADO DEL PROYECTO DE INFRAESTRUCTURA ELÉCTRICA Y DE TELECOMUNICACIONES.				IP
76	Operativo	CEIEC. CONTRATO NRO. 0047-2015 PROTOCOLIZADO DEL PROYECTO DE INFRAESTRUCTURA ELÉCTRICA Y DE TELECOMUNICACIONES.				IP

ANEXO 2: Actas de reuniones realizadas

YACHAY CIUDAD DEL CONOCIMIENTO	**Acta de Reunión de Trabajo** *Dirección de Operaciones Tecnológicas y Servicios de Computación de Alto Rendimiento*	GOBIERNO NACIONAL DE LA REPÚBLICA DEL ECUADOR
	ACTA DE REUNIÓN DE TRABAJO	

Fecha de reunión:	12 de junio del 2019
Hora de inicio:	11:00
Hora de conclusión:	12:00
Lugar:	Urcuquí
Realizado por:	Fernando Ortíz

Proyecto:	Implementación de servidor para gestión de activos
Tema de reunión:	Dimensionamiento para la máquina virtual

Asistentes:

Nombres	Institución	Teléfonos	Email	Firma
Fernando Ortíz	Yachay E.P.	0993648457	bortiz@yachay.gob.ec	
Jonathan Terán	UTN	0983932884	jgterane@utn.edu.ec	

Orden del día:

- Definición de recursos mínimos y operativos para el servidor GLPI.
- Creación de la máquina virtual para GLPI.

Sumillas de Participantes:	

YACHAY CIUDAD DEL CONOCIMIENTO	Acta de Reunión de Trabajo *Dirección de Operaciones Tecnológicas y Servicios de Computación de Alto Rendimiento*	GOBIERNO NACIONAL DE LA REPÚBLICA DEL ECUADOR
	ACTA DE REUNIÓN DE TRABAJO	

Antecedentes:

Se ha seleccionado la herramienta de gestión de activos GLPI para la implementación en la Empresa Pública Yachay E.P.

Observaciones:

Se ha investigado y definido parámetros mínimos para la implementación del sistema operativo (Debian 9) y los complementos necesarios de la herramienta GLPI.
Se ha estimado un 25% de sobredimensionamiento de la capacidad estimada para disco duro y memoria RAM por experiencia técnica para el mejor rendimiento del servidor.

Acuerdos/Compromisos:

N°	Descripción	Responsable Empresa/Persona	Fecha creación	Fecha propuesta	Fecha de cierre Cumplido/Pendiente
1	Creación de la máquina virtual	Fernando Ortiz	12/06/2019	12/06/2019	
2	Instalación de Sistema operativo Debian 9	Fernando Ortiz	12/06/2019	12/06/2019	
3	Instalación de GLPI	Jonathan Terán	12/06/2019	26/06/2019	

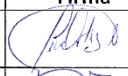
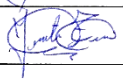
Sumillas de Participantes:	

YACHAY CIUDAD DEL CONOCIMIENTO	**Acta de Reunión de Trabajo** *Dirección de Operaciones Tecnológicas y Servicios de Computación de Alto Rendimiento*	GOBIERNO NACIONAL DE LA REPÚBLICA DEL ECUADOR
	ACTA DE REUNIÓN DE TRABAJO	

Fecha de reunión:	29 de mayo del 2019
Hora de inicio:	10:00
Hora de conclusión:	12:00
Lugar:	Urcuquí
Realizado por:	Fernando Ortíz

Proyecto:	Implementación de servidor para gestión de activos
Tema de reunión:	Definición de características para registro de activos y registro de tickets

Asistentes:

Nombres	Institución	Teléfonos	Email	Firma
Fernando Ortíz	Yachay E.P.	0993648457	bortiz@yachay.gob.ec	
Jonathan Teran	UTN	0983932884	jgterane@utn.edu.ec	

Orden del día:

- Definición de los parámetros mínimos para el registro de equipamiento de la red Data Center.
- Definición de las características mínimas para el registro de tickets generados para la solución de eventos e incidencias, con la finalidad de tener una mejor selección de la herramienta.

Sumillas de Participantes: 	Pág. 1

YACHAY CIUDAD DEL CONOCIMIENTO	**Acta de Reunión de Trabajo** *Dirección de Operaciones Tecnológicas y Servicios de Computación de Alto Rendimiento*	GOBIERNO NACIONAL DE LA REPÚBLICA DEL ECUADOR
	ACTA DE REUNIÓN DE TRABAJO	

Antecedentes:

Observaciones:

Se han definido como parámetros mínimos para el registro de equipamiento los siguientes:

- Nombre descriptivo del equipo.
- Marca del equipo de red.
- Modelo del equipo de red.
- Dirección IP de gestión configurada en el equipo de red.
- Nombre del equipo dentro de la red.
- Cantidad de puertos con los que cuenta el equipo de red.
- Número de serie descriptiva única del equipo de red (MAC).
- Lugar físico de ubicación del equipo de red.
- Nombre de el o los responsables del equipo.
- Registro de incidentes y eventos generados con el equipo.

Nota: Estos elementos pueden ser incluidos de forma manual o automática mediante SNMP

Se han definido como parámetros mínimos para el registro de ticket, los siguientes elementos:

- Numero identificativo de evento o incidencia
- Cuál es el daño encontrado
- Lugar físico de ubicación donde se tiene el fallo
- Nombre de el o los responsables encargado(s) de brindar soporte
- Dirección IP de gestión configurada en el equipo de red con falla.

Sumillas de Participantes:	

YACHAY CIUDAD DEL CONOCIMIENTO	**Acta de Reunión de Trabajo** *Dirección de Operaciones Tecnológicas y Servicios de Computación de Alto Rendimiento*	GOBIERNO NACIONAL DE LA REPÚBLICA DEL ECUADOR
	ACTA DE REUNIÓN DE TRABAJO	

- Nombre del equipo dentro de la red.
- Permitir registrar el o los cambios generados para solventar el fallo registrado

Todos estos elementos son definidos con la finalidad de hacer una mejor selección de la herramienta que permita

Acuerdos/Compromisos:

N°	Descripción	Responsable Empresa/Persona	Fecha creación	Fecha propuesta	Fecha de cierre Cumplido/Pendiente
1	Selección del servidor que cumpla con los parámetros definidos	Jonathan Teran	29/05/2019	12/06/2019	
2					
3					

Sumillas de Participantes:	
	Pág. 3

EMPRESA PÚBLICA SIEMBRA E.P.

DIRECCIÓN DE OPERACIONES TECNOLÓGICAS Y SERVICIOS DE COMPUTACIÓN DE ALTO RENDIMIENTO.

SIEMBRA

ACTA REUNIÓN

Instituciones Participantes: Siembra E.P. y Universidad Técnica del Norte	Fecha: 12 - Febrero - 2020	Hora de inicio: 10:00
Realizado por: Nataly Culqui	Lugar: Uruguay	Hora de fin: 11:00
Tema: Priorización de Eventos e Incidencias aplicando las Buenas Prácticas de Itil.		

Contenido de la Reunión	Acuerdos Establecidos
Definición de niveles de Impacto y Urgencia Niveles de Prioridad, definición de Códigos, Categorización de eventos e incidencias para cada nivel de Prioridad Definición del Procedimiento a seguir en cada nivel de Prioridad.	Códigos de Prioridad establecidos Criterios para que un evento o incidencia recaiga en un nivel de Prioridad Procedimiento a seguir en cuanto a la prioridad y el nivel de Servicio.

Nombres y Apellidos	Cargo	Institución	Teléfono	Correo Electrónico	Firma
Jonathan Terán		UTN	0983932884	jgteran e@utn.edu.ec	
Nataly Culqui	Técnico DOTSCAR	Siembra E.P	0980438045	aculqui@yachay.gob.ec	

ANEXO 3: ANEXO 3 ISO/IEC/IEEE 29148

INTERNATIONAL STANDARD

ISO/IEC/ IEEE 29148

First edition
2011-12-01

Systems and software engineering — Life cycle processes — Requirements engineering

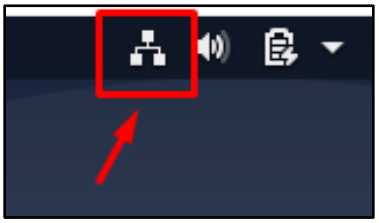
Ingénierie des systèmes et du logiciel — Processus du cycle de vie — Ingénierie des exigences

Reference number
ISO/IEC/IEEE 29148:2011(E)

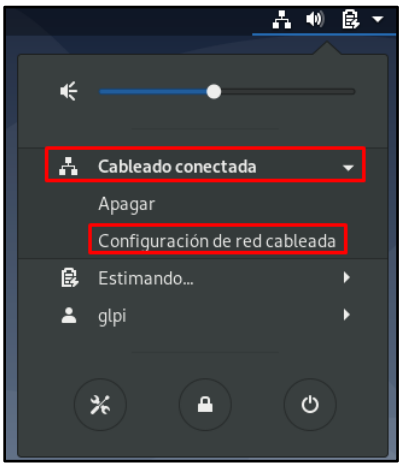
ANEXO 4: Configuración básica de GLPI

A. Configuración de interfaz de red

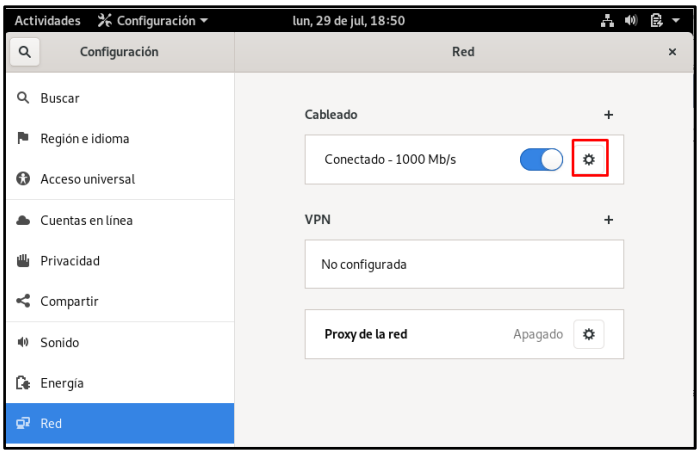
Al tener una máquina virtual en modo grafico su configuración se la realizara mediante la interfaz, para lo cual, en la pantalla principal, en la parte superior derecha se encuentra un icono de configuración de red como se muestra en la en la imagen inferior, donde se debe hacer un clic y se mostrara un menú contextual



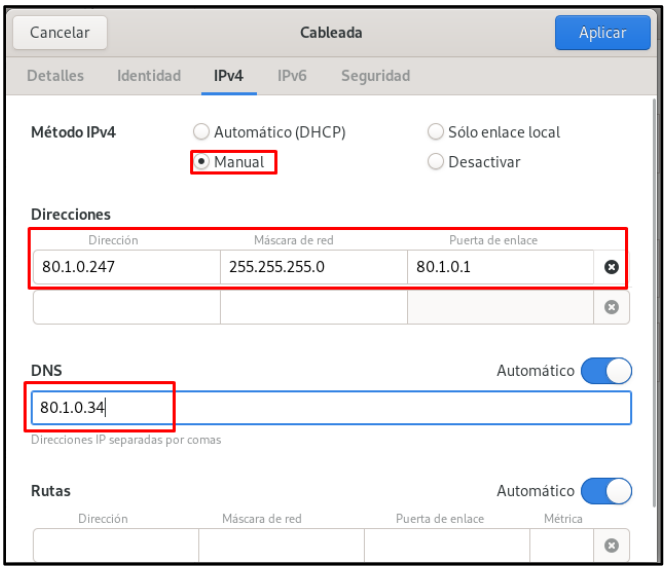
Dentro del menú que se seleccionara la opción “Cableado conectada” y posteriormente la opción “Configuración de red cableada”.



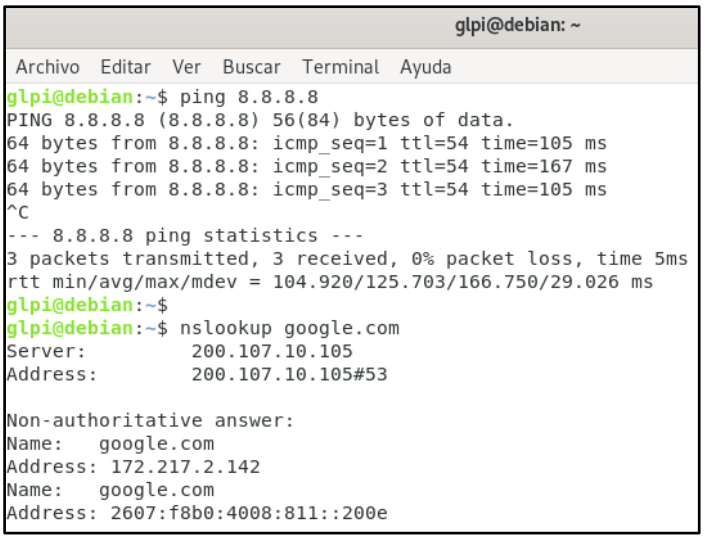
Al ingresar en esta opción abrirá una ventana de configuración como se muestra en la figura a continuación, donde se debe seleccionar el icono de configuración de la interfaz de red por la cual nos estamos conectando a la red interna.



Dentro de la ventana que se abre, se selecciona la pestaña “IPv4”, y se escoge el método de IPv4 “Manual”, y se llenara la información de acuerdo a la Tabla 32, que describe los elementos necesarios para la configuración de la red. Al completar la configuración contiene la información que se muestra en la siguiente imagen, posterior a esto se hace clic en aplicar para guardar los cambios. Al terminar esta configuración de red, es recomendable reiniciar la interfaz de red o a su vez reiniciar la máquina virtual.



Para verificar que la maquina tiene acceso a Internet se hace un ping hacia Google a la IP 8.8.8.8 con el comando ***ping 8.8.8.8*** y para probar el funcionamiento del DNS se ejecuta el comando ***nslookup google.com***, dentro del terminal de Debian.



B. Configuración de SSH

Previamente a la instalación de la herramienta se necesita tener habilitado el protocolo de comunicación SSH, para lo cual en el terminal de la máquina virtual con Debian se accede a modo root con el comando: ***su*** y con la contraseña de root, como se muestra en la imagen.

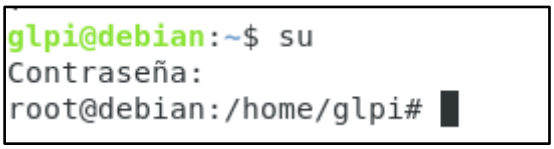
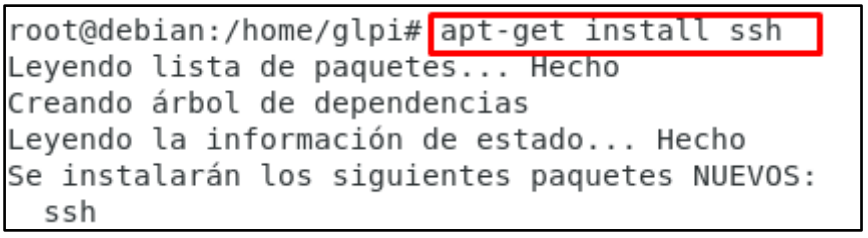


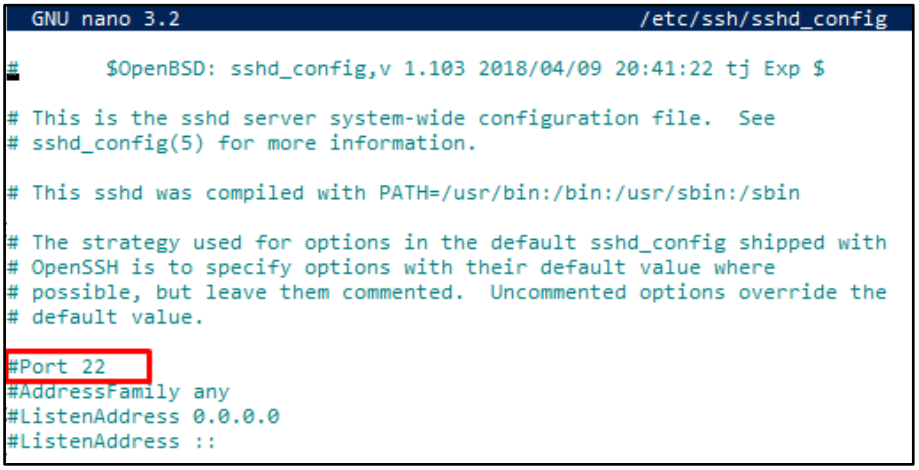
Figura 45. Acceso como usuario root en Debian

Fuente: Captura Debian.

En la máquina virtual y para el acceso remoto se habilitará SSH, mediante el comando: **apt-get install ssh**



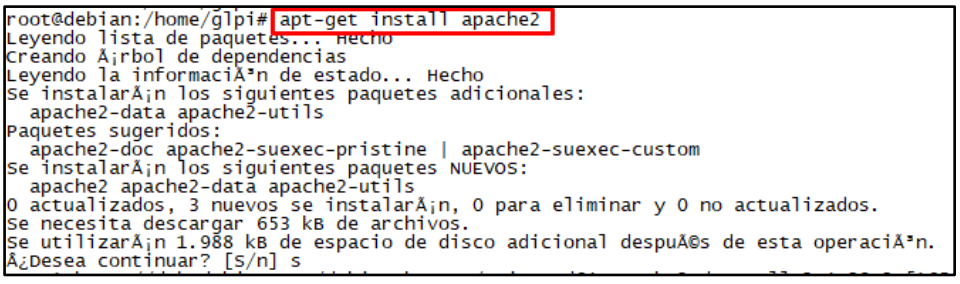
Por defecto la comunicación de SSH se realiza por el puerto 22, en el caso de que se quiera cambiar dicha configuración se lo realizará dentro del archivo de SSH, ejecutando el comando ***nano /etc/ssh/sshd_config*** y se abrirá el archivo de configuración donde se permitirá cambiar el puerto mediante el cual se está realizando esta comunicación.



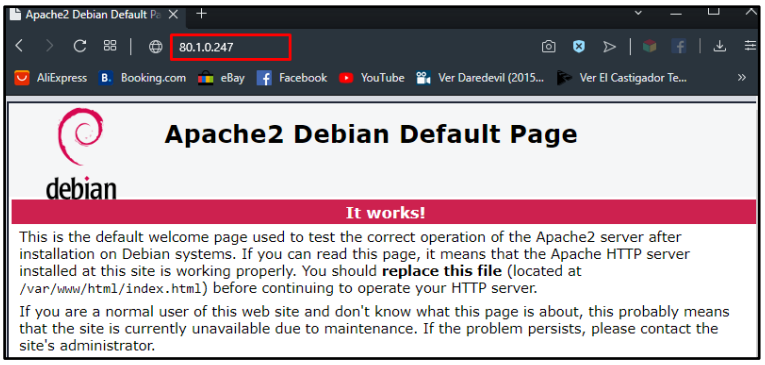
C. Instalación del servidor WEB

Para instalar el servidor web Apache y habilitar el servicio de arranque se sigue el siguiente proceso usando los comandos mencionados a continuación:

apt-get install apache2



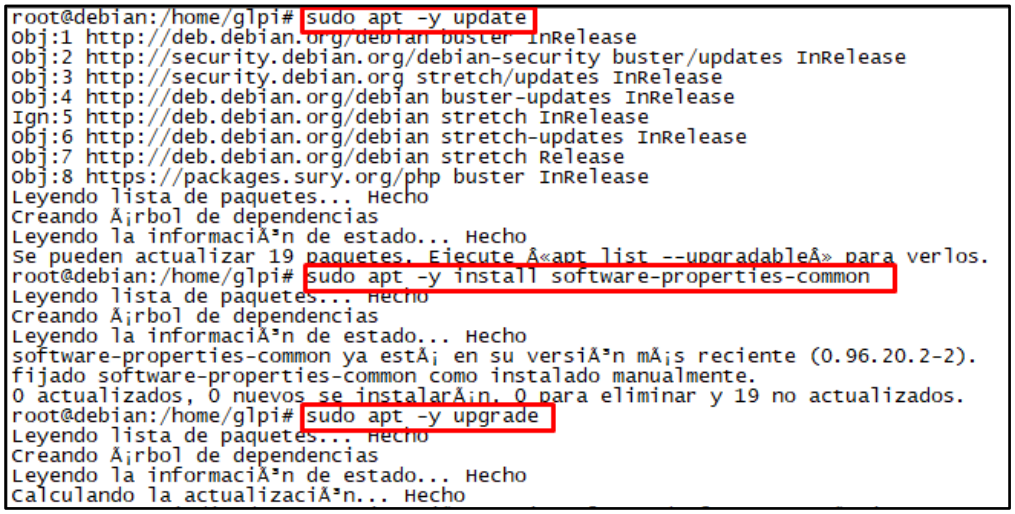
Se procede a abrir un navegador desde un computador remoto dentro de la misma red, con la dirección IP del servidor, y debe acceder a la página web predeterminada de apache que se acaba de instalar.



Para que el servicio web se ejecute automáticamente al encender el servidor se lo habilita mediante el comando: ***systemctl enable apache2.service.***

D. Instalación de la base de datos

Como recomendación se debe actualizar el sistema y actualizar los paquetes instalados con los comandos que se muestran en la imagen:



Ahora se procede a importas las claves gpg de MariaDB, mismas que contienen las firmas para los paquetes Debian MariaDB, y posteriormente se agrega un repositorio adicional, con los siguientes comandos:

sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 0xF1656F24C74CD1D8

sudo add-apt-repository 'deb [arch=amd64] http://mariadb.mirror.liquidtelecom.com/repo/10.4/debian buster main'

```
root@debian:/home/glpi# sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 0xF1656F24C
74CD1D8
Executing: /tmp/apt-key-gpghome.5i9wd/bkXq/gpg.1.sh --recv-keys --keyserver keyserver.ubuntu.com
0xF1656F24C74CD1D8
gpg: key F1656F24C74CD1D8: 6 firmas no comprobadas por falta de claves
gpg: clave F1656F24C74CD1D8: "MariaDB Signing Key <signing-key@mariadb.org>" sin cambios
gpg: Cantidad total procesada: 1
gpg:              sin cambios: 1
root@debian:/home/glpi# sudo add-apt-repository 'deb [arch=amd64] http://mariadb.mirror.liquidte
ecom.com/repo/10.4/debian buster main'
root@debian:/home/glpi#
```

Una vez agregado un repositorio es necesario actualizar el sistema para que este empiece a funcionar, y posteriormente se instala MariaDB, con los siguientes comandos:

sudo apt update
sudo apt install mariadb-server mariadb-client

```
root@debian:/home/glpi# sudo apt install mariadb-server mariadb-client
Leyendo lista de paquetes... Hecho
Creando Ã¡rbol de dependencias
Leyendo la informaciÃ³n de estado... Hecho
Los paquetes indicados a continuaciÃ³n se instalaron de forma automÃ¡tica y ya no son necesarios.
  libconfig-inifiles-perl libncurses5 libtinfo5
Utilice Â«sudo apt autoremoveÂ» para eliminarlos.
Se instalarÃ¡n los siguientes paquetes adicionales:
```

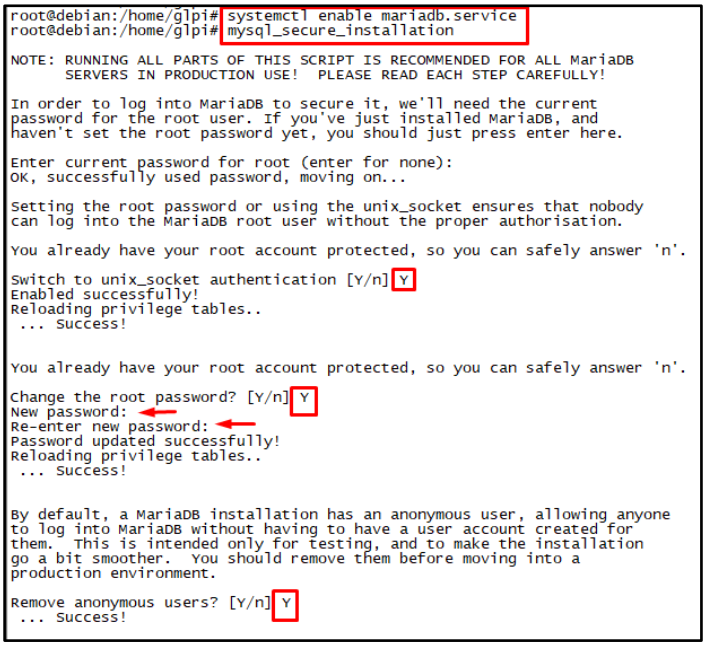
Se hace una prueba del estado de funcionamiento de la base de datos con el comando: ***systemctl status mariadb***, con el cual aparte de ver el estado se puede apreciar además la versión instalada, como se muestra en la **¡Error! No se encuentra el origen de la referencia.** ontinuación, donde se puede apreciar que el proceso MariaDB está activo y funcionando con una versión 10.4.6.

```
root@debian:/home/glpi# systemctl status mariadb
â—  mariadb.service - MariaDB 10.4.6 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled
  Drop-In: /etc/systemd/system/mariadb.service.d
           â""â"€migrated-from-my.cnf-settings.conf
   Active: active (running) since Wed
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
 Main PID: 3918 (mysqld)
```

Posteriormente se habilita el arranque automático del servicio MariaDB con el comando ***systemctl enable mariadb.service.***

Para mejorar la seguridad de la instalación de MariaDB se ejecuta el comando: ***mysql_secure_installation***. Este comando ejecutado pedirá que se establezca una contraseña

de usuario root a la maquina local y elimina la base de datos de prueba, además realiza algunas preguntas de seguridad como el acceso remoto a la base de daros mediante usuario root o usuarios anónimos, y al final permitirá reiniciar la tabla de privilegios de los usuarios, por recomendación se establecerá todos estos valores en Y para denotar que es un valor afirmativo a todas las preguntas que se realizan, como se muestra en la siguiente figura.



Al final el script recargará las tablas de privilegios asegurando que todos los cambios surtan efecto inmediatamente.

E. Instalación de PHP

Una vez concluida esta parte de configuración inicial, es necesario cargar nuevos paquetes necesarios para actualizar los repositorios y las firmas de paquetes para la instalación de PHP 7.3, para lo cual se ejecuta los comandos:

sudo apt install ca-certificados apt-transport-https
wget -q https://packages.sury.org/php/apt.gpg -O- | sudo apt-key add -
sudo echo "deb https://packages.sury.org/php/ buster main" | tee /etc/apt/sources.list.d/php.list

```
root@debian:/home/glpi# sudo apt install ca-certificados apt-transport-https
Leyendo lista de paquetes... Hecho
root@debian:/home/glpi# wget -q https://packages.sury.org/php/apt.gpg -O- | sudo apt-key add -
OK
root@debian:/home/glpi#
root@debian:/home/glpi# sudo echo "deb https://packages.sury.org/php/ buster main" | tee /etc/apt
/sources.list.d/php.list
deb https://packages.sury.org/php/ buster main
root@debian:/home/glpi#
```

Para la instalación de PHP 7.3 se actualiza los repositorios con el comando ***apt update***, una vez completada la actualización se ejecuta el comando ***apt install php7.3,*** el cual descargara e instalara la versión 7.3 de PHP.

```
root@debian:/home/glpi# apt update
Obj:1 http://security.debian.org/debian-security buster/updates InRelea
Obj:2 http://security.debian.org stretch/updates InRelease
Obj:3 http://deb.debian.org/debian buster InRelease
Obj:4 http://deb.debian.org/debian buster-updates InRelease
Ign:5 http://deb.debian.org/debian stretch InRelease
root@debian:/home/glpi# apt install php7.3
Leyendo lista de paquetes... Hecho
Creando Ã¡rbol de dependencias
Leyendo la informaciÃ³n de estado... Hecho
```

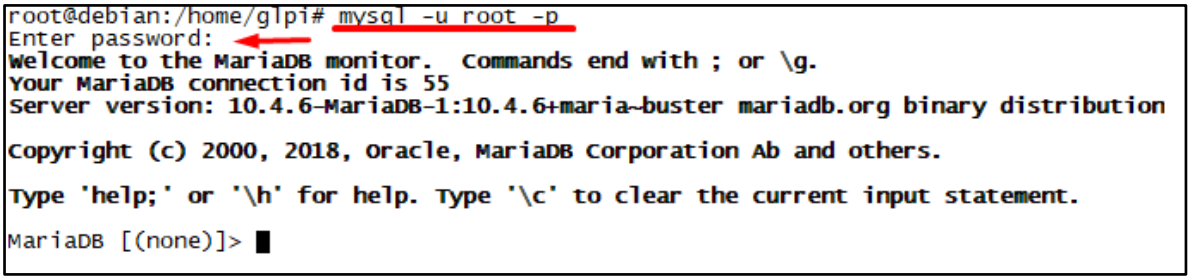
Adicional se debe instalar también algunos complementos de php para que GLPI funcione correctamente, para lo se debe ejecutar el comando siguiente:

sudo apt install php7.3-curl php7.3-zIP php7.3-gd php7.3-intl php-pear php-imagick php7.3-imap php-memcache php7.3-pspell php7.3-recode php7.3-tidy php7.3-xmlrpc php7.3-xsl php7.3-mbstring php-gettext php7.3-ldap php-cas php-apcu libapache2-mod-php7.3 php7.3-mysql

```
root@debian:/home/glpi#
root@debian:/home/glpi# sudo apt install php7.3-curl php7.3-zip php7.3-gd php7.3-intl php-pear ph
p-imagick php7.3-imap php-memcache php7.3-pspell php7.3-recode php7.3-tidy php7.3-xmlrpc php7.3-x
sl php7.3-mbstring php-gettext php7.3-ldap php-cas php-apcu libapache2-mod-php7.3 php7.3-mysql
Leyendo lista de paquetes... Hecho
Creando Ã¡rbol de dependencias
Leyendo la informaciÃ³n de estado... Hecho
php-apcu ya estÃ¡ en su versiÃ³n mÃ¡s reciente (5.1.17+4.0.11-1+0~20190217111312.9+stretch~1.gbp1
92528).
Se instalarÃ¡n los siguientes paquetes adicionales:
```

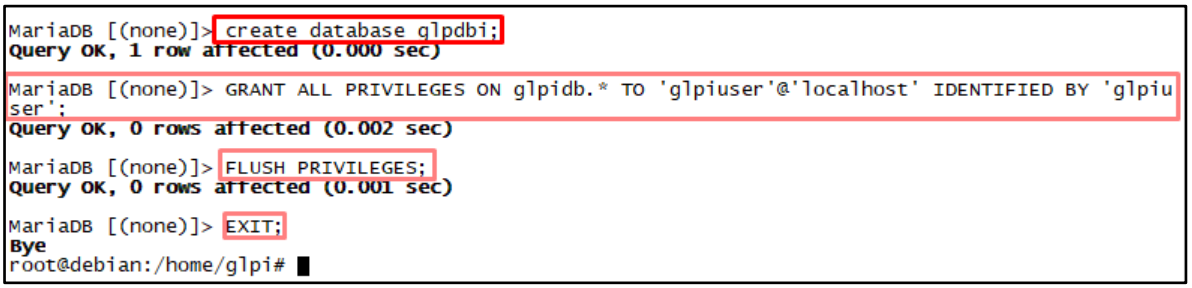
F. Configuración de base de datos para glpi

Como siguiente paso se tiene la creación de la base de datos que GLPI utilizará para su almacenamiento de información, para lo cual primero debemos acceder a la base de datos, para esto ejecutaremos el comando ***mysql -u root -p*** mismo que luego de ejecutarse pedirá la contraseña de administrador que se configuro previamente, además muestra la versión de MariaDB instalada.



Posteriormente al haber accedido a la base de datos ejecutaremos los siguientes comandos que permiten crear una base de datos de nombre **glpdbi**, además se crea un usuario administrador como usuario local de la base de datos, y se le asignan todos los privilegios como se muestra en la imagen inferior. Para esto se ejecutan los siguientes comandos:

create database glpdbi;
GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost' IDENTIFIED BY 'glpiuser';
FLUSH PRIVILEGES;
EXIT;



G. Instalación y configuración de GLPI

Previa su instalación se debe descargar el paquete de instalación mismo que se lo realizara utilizando el siguiente comando:

wget -c https://github.com/glpi-project/glpi/releases/download/9.4.3/glpi-9.4.3.tgz

Es necesario mover el fichero comprimido a la carpeta habitual de los proyectos web, y luego se procede a acceder al directorio para descomprimir dicho archivo. Para que la ejecución de GLPI no tenga inconvenientes se le brindan permisos 755 de chmod, que son los permisos de directorio, el cual permite al propietario del fichero leer, escribir y ejecutar el archivo y a los demás usuarios únicamente leer y ejecutar el archivo, esto para la carpeta de acceso web. Adicionalmente con el comando chown permite dar la propiedad de acceso web a la carpeta que contiene el servicio web, con los siguientes comandos:

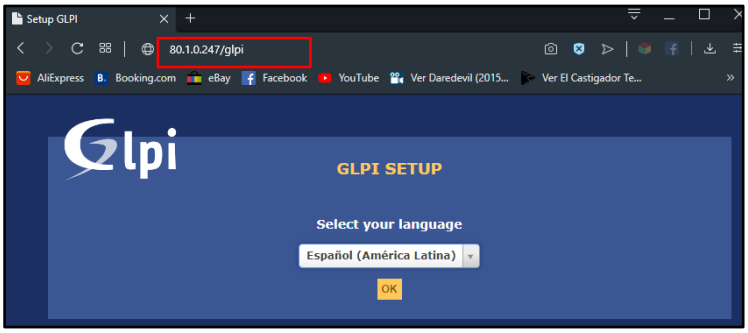
mv glpi-9.4.3.tgz /var/www/html/
cd /var/www/html/
tar -xvf glpi-9.4.3.tgz
chmod 755 -R /var/www/html/
chown www-data:www-data -R /var/www/html/

```
root@debian:/home/glpi# wget -c https://github.com/glpi-project/glpi/releases/download/9.4.3/glpi-9.4.3.tgz
root@debian:/home/glpi# cd /var/www/html/
root@debian:/var/www/html# tar -xvf glpi-9.4.3.tgz
root@debian:/var/www/html# chmod 755 -R /var/www/html/
root@debian:/var/www/html# chown www-data:www-data -R /var/www/html/
```

Como siguiente paso se tiene el reinicio del servidor web para que los cambios realizados surtan efecto, esto se lo realiza utilizando el comando: ***systemctl restart apache2,*** así también se debe reiniciar el servicio mysql con el comando: ***sudo /etc/init.d/mysql restart.***

Para continuar con la configuración, se utiliza un navegador web, en el cual accederemos a glpi mediante la dirección IP 80.1.0.247/glpi (IP con la que se configuro en el

servidor GLPI). Y seleccionar el idioma de preferencia con el que se desea terminar la configuración.



Se debe aceptar los términos y condiciones de uso de GLPI, para continuar con la instalación.

En la siguiente opción que se muestra, hay dos opciones de configurar GLPI, la primera y la que se escogerá es de una instalación completamente desde cero, y la segunda opción es para actualizar una instalación de GLPI existente.

Se procede a realizar una verificación de los requisitos de compatibilidad con GLPI y los elementos necesarios para su instalación, en caso de no contar con alguno no se podrá continuar con la instalación

Paso 0

Verificación de la compatibilidad de su entorno con la ejecución de GLPI

Prueba realizada	Resultados
Prueba del intérprete PHP	✔
Prueba de Sesiones	✔
Prueba de utilización de Session.use_trans_sid	✔
mysqli extension test	✔
ctype extension test	✔
fileinfo extension test	✔
json extension test	✔
mbstring extension test	✔
zlib extension test	✔
curl extension test	✔
gd extension test	✔
simplexml extension test	✔
xml extension test	✔
ldap extension test	✔
imap extension test	✔
Zend OPcache extension test	✔
APCu extension test	✔
xmlrpc extension test	✔
Comprobar la memoria asignada	✔
Prueba de escritura del archivo de configuración	✔
Prueba de escritura de archivos de documentos	✔
Pruebas de escritura de archivos dump	✔
Prueba de escritura de archivos de sesiones	✔
Prueba de escritura para acciones automáticas sobre archivos	✔
Prueba de escritura de los archivos gráficos	✔
Prueba de escritura para archivos	✔
Prueba de escritura sobre documentos de plugins	✔
Prueba de escritura sobre archivos temporales	✔
Prueba de escritura de los archivos de caché	✔
Prueba de escritura sobre archivos rss	✔
Prueba de escritura sobre archivos de carga	✔
Revise los permisos para los archivos de imagen	✔
Prueba de escritura de los archivos de log	✔
Acceso web al directorio de archivos está protegido	ⓘ Acceso web al directorio de archivos no debe ser permitido. Verificar el archivo .htaccess y la configuración del servidor web
El modo SELinux es Permissive	✔
La configuración booleana de SELinux para httpd_can_network_connect --> on	✔
La configuración booleana de SELinux para httpd_can_network_connect_db --> on	✔
La configuración booleana de SELinux para httpd_can_sendmail --> on	✔

Desea continuar?

Continuar Reintentar

Posteriormente la interfaz de GLPI pide que se seleccione una base de datos, para lo cual se seleccionara la opción GLPI, ya que esta es la base de datos que se creó anteriormente

El siguiente paso es configurar la conexión de la base de datos con GLPI, llenaremos esta información con los datos del usuario que se creó anteriormente dentro de la base de datos.

Si la conexión se realizó con éxito, el sistema muestra un mensaje demostrando que la base de datos ha sido inicializada, caso contrario no se realizara la conexión con la base de datos. Una vez que la conexión fue exitosa no queda más que finalizar la instalación del servidor y utilizar GLPI.

Para el ingreso por primera vez a GLPI, se tiene un usuario por defecto “glpi” con una contraseña “glpi”, misma que por seguridad debe ser cambiada luego del primer acceso.

Una vez que se ha concluido con la instalación de manera exitosa, es recomendable como medida de seguridad, eliminar el instalador de GLPI, para lo cual se ejecutaran lo siguientes comandos:

cd /var/www/html/glpi/install
rm install.php
systemctl restart apache2

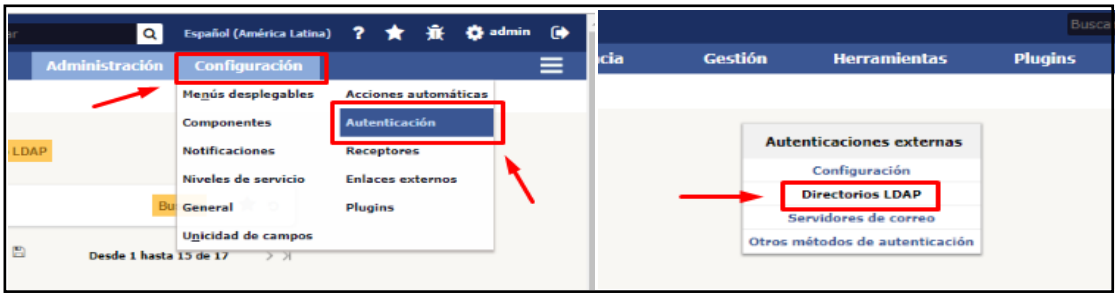
ANEXO 5: Enlace de GLPI con un directorio activo.

GLPI es una herramienta que permite importar usuarios desde una base LDAP en este caso el Active Directory (AD) . Se debe crear una conexión la cual permitirá enlazar GLPI con Active Directory, para ello se debe seguir de forma ordenada y secuencial el proceso que se detalla a continuación.

A. Configuración LDAP en GLPI

Ingresar como super administrador a GLPI, para ello se selecciona Super Admin en la pestaña mostrada en la siguiente imagen.

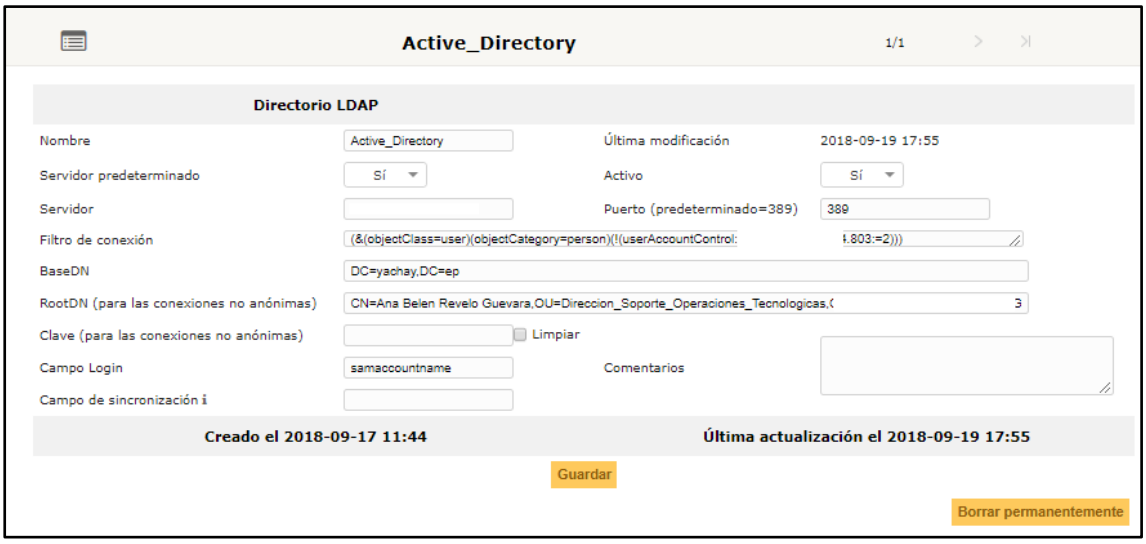
Una vez ingresado a GLPI como super administrador, se debe dirigir a configuración, seleccionar autenticación, y en la pantalla siguiente seleccionar directorios LDAP.



En la ventana seleccionar el icono “+”, que aparece en la parte superior, luego del cual se mostrará una pantalla, en la que se debe ingresar los campos requeridos para establecer la conexión con el Directorio LDAP, mostrados en la siguiente tabla:

Ítem	Informacion que debe incluir
Nombre	Nombre descriptivo de la conexión
Por defecto	Permite seleccionar el directorio activo actual como medio de acceso principal.
Activo	Permite habilitar o deshabilitar la conceccion con el directorio activo.
Servidor	Incluir la direccion IP del servidor ldap en la siguiente estructura: ldap://ip_servidor
Puerto	Ingrese el puerto de conexión con el servidor LDAP, por defecto el puerto 389
Filtro	Se incluiye un filtro para la obtenciond e credenciales dependiendo de la empresa y el servidor LDAP configurado, en este caso: (&(objectClass=user)(objectCategory=person)(!(userAccountControl:803:=2)))
Base DN	Ingrese el dominio de la empresa.
RootDN	Es la ubicación donde se encuentran almacenados los usuarios en el servidor LDAP, donde ademas se incluye un usuario CN=USUARIO, mismo que permite enlazar el AD con GLPI.
Clave	La contrasela del usuario CN para la conexión con el AD

En el root DN se coloca el dominio de un usuario válido en el directorio activo.

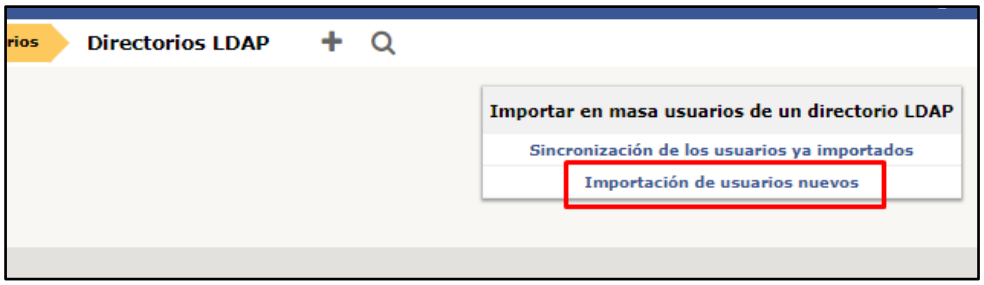


Al terminar la configuración se debe hacer clic en el botón guardar, y para hacer una prueba de funcionamiento de la conectividad con el AD, en la parte izquierda de la ventana se muestra un botón denominado “Probar”, hacer clic en él, y luego verificar si la conexión fue configurada de manera correcta, de no ser el caso mostrara un mensaje de error, verifique las

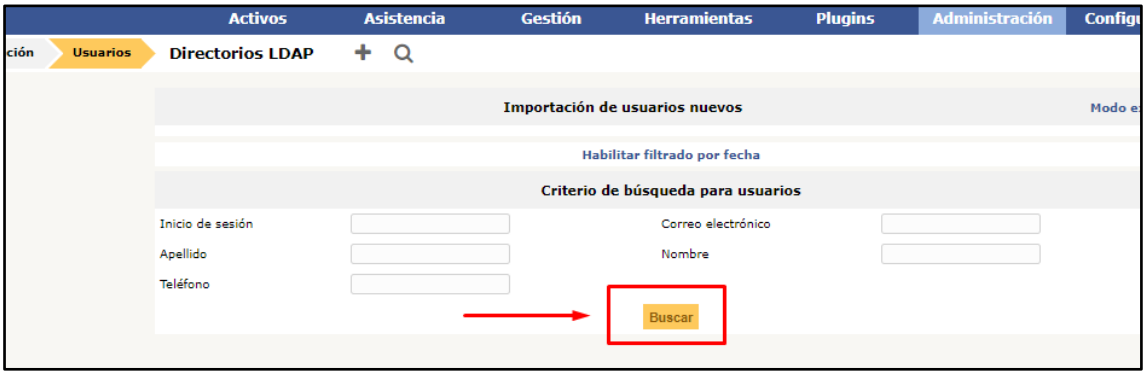
configuraciones del directorio nuevamente y realice otra prueba en el caso de que la prueba haya resultado correcta se mostrará un mensaje de prueba exitosa.

B. Importación de usuarios desde el directorio activo

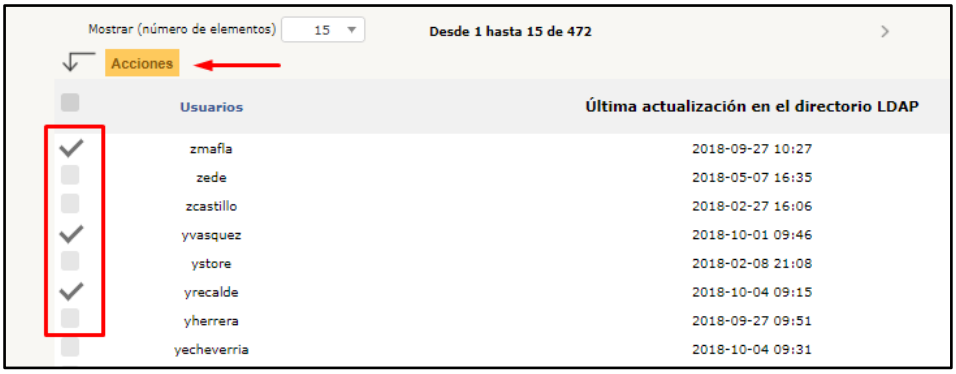
Para importar los usuarios de un Active Directory (AD) configurado se dirige a la siguiente ubicación haciendo clic en los botones y pestañas con la siguiente ruta: Administración > Usuarios > Enlace de directorio LDAP > Importación de usuarios nuevos



En la pestaña que se muestra no llenar ningún campo y hacer clic en el botón buscar



Cuando la búsqueda finalice se habrá llenado una lista de usuarios, mismos que están registrados en el AD, de esta lista seleccione los usuarios que quiere incluir para el acceso al servidor GLPI.



Al terminar con la selección haga clic en el botón Acciones, y seleccione la acción "Importar" y hacer clic en aceptar.

Al terminar con la importación de los usuarios, estos pueden verse reflejados en la ubicación, Administración > Usuarios.

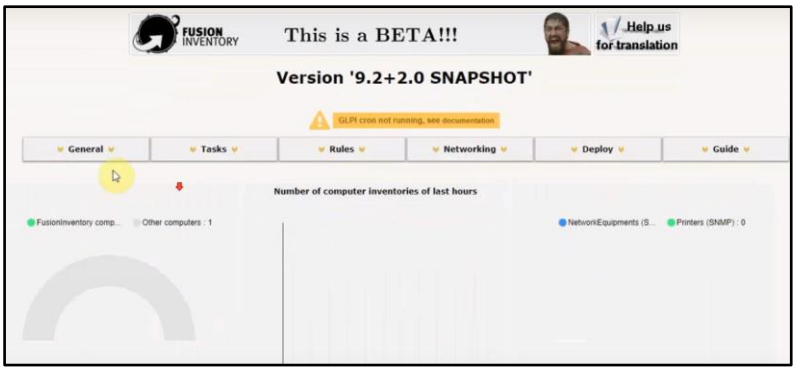
ANEXO 6: Instalación y configuración de FusionInventory

A. Instalación de plugin FusionInventory en GLPI

El plugin FusionInventory en GLPI permite la obtención de información de los dispositivos conectados en la red mediante una comunidad SNMP. Para la instalación de este plugin es necesario dirigirse a la página oficial y descargar la versión de FusionInventory compatible con la versión instalada de GLPI. Desde la pagina https://github.com/fusioninventory/fusioninventory-for-glpi/releases.

Una vez descargado el archivo se debe descomprimir en la ubicación: /var/www/html/glpi/plugins, dentro de la máquina virtual de GLPI. Una vez realizado este proceso se debe abrir en un navegador el agente de GLPI con un usuario con privilegios de super administrador, con el cual se debe ingresar a la pestaña configuración en la opción plugins, donde se habrá actualizado automáticamente el plugin, actualmente está sin usar, por lo que se debe hacer clic en el botón activar,

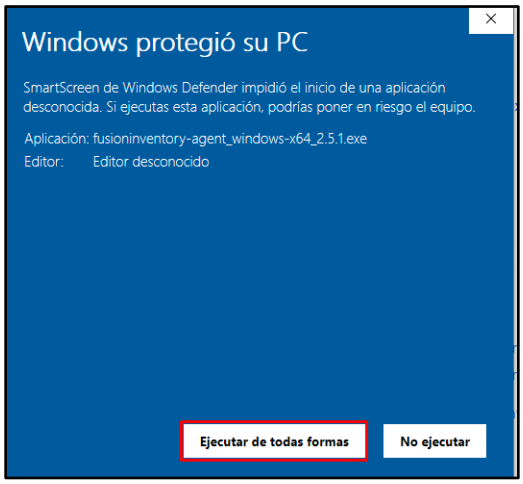
Si todo el proceso se ejecutó correctamente al activar aparecerá un mensaje que indicara que la activación fue satisfactoria. para abrir el plugin instalado se debe abrir la pestaña Administración y el final aparece un nuevo sub menú de nombre FusionInventory, hacer clic en él y mostrara información como la que se muestra a continuación.



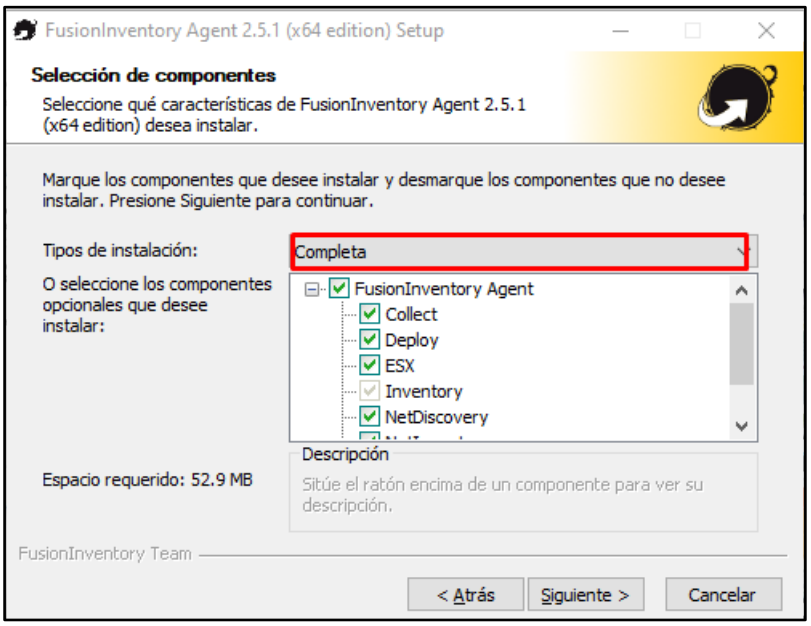
B. Instalación y configuración de agente de FusionInventory en Windows

El computador, máquina virtual o equipo donde se instalará el agente debe estar habilitado SNMP para la recolección de información, en este caso se ha instalado el agente en un computador con sistema operativo Windows 10. El procedimiento para la instalación es el siguiente:

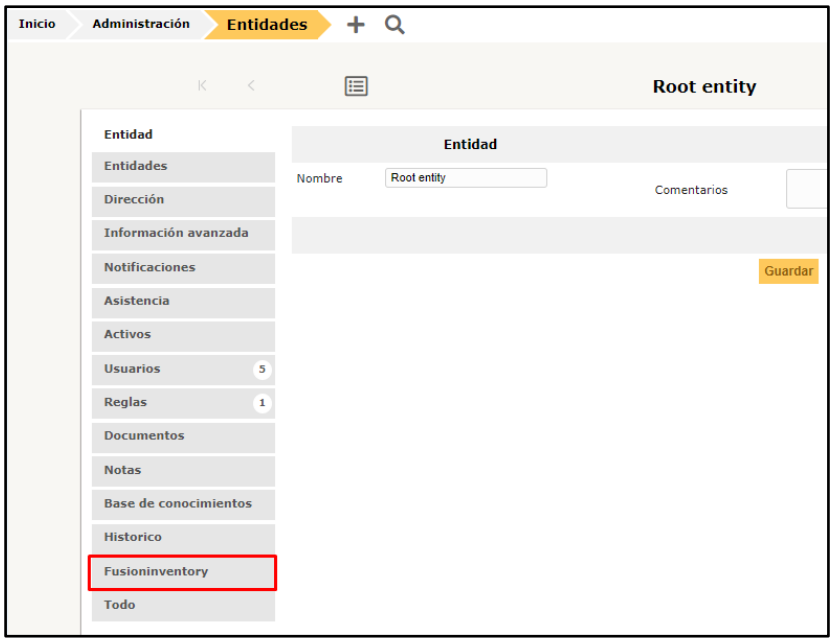
Descargar el instalador del agente desde la página oficial de FusionInventory http://fusioninventory.org/2019/12/16/fusioninventory-agent-2.5.2.html , y ejecutarlo, al hacer doble clic sobre este instalador pedirá permisos, los cuales hay que conceder para proceder con la instalación.



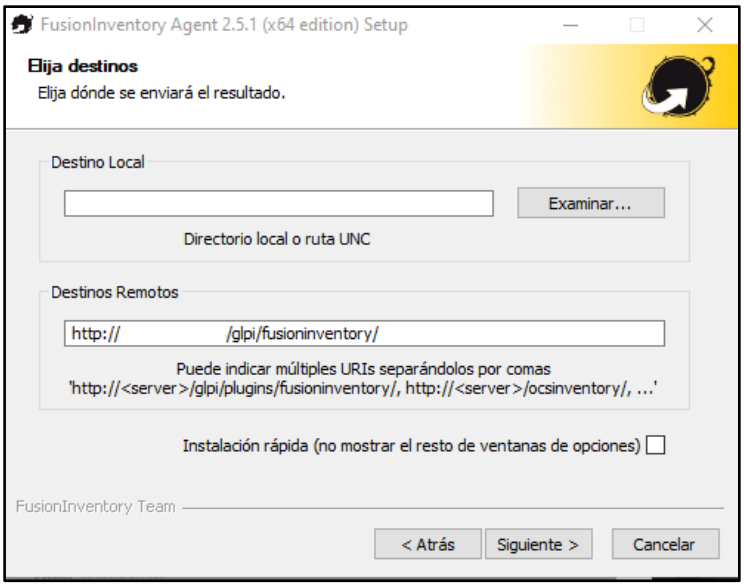
Posterior a dar los permisos, el programa de instalación mostrara una secuencia de pantallas en las cuales se debe configurar información referente a la red y al servidor al que se le permitirá el envío de información, para la instalación se seleccionara una instalación completa como se muestra en la siguiente imagen.



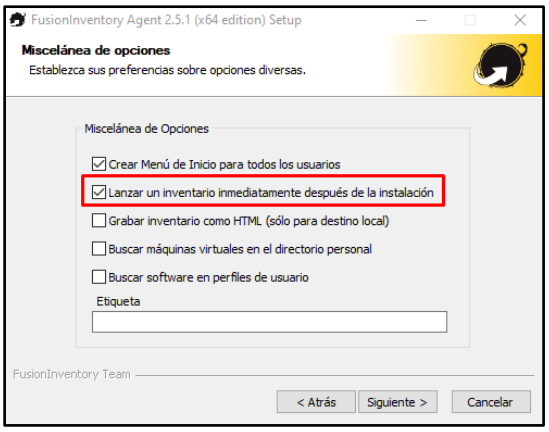
Para la siguiente ventana se necesita información desde el servidor GLPI, para lo cual accedemos a la página web del servidor GLPI instalado, haciendo clic en los botones y pestañas seguimos el siguiente orden: Administracion > Entidades > Root entity, en la parte izquierda se muestra un menú denominado “FusionInventory”, hacer clic ahí.



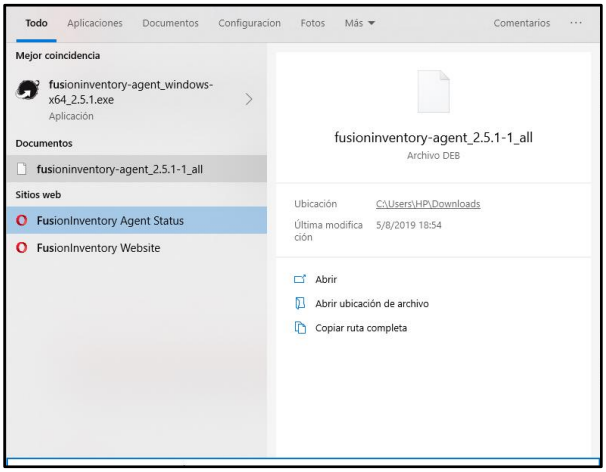
En la pantalla mostrara información Service URL, el cual se debe copiar de igual manera en la ventana de instalación como se muestra en la siguiente imagen.



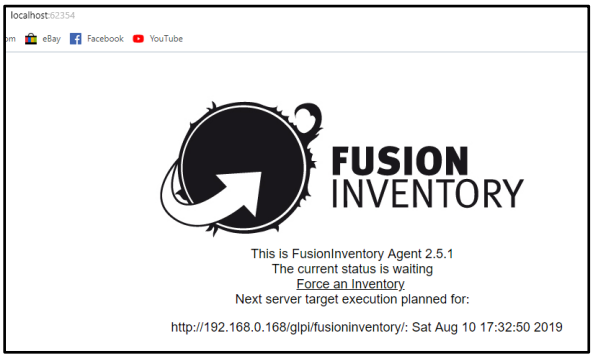
Se debe verificar que la instalar el inventario se ejecute de manera inmediata luego de la instalación del agente como se muestra en la imagen inferior, en todos los procesos no mencionados si no está seguro de las configuraciones hacer clic en siguiente con los parámetros establecidos por defecto.



Tras la instalación se puede ejecutar una búsqueda en el panel de Windows con la expresión FusionInventory, el cual brinda el resultado del estado del agente, como se muestra a continuación.



El cual brindara una página similar a la siguiente, donde el usuario o administrador puede forzar un inicio de inventario.

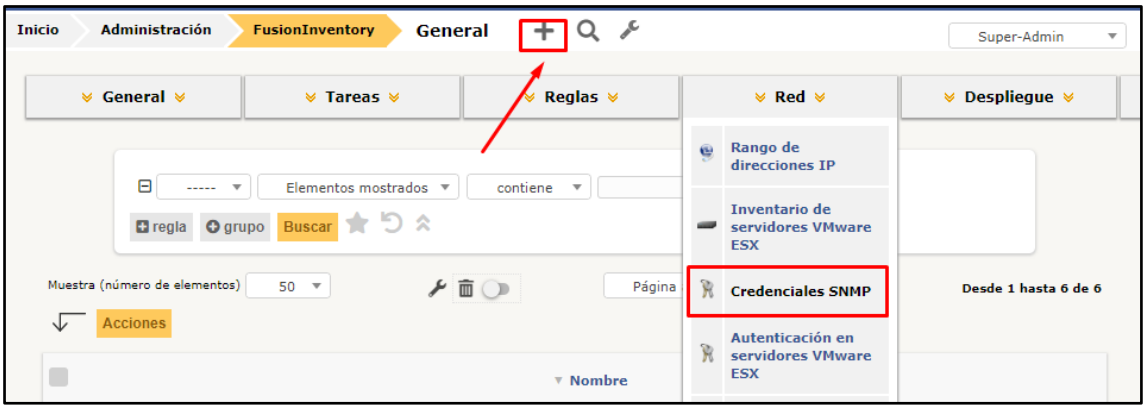


ANEXO 7: Inventario automático de equipamiento de red con GLPI

GLPI permite la recolección de información automática de los dispositivos de uno o varios segmentos de red mediante el uso de una red SNMP, para lo cual GLPI ejecuta una o varias tareas cada una con su respectivo trabajo en un horario establecido, para lo cual es necesario seguir el proceso que se menciona a continuación.

A. Configuración de credenciales SNMP en GLPI.

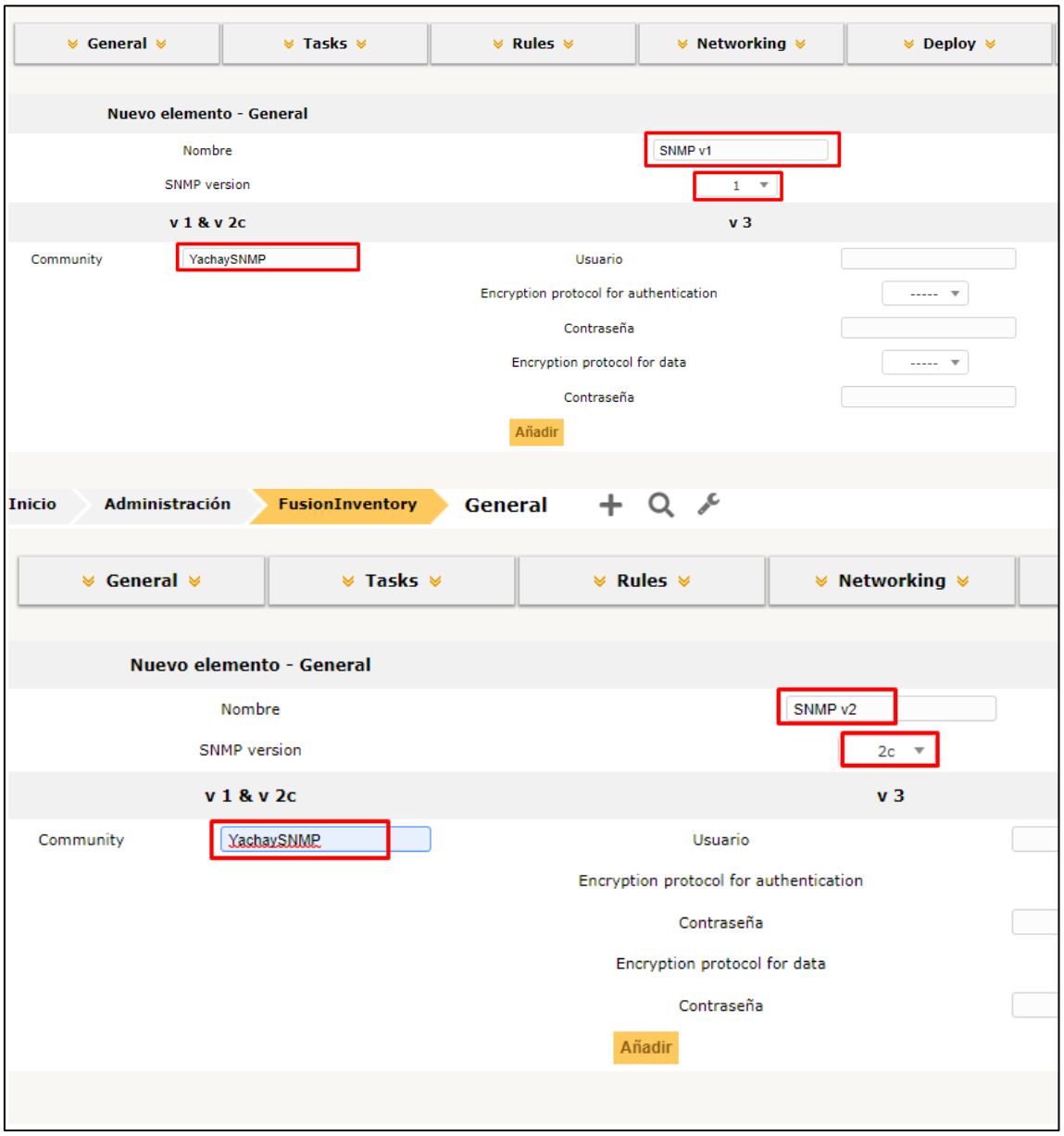
Sedebe ingresar a GLPI con un usuario con perfil de Super-Administrador, para poder acceder a esta configuración. Paa la configuracion de las credenciales SNMP se debe acceder haciendo clic en los botones y pestañas con la siguietne ruta: Administracion > FusionInventory > Red > Credenciales SNMP , y hacer clic en el "+" ubicado al lado de la ruta para agregar una nueva credencial.



Para cada comunidad SNMP se debe agregar dos credenciales en GLPI, la primera para SNMP version 1 y la segunda para SNMP version 2, siguiendo el mismo proceso.

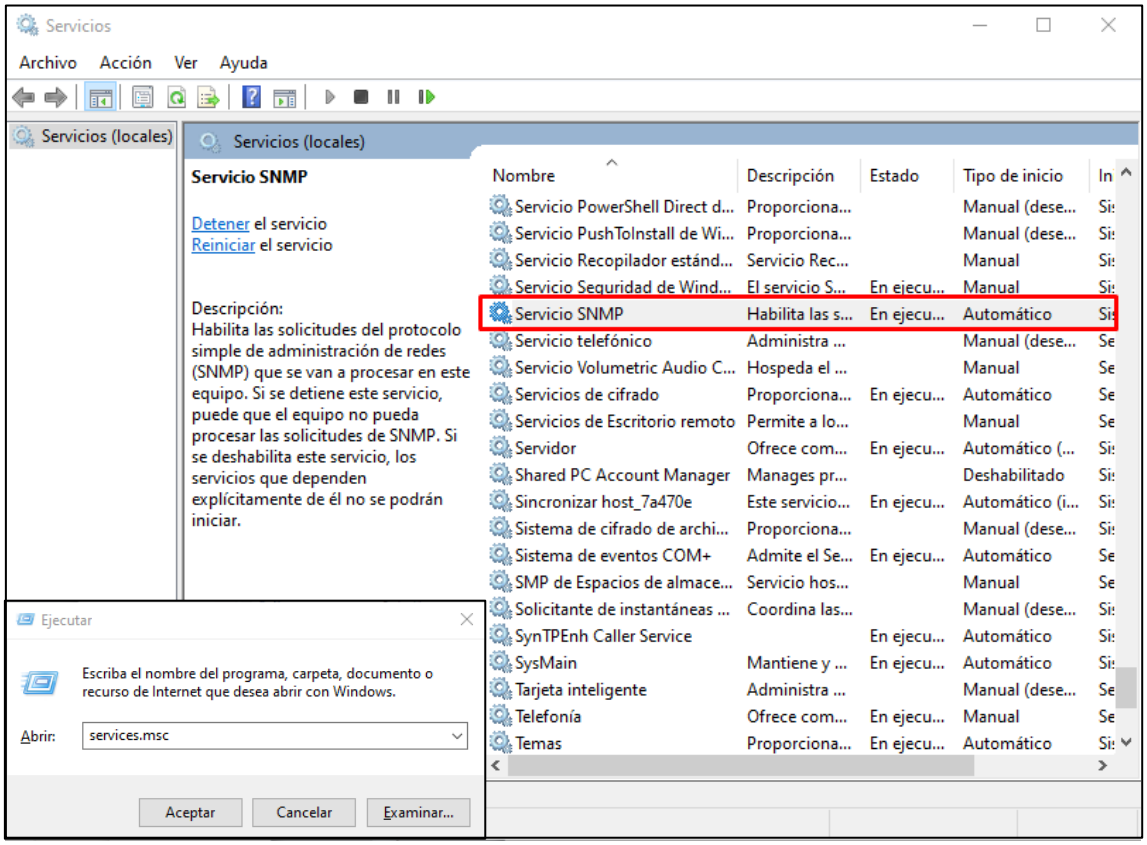
en la pantalla mostrada luego de presionar el boton "+" para agregar una nueva credencial, se debe ingresar un nombre identificativo dentro de GLPI, se debe seleccionar la

version (1, 2c o 3) seguns ea el caso, y la parte principal la comunidad que en este ejemplo es “YachaySNMP”.

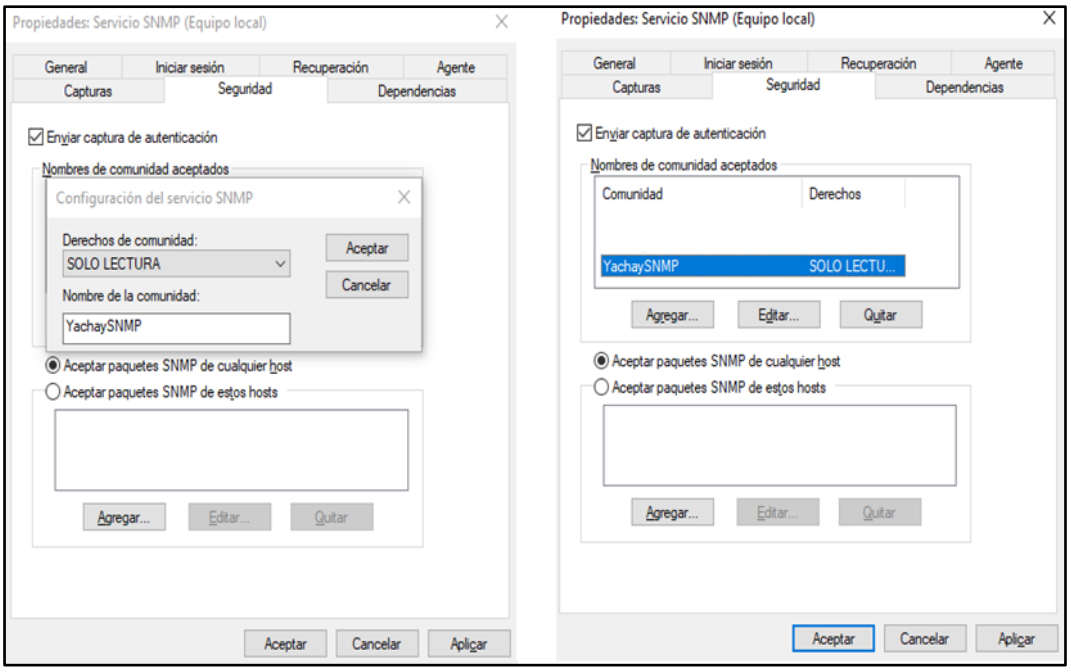


B. Configuración de comunidad SNMP en el agente

Para la configuración de SNMP en el agente instalado en Windows 10, se debe abrir los servicios de Windows ejecutando el comando Ctrl+R y en la ventana ejecutar ingresar services.msc, y en la ventana seleccionar el “Servicio SNMP”

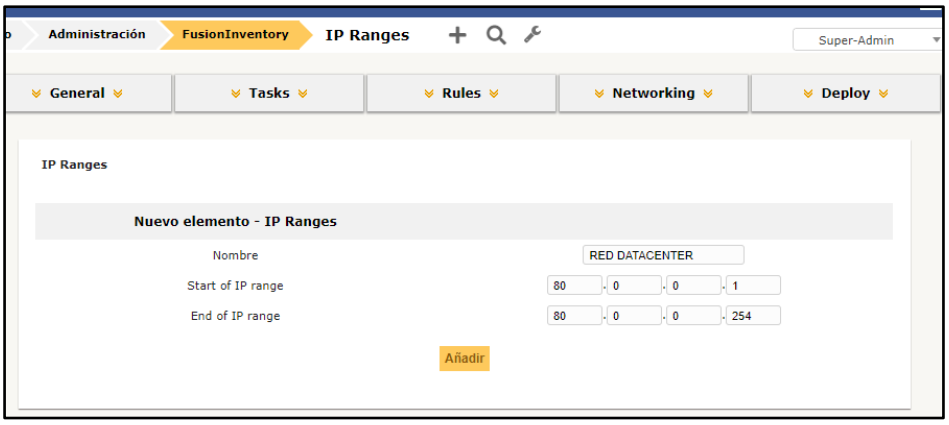


A continuacion se abre una ventana de configuracion en la cual se debe seleccionar la pestaña seguridad, habilitar el check para enviar captura de autenticacion, y hacer clic en el boton agregar e ingresar la comunidad SNMP configurada en los equipos de red, hacer clic en aplicar y aceptar para guardr los cambios.



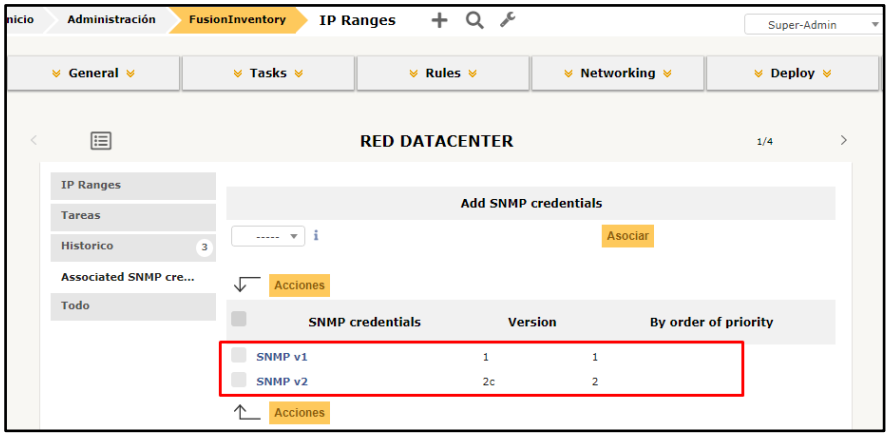
C. Configuración de rangos de IP.

Para gestionar un rango de IP se debe acceder a la siguiente ruta, haciendo clic en las pestañas y botones en el siguiente orden: Administracion > FusionInventory > Red > Rangos de IP, hacer clic en el icono “+” para agregar un rango de IP nuevo, una vez dentro de esta ruta en pantalla debemos ingresar un nombre identificativo dentro de GLPI de esta red, y la IP de inicio y la IP final del rango establecido y hacer clic en el boton añadir.



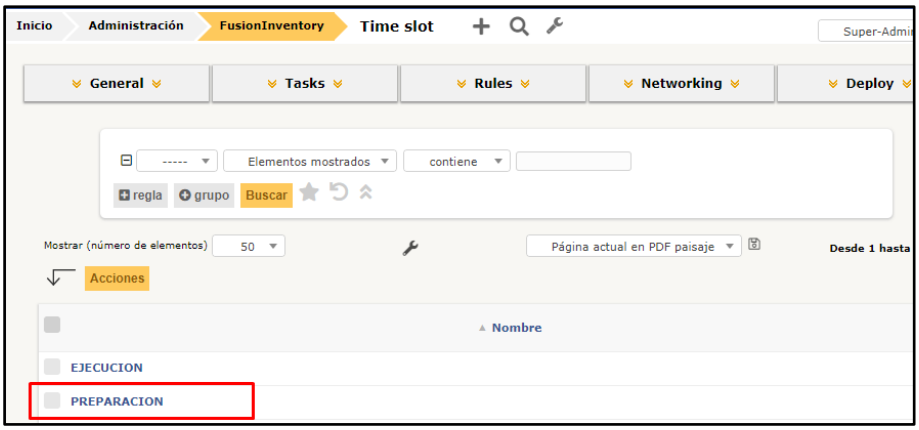
D. Asociar las credenciales SNMP al rango de IP.

Una vez creado el rango de IP se debe acceder a la ruta: Administracion > FusionInventory > Red > Rangos de IP, donde se listaran las rdes IP creadas, se debe seleccionar la red a la que se quiere asociar las credenciales SNMP, y luego mostrara una pantalla done, en la parte izquierda se debe seleccionar la opcion “Asociar credenciales SNMP”, selecccionar las credenciales SNMP creadas y hacer clic en el boton “Asociar”.

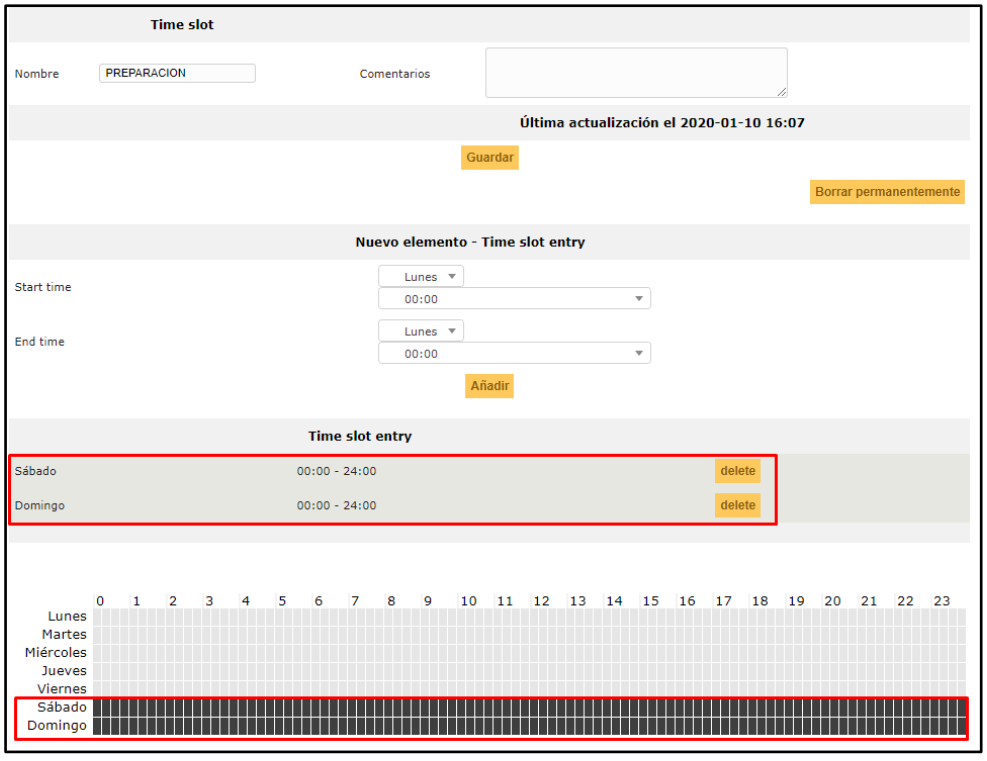


E. Configuración de intervalos de tiempo

Para la creación y ejecución de tareas automáticas se deben crear intervalos de tiempo para su ejecución. Para lo cual se debe ingresar en GLPI en la siguiente ruta: Administracion > FusionInventory > Tareas > Intervalo de tiempo y hacer clic en el “+” ubicado en la parte superior para agregar un intervalo nuevo, en el cual luego de agregar un nombre y un comentario se hace clic en añadir. Se vuelve a intervalo de tiempo para listar los intervalos creados.



Al seleccionar el intervalo requerido (para el ejemplo se selecciona el tiempo de nombre "PREPARACION" mostrará en pantalla una ventada donde se permite la selección de horarios en varios dias para la ejecucion de las tareas, se recomienda seleccionar tiempos en los que la red se encuentre menos congestionada, en este ejemplo se ha seleccionado el intervalo de las 00:00 horas del sábado hasta las 24 horas del domingo.



Puede seguir agregando intervalos de tiempos en diferentes días si se desea, además se deben crear dos tiempos uno para preparación y uno para ejecución, donde, el tiempo de

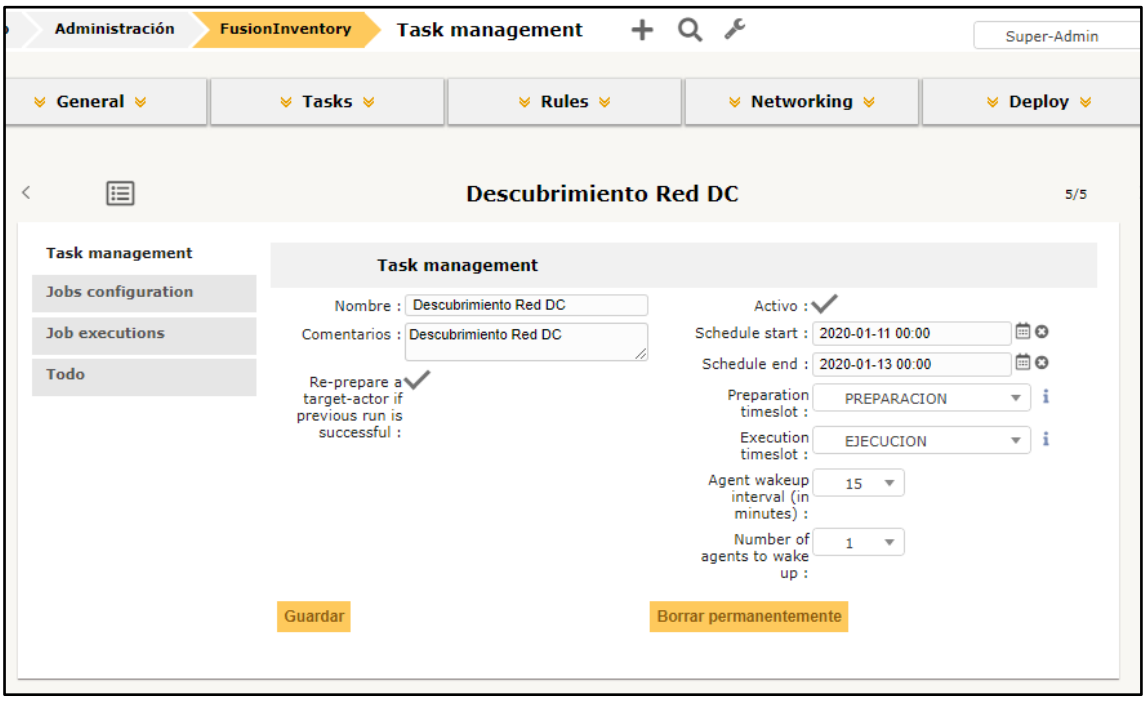
ejecución debe tener un tiempo 15 minutos mayor que el de preparación, un tiempo definido gracias a las pruebas que se han realizado.

F. Creación de tareas

De igual manera que en los procesos anteriores se debe hacer clic en las pestañas y botones con la siguiente ruta: Administración > FusionInventory > Tareas > Gestión de tareas y presionar en el botón "+" para añadir una nueva tarea, donde pedirá al usuario que ingrese un nombre identificativo para la tarea y un comentario si se necesita y se presiona en el botón añadir.

Al hacer clic en el botón añadir se muestra una ventada donde se debe incluir información más específica dependiendo de las necesidades. En este caso se muestra un ejemplo de ejecución del descubrimiento de red, el cual debe permanecer en un estado activo, se incluyen la fecha y hora de inicio de escaneo y la fecha y hora de finalización de la ejecución de la tarea, así también se selecciona el tiempo de preparación y el tiempo de ejecución que se configuró anteriormente, seleccionar el tiempo en el cual la tarea se vuelve a ejecutar un tiempo

prudencial es de 15 o 30 minutos dependiendo de la cantidad de hosts (tiempo establecido gracias a las pruebas realizadas), además se selecciona el número de agentes en este caso se ejecuta en un solo agente, las configuraciones de esta sección se pueden ver en la siguiente imagen.



G. Configuración de trabajos

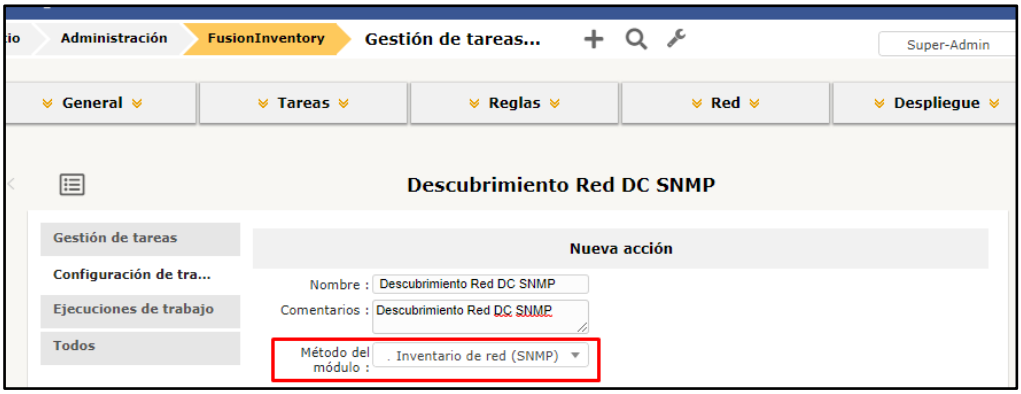
En la parte derecha de la configuración de la tarea hacer clic en el apartado "Configuración de trabajo" en el cual se debe incluir un nombre identificativo y una descripción, y como siguiente parámetro seleccionar como método de modulo "Descubrimiento de red" y hacer clic en añadir.

En la configuración que aparece se debe configurar un destino y un actor, para el destino se debe seleccionar el tipo de Rango de IP y el elemento de destino la red creada anteriormente en este caso “RED DATACENTER” y hacer clic en añadir elemento de destino.

En la misma pestaña se debe agregar un actor, de tipo agente y se selecciona como elemento de actor el agente previamente configurado y hacer clic en añadir elemento de actor.

Para que estos parámetros se almacenen debe hacer clic en actualizar. Con este proceso se ha terminado de configurar el descubrimiento de red por IP.

Para que el servidor recepte la información completa de los equipos mediante SNMP se debe crear una nueva tarea con el mismo proceso anterior y se debe crear un trabajo donde en el método de modulo se debe seleccionar “Inventario de red SNMP”.

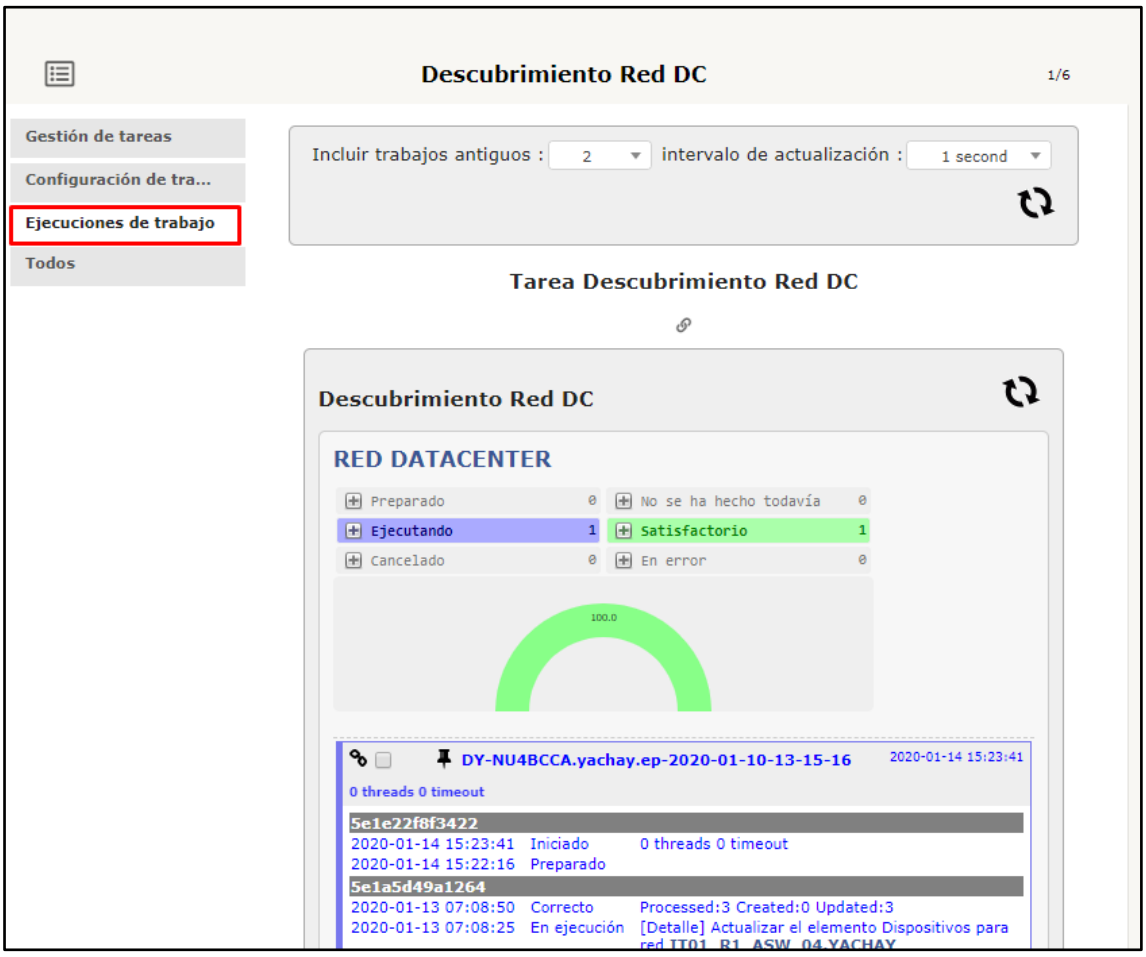


Y al igual que en el anterior proceso se configura el mismo destino y el mismo actor.

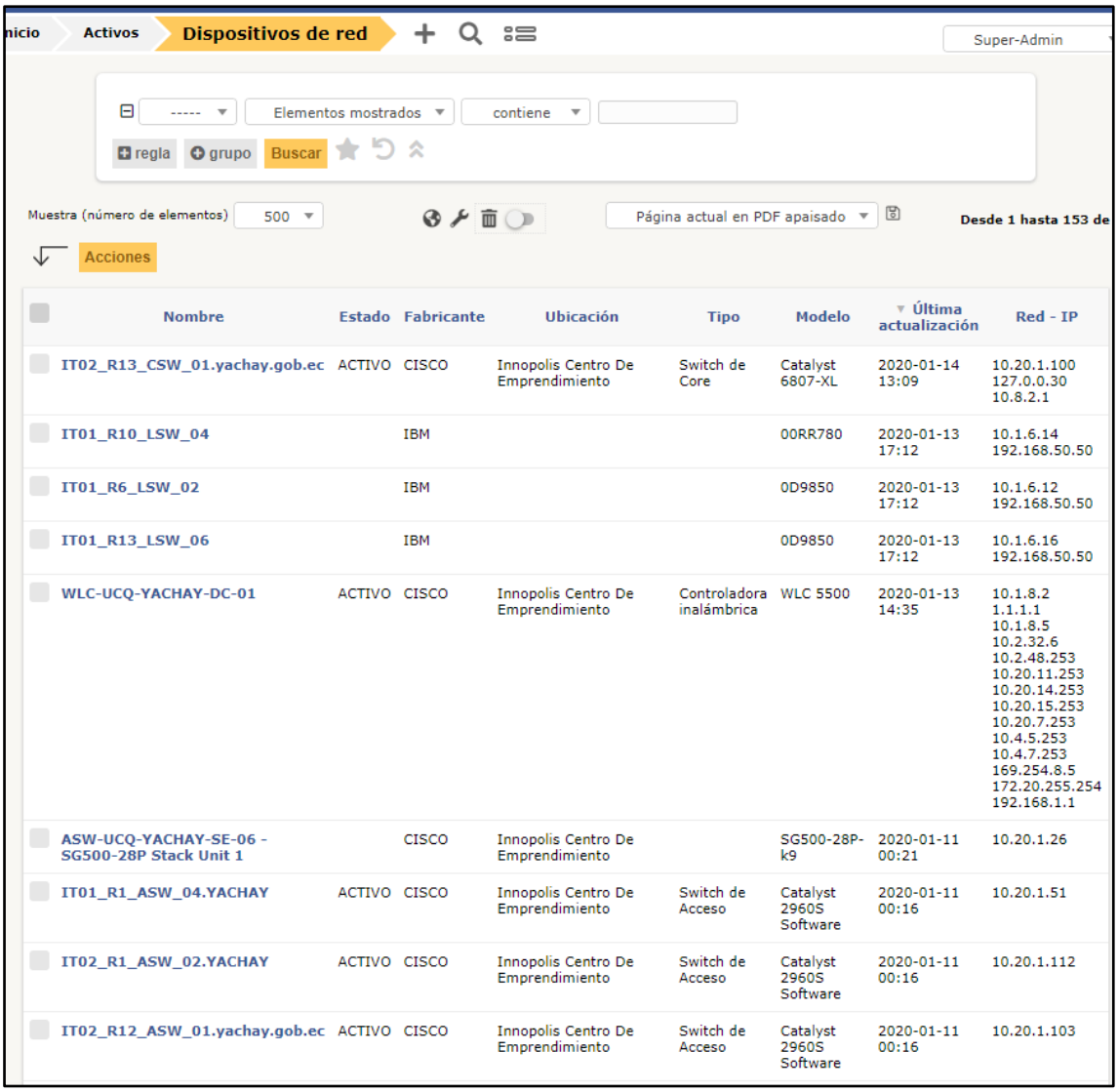
H. Ejecución de tareas automáticas

Al revisar el inventario actual en la sección dispositivos de red no se encuentra ningún dispositivo registrado, como se muestra en la imagen siguiente.

En el tiempo establecido para la recolección de información las tareas se ejecutarán de manera automática sin que el usuario realice alguna acción, para revisar este proceso se puede acceder a la siguiente dirección: Administración > FusionInventory > Gestión de Tareas > NOMBRE_DE_TAREA > Ejecución de trabajos



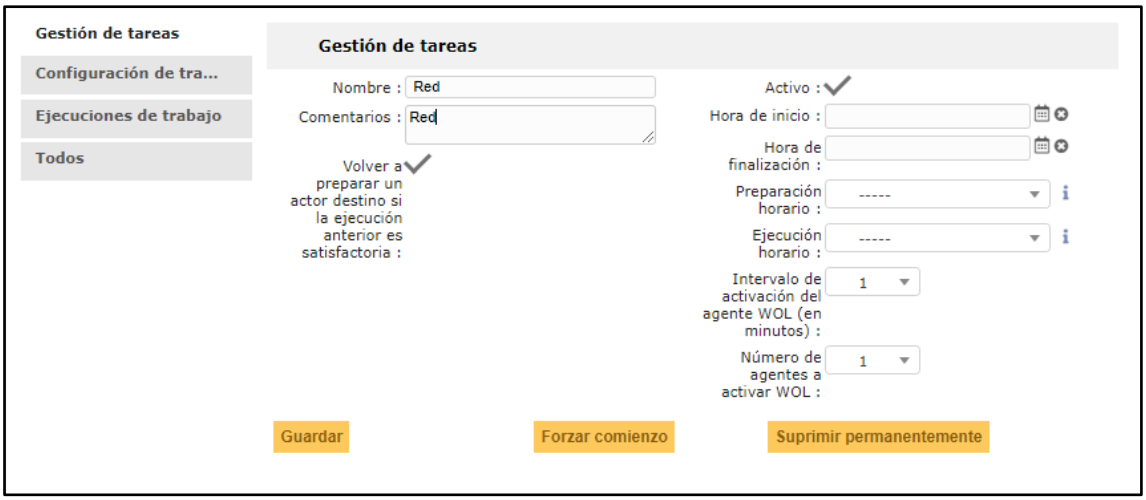
Luego de la ejecución del descubrimiento de red, y del inventario SNMP los equipos deben haber sido agregados correctamente, se puede revisar en Activos > Dispositivos de red, en caso de que no se encuentren en este apartado pueden estar incluidos en “Dispositivos no gestionados”.



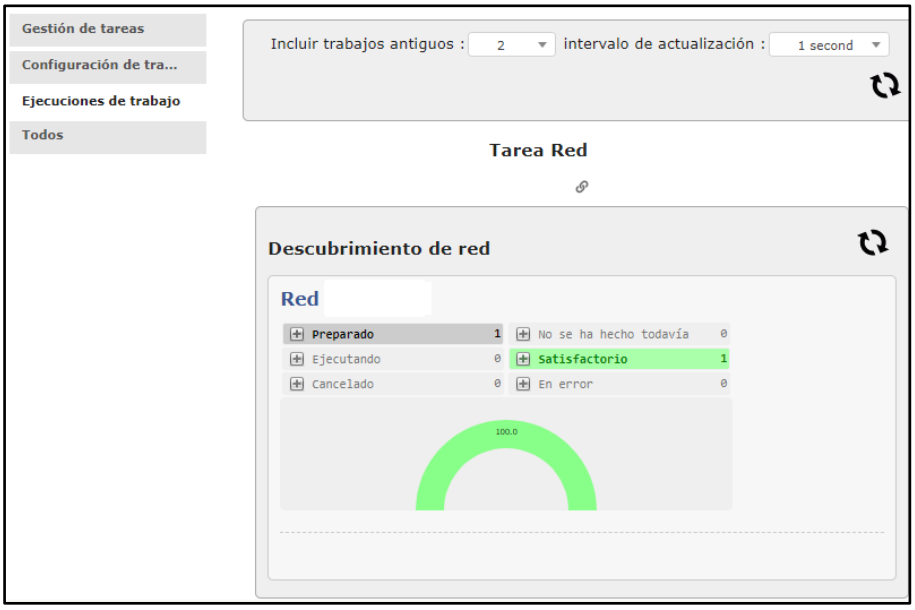
Nombre	Estado	Fabricante	Ubicación	Tipo	Modelo	Última actualización	Red - IP
IT02_R13_CSW_01.yachay.gob.ec	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Core	Catalyst 6807-XL	2020-01-14 13:09	10.20.1.100 127.0.0.30 10.8.2.1
IT01_R10_LSW_04		IBM			00RR780	2020-01-13 17:12	10.1.6.14 192.168.50.50
IT01_R6_LSW_02		IBM			0D9850	2020-01-13 17:12	10.1.6.12 192.168.50.50
IT01_R13_LSW_06		IBM			0D9850	2020-01-13 17:12	10.1.6.16 192.168.50.50
WLC-UCQ-YACHAY-DC-01	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Controladora inalámbrica	WLC 5500	2020-01-13 14:35	10.1.8.2 1.1.1.1 10.1.8.5 10.2.32.6 10.2.48.253 10.20.11.253 10.20.14.253 10.20.15.253 10.20.7.253 10.4.5.253 10.4.7.253 169.254.8.5 172.20.255.254 192.168.1.1
ASW-UCQ-YACHAY-SE-06 - SG500-28P Stack Unit 1		CISCO	Innopolis Centro De Emprendimiento		SG500-28P-k9	2020-01-11 00:21	10.20.1.26
IT01_R1_ASW_04.YACHAY	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Acceso	Catalyst 2960S Software	2020-01-11 00:16	10.20.1.51
IT02_R1_ASW_02.YACHAY	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Acceso	Catalyst 2960S Software	2020-01-11 00:16	10.20.1.112
IT02_R12_ASW_01.yachay.gob.ec	ACTIVO	CISCO	Innopolis Centro De Emprendimiento	Switch de Acceso	Catalyst 2960S Software	2020-01-11 00:16	10.20.1.103

I. Ejecución de tareas manuales

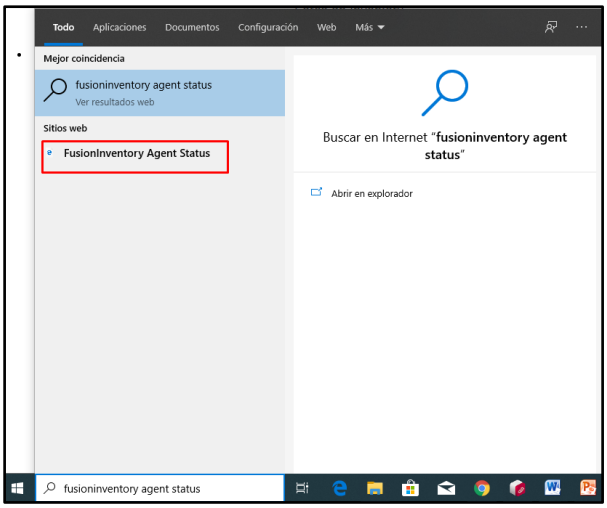
Para la ejecución de las tareas de manera manual, se debe realizar el mismo proceso para crear una tarea, con la diferencia de que no agregaremos ningún tiempo como se muestra en la **¡Error! No se encuentra el origen de la referencia.**, y adicional se crean los trabajos de gual manera.



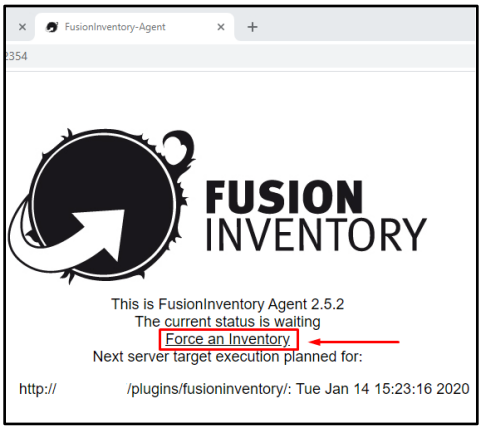
En la gestión de tareas se puede “Forzar comienzo” hacer clic en dicho botón, una vez que se haga clic en el botón revisar la ejecución de trabajos, en el apartado de preparado debe aparecer “1” caso contrario forzar comienzo nuevamente, cuando ya se tenga preparada una ejecución de trabajo como se muestra en la imagen.



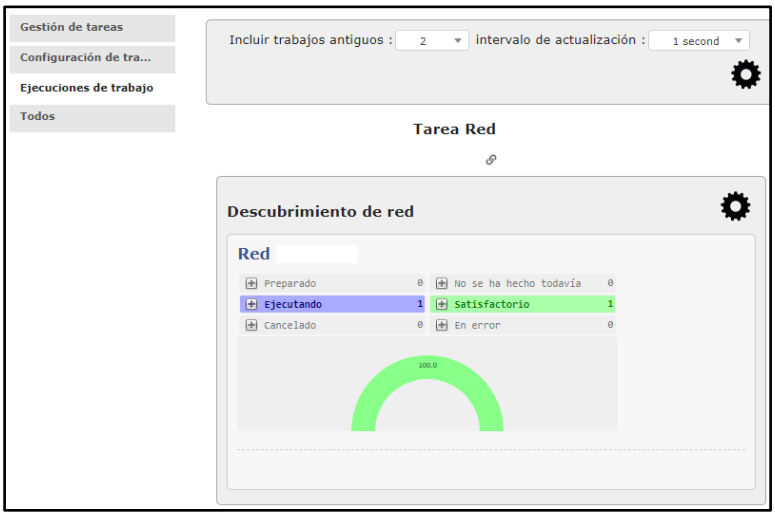
El en computador donde se encuentra el agente instalado en la barra de búsqueda, ingrese FusionInventory, y seleccionar FusionInventory Agent Status como se muestra en a continuación.



Este se abrirá en un navegador, en el cual se debe hacer clic en “Force an Inventory”



Una vez forzado el agente se debe revisar el estado de la tarea nuevamente, esta debe haber pasado de estado “Preparado” al estado “Ejecutando”.



ANEXO 8: Configuración de correo electrónico

A. Recepción de correos y creación de tickets automáticos.

Con un usuario con nivel de super administrador ingresar a la siguiente ruta: Configuración > Destinatarios > "+" y hacer clic en agregar para crear un nuevo destinatario.

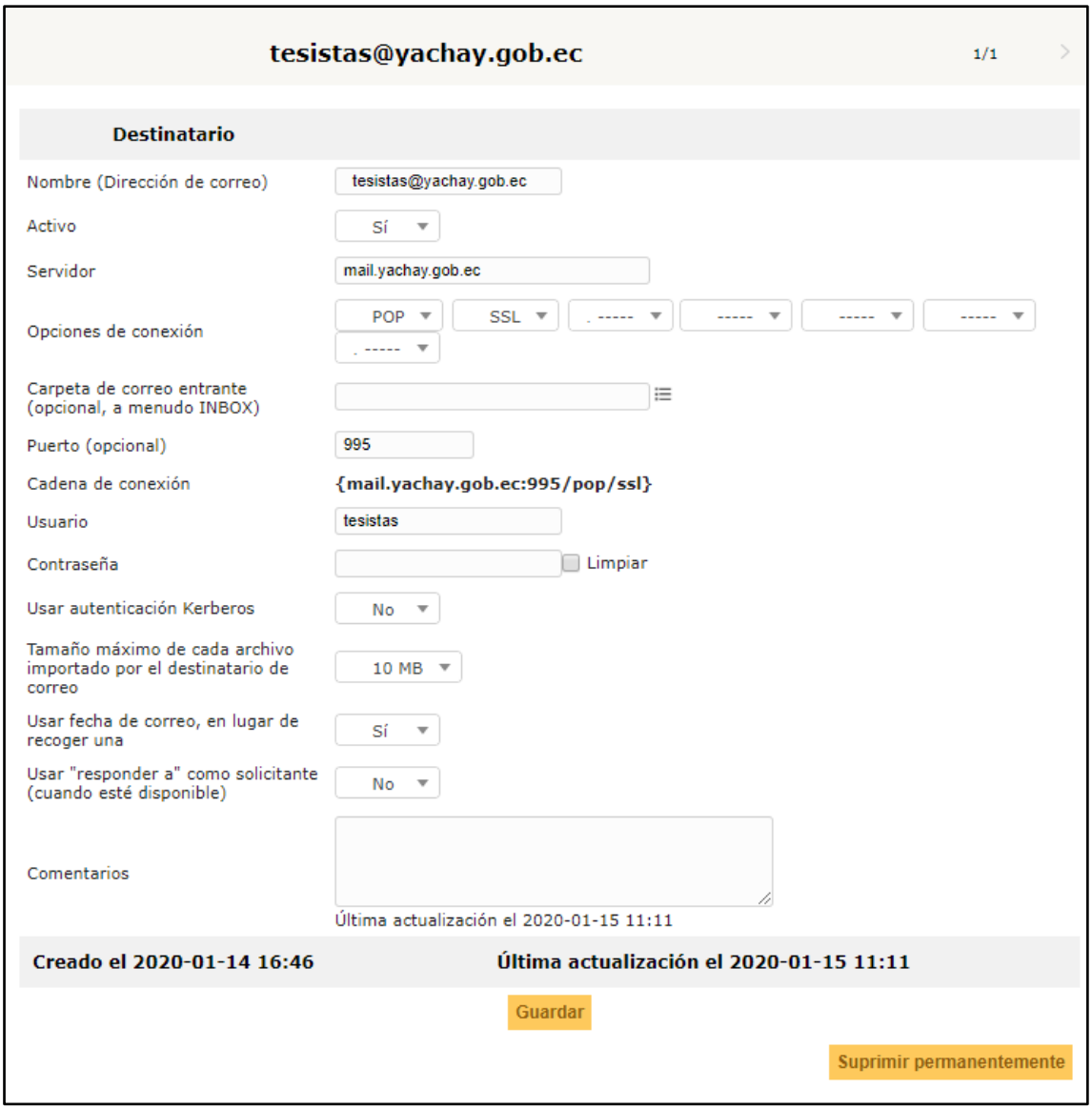
Figura 46. Creación de nuevo destinatario de correo electrónico para GLPI

Fuente: Interfaz GLPI

Llenar la información solicitada donde:

- Nombre: ingresar la dirección de correo electrónico
- Activo: permite seleccionar si el correo se encuentra n modo funcional o no
- Servidor: ingresar la dirección completa del dominio o la IP del servidor de correo electrónico.
- Opciones d conexión: puede seleccionar diferentes opciones según su servidor de correo ya sea POP o IMAP, tiene certificado SSL o no, con certificado TTL o TLS entre otros.
- Carpeta de correo entrante: la ubicación de la carpeta que se ha configurado dentro del servidor, esta no es necesaria si no se conoce la ruta específica.
- Puerto: el número de puerto de comunicación para la recepción de correo.

- Usuario: el usuario creado en el servidor de correo.
- Contraseña: la clave de acceso al servidor de correo.
- Autenticación Kerberos: pregunta si el servidor de correo es Kerberos.
- Tamaño máximo de cada archivo incorporado por el destinatario de correo: permite seleccionar el tamaño máximo del correo electrónico si este excede este tamaño no lo tomara como un ticket valido.
- Usar fecha de correo: brinda la opción de que el ticket se cree con la fecha que se envió el correo, o la opción de escoger una fecha y hora al momento de asignar el ticket.



sFigura 47. Ejemplo de configuración de destinatario para recepción correo electrónico en GLPI

Fuente: Interfaz GLPI

Para almacenar la información se debe hacer clic en el botón guardar. En la parte izquierda se encuentra un sub menú “Acciones”, dentro del cual tiene un botón con la función de recuperar los coreos electrónicos y crearlos como tickets, esta función puede usarse para crear los tickets de manera manual.

Figura 48. Recuperación de correos y generación de tickets

Fuente: Interfaz GLPI

Si las configuraciones anteriores fueron realizadas correctamente obtendremos un mensaje de información con el número de peticiones generadas, caso contrario aparecerá un mensaje de error de color rojo.

Una vez concluida esta configuración se deben receptar las solicitudes automáticamente en un lapso de 10 minutos, para cambiar este tiempo hay que dirigirse a la siguiente ruta: Configuración > Acciones automáticas, y buscar la acción de nombre “mailgate”

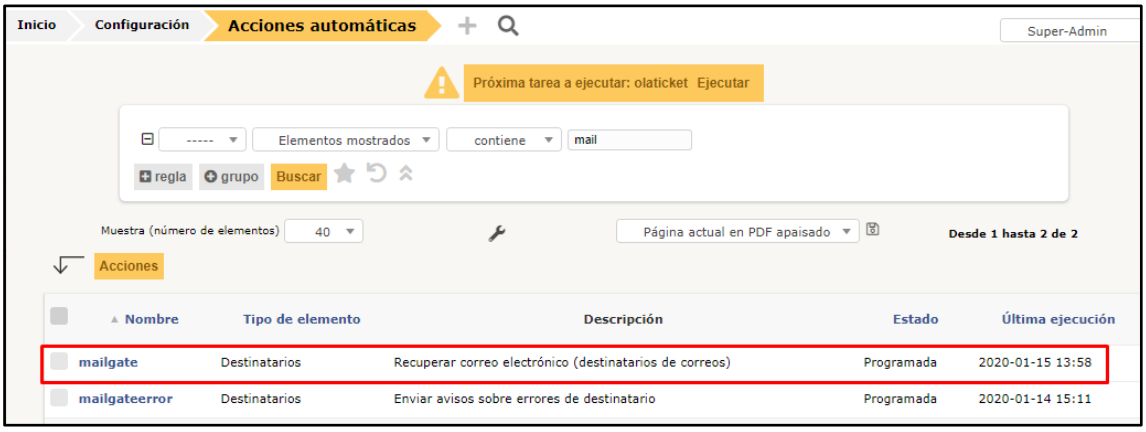


Figura 49. Búsqueda de proceso para recepción de correos automáticamente

Fuente: Interfaz GLPI

Hacer clic sobre el nombre y en la información mostrada escoger la frecuencia en la cual se debe ejecutar la tarea, además verificar si el modo de ejecución está en la opción CLI, el cual es un proceso de Cron generado por el sistema de GLPI.

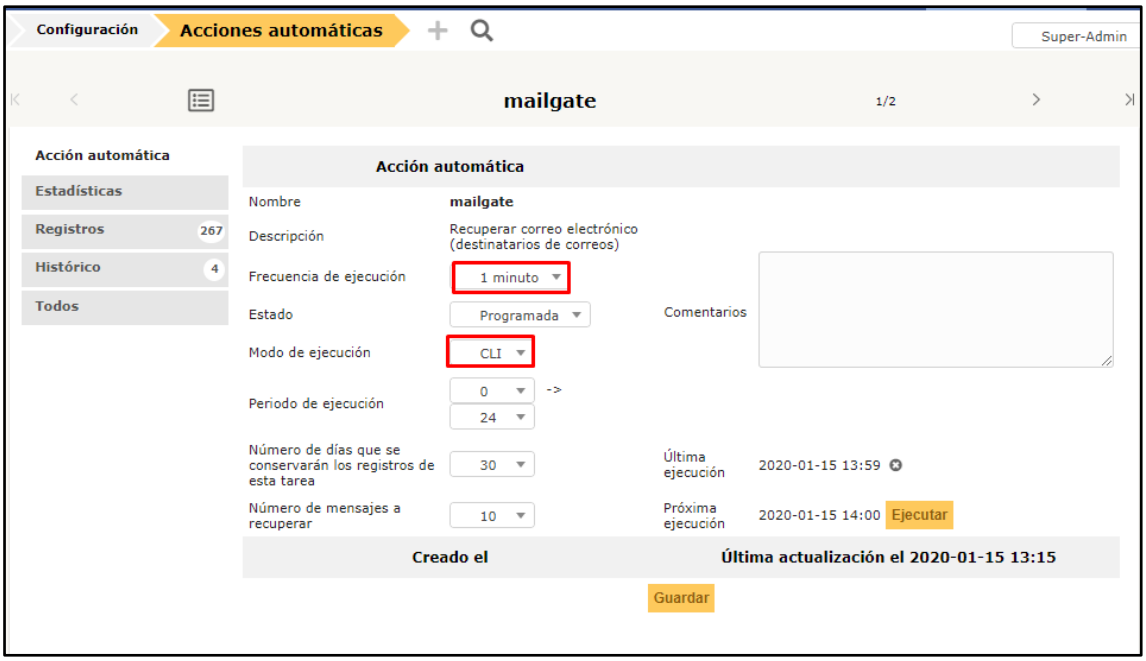


Figura 50. Configuración de tiempo para recepción de correos electrónicos y creación de tickets

Fuente: Interfaz GLPI

Para que los cambios surjan efecto debe hacer clic en guardar.

B. Envío de notificaciones automáticas.

Para enlazar a GLPI a un servidor de correo para el envío de correos, con un usuario con privilegios de superadministrador, se ingresa a la siguiente ruta: Configuración > Notificaciones > Configuración de los seguimientos por correo

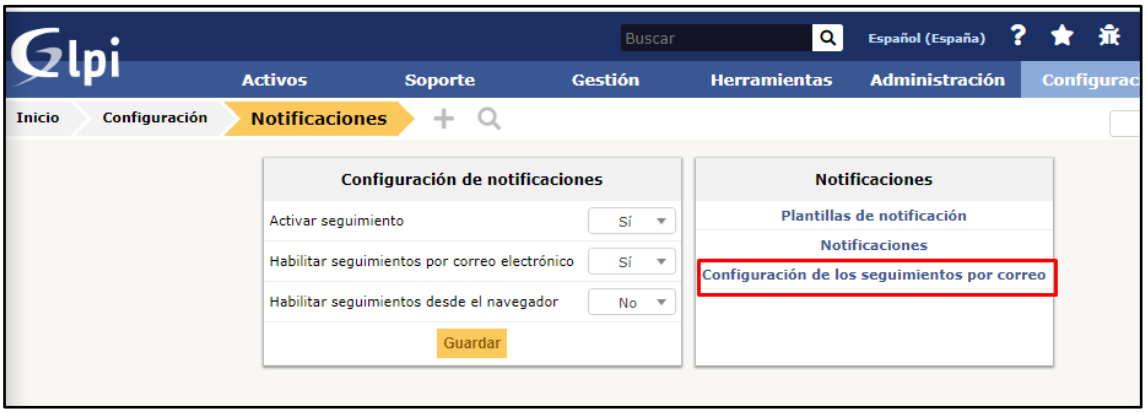


Figura 51. Creación de seguimiento de correo en GLPI

Fuente: Interfaz GLPI

En esta ventana se debe ingresar la información referente al correo de soporte que va a ser el que enviara los correos donde:

- Correo del administrador: ingrese el correo del administrador
- Nombre del administrador: ingrese el nombre del administrador registrado en el servidor de correo electrónico
- Desde el correo electrónico: ingrese la dirección de correo desde el cual se va a enviar el correo electrónico (puede ser el mismo que el anterior) a los usuarios.
- De nombre: poner el nombre del usuario o cuenta registrada para el envío de correos con la que se registró en el servidor de correo electrónico
- Añadir documentos en las notificaciones de las peticiones: permite la inclusión de documentos en caso de ser necesario hacia el técnico o al usuario que realizo la petición.

- Firma de los correos: Ingrese un mensaje el cual se enviará al pie del correo electrónico.
- Forma de envío de correos: Seleccionar el tipo de envío entre PHP, SMTP, SMPT+SSL, o SMTP+TLS.
- Máx. Reintentos de entrega: seleccione la cantidad de intentos de envío de un correo electrónico antes de marcar error.
- Tratar de entregar de nuevo en: seleccione el tiempo en minutos en el cual se vuelve a hacer el intento de envío de un correo electrónico.

Al seleccionar una forma de envío diferente a PHP, se habilita la sección Servidor de correo donde:

- Comprobar certificado: permite verificar la validez de los certificados.
- Servidor SMTP: ingrese la dirección completa del dominio del servidor de correo, o a su vez la ip.
- Puerto: el puerto de comunicación por el cual se va a enviar el correo.
- Usuario SMTP (opcional): ingresar el usuario que envía el correo electrónico desde glpi, en este caso el usuario de soporte.
- Contraseña SMTP (opcional): ingrese la contraseña del usuario de correo electrónico.

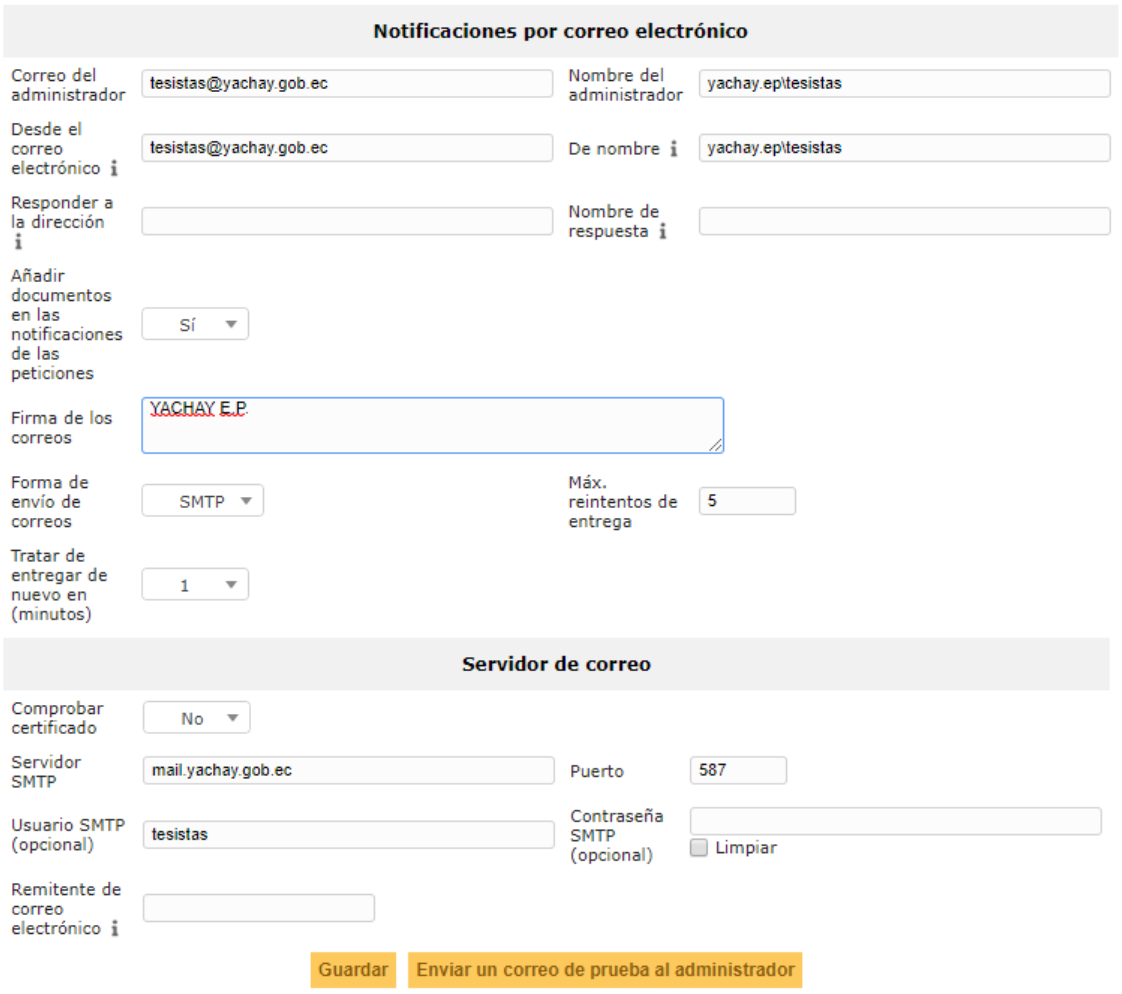


Figura 52. Configuración de notificaciones por correo electrónico

Fuente: Interfaz GLPI

Para almacenar la información debe hacer clic en el botón guardar, para probar si las configuraciones realizadas están correctas puede hacer clic en el botón enviar un correo de prueba al administrador.