UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad de Ingeniería

Carrera Profesional de Ingeniería informática y de Sistemas

INFLUENCIA DE LA IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE INFRAESTRUCTURA TI PARA GESTIONAR LAS INCIDENCIAS EN LA RED LAN DEL HOSPITAL REGIONAL DE CAJAMARCA.

Ortiz Valderrama, Mauricio Juan

Mori Chavez, Anjhel Yeferson

Asesor:

Ing. Jose Carlos Távara Carbajal

Cajamarca - Perú

Junio – 2017

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad de Ingeniería

Carrera Profesional de Ingeniería informática y de Sistemas

INFLUENCIA DE LA IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE INFRAESTRUCTURA TI PARA GESTIONAR LAS INCIDENCIAS EN LA RED LAN DEL HOSPITAL REGIONAL DE CAJAMARCA.

Tesis presentada en cumplimiento parcial de los requerimientos para optar el Título Profesional de Ingeniero Informático y de Sistemas.

Bach. Ortiz Valderrama, Mauricio Juan

Bach. Mori Chavez, Anjhel Yeferson

Asesor:

Ing. Jose Carlos Távara Carbajal

Cajamarca - Perú

Junio – 2017

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

APROBACIÓN DE TESIS PARA OPTAR TÍTULO PROFESIONAL

INFLUENCIA DE LA IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE INFRAESTRUCTURA TI PARA GESTIONAR LAS INCIDENCIAS EN LA RED LAN DEL HOSPITAL REGIONAL DE CAJAMARCA.

Presidente: _____

Secretario: _____

Vocal: _____

Asesor: _____

A:

Dios por habernos permitido llegar hasta éste punto y habernos dado salud para lograr nuestros objetivos, además de su infinita bondad y amor. Por habernos dado paciencia y sabiduría cuando más lo necesitábamos.

A nuestros padres por ser el pilar fundamental en todo lo que somos, en toda nuestra educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

A nuestros amigos Junior Yañez, Luis Gastolomendo, Carlos León, Eloy Arribasplata, Nelson Muñoz, Geison de la Cruz y Anthony Perez por su compañerismo, sus bromas y sus ánimos para culminar esta tesis.

AGRADECIMIENTOS

- A Dios por darnos salud para poder culminar la carrera, el proyecto y ahora la tesis.
- A nuestros Padres por el apoyo incondicional de inicio a fin en nuestra carrera y en el desarrollo de ésta tesis.
- Al Hospital Regional de Cajamarca, por habernos brindado información y la utilización de sus equipos para poder implementar y hacer las pruebas correspondientes.
- Al Ing. Carlos Hoyos Chávez por los aportes y apoyo que nos brindó de principio a fin en todas las interrogantes que suscitaron.
- A la Upagu y a sus docentes, por los aprendizajes obtenidos para mi formación personal.

RESUMEN

Influencia de la implementación de un sistema de monitoreo de infraestructura TI para gestionar las incidencias en la red LAN del Hospital Regional de Cajamarca es una tesis motivada en las incidencias presentadas en una red y como un sistema de monitoreo de TI las puede gestionar de acuerdo a las necesidades del cliente. Tiene como objetivo principal determinar la influencia de la implementación de un sistema de monitoreo de TI para gestionar las incidencias en la red Lan del Hospital Regional de Cajamarca, según sus dimensiones de tiempo de respuesta a la atención de una incidencia, exactitud para encontrar la incidencia en la red y la satisfacción de los usuarios finales del Hospital Regional de Cajamarca. Como hipótesis se plantea que la implementación de un sistema de monitoreo de TI influye de manera positiva en la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca. El tipo de investigación es aplicada, de carácter cuantitativo - no experimental – transeccional, se tomó un muestreo no probabilístico – intencional, ésta muestra consta de 6 ingenieros, los cuales conforman el área de informática del Hospital, ésta área es la encargada de atender las incidencias presentadas en la red. La principal conclusión es que la implementación de un sistema de monitoreo de TI influye positivamente en la gestión de incidencias de la red Lan, acortando a 10 minutos aproximadamente los tiempos de respuesta de atención a incidentes, acortando a 5 minutos aproximadamente el tiempo en encontrar una incidencia en la red y satisfaciendo

la necesidad del Hospital Regional de Cajamarca. Se recomienda implementar en cualquier tipo de organización, ya que, informará detalladamente en tiempo real toda la infraestructura TI de la red y así, las operaciones estarán más controladas lo cual, genera más ingresos.

Palabras Clave: Sistema de monitoreo, Infraestructura TI, Incidentes y red LAN.

ABSTRACT

Influence of the implementation of a system of monitoring of IT infrastructure to manage the impacts on the network LAN of the Regional Hospital of Cajamarca is a thesis that is motivated in the incidents presented in a network and as a system of monitoring of TI can manage them according to the needs of the client. Has as objective main determine the influence of the implementation of a system of monitoring of you for manage them incidents in it network Lan of the Hospital Regional of Cajamarca, according to their dimensions of time of response to the attention of an incidence, accuracy for find it incidence in it network and the satisfaction of the administrator of network of the Hospital Regional of Cajamarca. As hypothesis are raises that the implementation of a system of monitoring of yo influences of way positive in the management of incidents of the network LAN of the Hospital Regional of Cajamarca. The type of research is applied, of character quantitative-not experimental-transactional, is took a sampling not probabilistic-intentional, this shows consists of 6 engineers, which make up the area of computer of the Hospital, this area is it responsible of meet them incidents presented in the network. The main conclusion is that the implementation of a system of monitoring of you influences positively in the management of incidents of the network Lan, shortening to 10 minutes approximately them times of response of attention to incidents, shortening to 5 minutes approximately the time in find an incidence in the network and satisfying the need of the Hospital Regional of Cajamarca. Is recommended implement in any type of organization, since, will inform in detail in time real all the

infrastructure YOU of it network and thus, the operations will be more controlled which, generates more income.

Key words: System of monitoring, infrastructure TI, incidents and network LAN.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

En la actualidad, la aplicación de tecnología significa la gestión de procesos veloces de atención al cliente, debido a que agiliza todas aquellas tareas que podrían tener una mayor duración y ser más complicadas de realizar sin ella, mejorando así los procesos internos y externos, la organización de la información y la atención al cliente. Por consiguiente, la tecnología es el apoyo primordial para cualquier empresa y más aún para aquellas que poseen servicio de atención al cliente. Entre estos recursos tecnológicos se puede mencionar la herramienta de sistema de gestión de incidencias, la cual permite a los usuarios mantener un seguimiento de los problemas y resoluciones durante su ciclo de vida. El uso de este tipo de sistema ha tenido un impacto importante en la productividad de aquellas empresas que los utilizan, por lo que el desempeño mejora debido a sus propiedades y a los beneficios que aporta. En tal sentido, el estudio a continuación, basándose en un sistema de gestión de incidencias, está orientado a la influencia de la implementación de un sistema de monitoreo de infraestructura ti para gestionar las incidencias en la red LAN del Hospital Regional de Cajamarca.

En un mundo tan competitivo como el actual, el desarrollo de la Internet, el mercado globalizado (mecanismos financieros internacionales y mercados conectados entre sí) y el crecimiento tecnológico de las empresas, más el gran volumen de información que fluye a través de estas; las organizaciones deben estar más preparadas para asegurar que la información que fluye a través de su red

y servicios, tengan una mayor disponibilidad y performance. Ante lo mencionado, los encargados de TI deben estar constantemente monitoreando y observando cuales son las posibles fallas en la infraestructura TI que dificulten la eficiencia de los procesos. Actualmente existen un sin número de dispositivos TI que pertenecen a la red y servicios de una organización, los cuales, si no son controlados eficazmente pueden causar problemas de conectividad, performance y disponibilidad de servicios internos. A sí mismo, si tomamos en cuenta el tipo de información que puede fluir a través de estos servicios y se ven afectados por fallos no controlados a tiempo en los dispositivos, la magnitud del problema puede ser mayor. Por ello, se debe monitorear constantemente la infraestructura de TI (Tecnologías de Información). Sin embargo, el procedimiento de monitoreo de servidores y servicios puede ser tedioso y peligroso (Zhang & Zhang, 2010). Es por ello que las compañías y organizaciones actualmente en el mundo requieren que sus servicios sean monitoreados para detectar con mayor rapidez cualquier caída o alteración que estos puedan sufrir (Papazoglou, 2005).

En el Perú, la implementación de sistemas de monitoreo de infraestructura TI aún es incipiente, debido a que la accesibilidad, instalación o mantenimiento de un sistema de monitorización de TI es poco difundido. Además, la instalación de un sistema de infraestructura TI es una serie de pasos con cierto grado de dificultad y no es disponible para cualquier persona que no tenga conocimientos informáticos. (Gallardo, 2011) En la región de Cajamarca, hasta el momento no se ha registrado proyectos de ningún tipo que involucren la implementación o hagan referencia a un sistema de monitoreo de infraestructura TI, por lo que, resulta un tanto difícil

encontrar información en forma de conclusiones o recomendaciones que puedan servir de ayuda en este proyecto.

1.2. Definición del problema

En el Hospital Regional de Cajamarca, el monitoreo de la red es una tarea que se vuelve compleja, debido a una gran variedad de factores, por ejemplo:

- La gran cantidad de dispositivos TI: En el Hospital Regional de Cajamarca los dispositivos TI son mayores a 150 unidades y atenderlos demanda un costo y tiempo.
- Los diversos estados a recolectar continuamente por cada dispositivo: tener que ir presencialmente a todos los dispositivos para recolectar información sobre el funcionamiento demanda tiempo y dinero.
- La carencia de un criterio que establezca una guía para seleccionar los parámetros críticos del Hospital Regional de Cajamarca.
- Falta de un procedimiento que apoye y guie al encargado de TI, en el proceso de implementación y actualización de un sistema de monitoreo de la infraestructura TI del Hospital.

Las fallas y consecuencias más comunes son las siguientes:

- Controles manuales poco confiables
- Actividades y funciones no definidas del personal a cargo de atender los incidentes
- No existe atención oportuna y toma mucho tiempo darle solución
- Encontrar el problema a veces tarda demasiado

- Servicios caídos
- Ningún sistema que notifique mediante alertas o algún evento.

Lo que genera las siguientes consecuencias:

- Daños de equipos y pérdida de información importante
- Caídas de los sistemas y por ende suspensión en determinado tiempo de la operatividad
- Quejas de usuarios internos y externos por mal servicio
- Identificación tardía de un problema futuro que pudiera surgir en un tiempo determinado
- Bajo rendimiento del sistema operativo

- Desgaste de recursos materiales y humanos en procesos que pueden ser automatizados.
- Pérdida de recursos económicos.

En tal sentido y considerando lo anteriormente mencionado, es evidente que el administrador requiere contar con herramientas y procedimientos para realizar el monitoreo de la infraestructura TI, y así poder simplificar sus tareas y aprovechar las ventajas de monitoreo.

1.3. Formulación del problema de investigación

¿De qué manera la implementación de un sistema de monitoreo de infraestructura TI influye en la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca?

1.4. Objetivos

1.4.1. Objetivo General

Determinar la influencia de la implementación de un sistema de monitoreo de infraestructura TI para gestionar las incidencias en la red LAN del Hospital Regional de Cajamarca

1.4.2. Objetivos Específicos

- Realizar una comparación de los diferentes sistemas de monitoreo más representativas y reconocidas por su desempeño y elegir la que mejor se adecue a los objetivos de la infraestructura tecnológica de la red LAN del Hospital.
- Implementar el sistema de monitoreo de infraestructura TI
- Establecer los parámetros críticos a ser medidos en los diferentes dispositivos de la infraestructura tecnológica de acuerdo a la importancia y beneficio al Hospital.
- Generar alertas ante la presencia de fallos o posibles fallos en la infraestructura TI del Hospital.

1.5. Justificación e Importancia

El hospital Regional de Cajamarca se ve en la necesidad de optimizar procesos vitales para su crecimiento, por el aumento de clientes y la gran cantidad de información que cada cliente genera. Dichos procesos requieren ser más específicos y a su vez tener un tiempo de respuesta más eficiente.

Tanto una empresa o institución debe mantenerse actualizada e innovar sus sistemas de información, con la necesidad de balancear de manera proporcional sus crecimientos, entre los cuales se destaca el aumento del número de clientes, lo que demanda una ampliación y mejoramiento de los sistemas de información.

Si se posee un sistema el cual genere una respuesta con mayor rapidez al cliente, el impacto se verá reflejado totalmente en la productividad y confiabilidad de la empresa, pues se fortifica todo proceso y todo aspecto, tanto económico como administrativo.

Es importante para el Hospital Regional de Cajamarca pueda contar un sistema que ayude a mejorar el rendimiento y el tiempo de respuesta en la gestión de incidencias de los dispositivos de la infraestructura TI. Por lo que, en el presente proyecto de tesis, se propone un modelo de implementación de un sistema de monitoreo que proporcione mecanismos para responder a los problemas previamente planteados:

- Proveer un modelo que guie el proceso de implementación de un sistema de monitoreo de la infraestructura TI de la red LAN.
- Proporcionar una herramienta de monitoreo centralizada para los dispositivos de la infraestructura TI de la red LAN que recolecte información de sus parámetros críticos.
- Mejorar la calidad de los servicios de tecnología prestados.
- Facilitar la gestión del administrador, proporcionándole información acerca de los estados de los dispositivos.

- Disminuir la incidencia de fallas y el tiempo de afectación de los servicios, precisando el origen de las mismas.
- Permitir delegación de las funciones de monitoreo sobre la herramienta a proponer, para que el administrador pueda aprovechar el tiempo en ejecutar otras tareas.
- Controlar vía web los estados de los dispositivos pertenecientes a la infraestructura TI de la red LAN.
- Optar por el uso de software libre en la mayoría de aplicaciones para reducir costos y problemas referentes al uso de licencias.

CAPÍTULO II

MARCO TEÓRICO

En el marco teórico, se explican los aspectos y tecnologías que fundamentaron el desarrollo del presente proyecto. Dentro de los aspectos que conforman el marco teórico se incluyeron: conceptos y elementos históricos, que permitieron la inferencia de tales conceptos, al igual que componentes y/o herramientas que hacen posible la implementación de los mencionados conceptos, que en la actualidad conforman estándares internacionales. La consideración de estos aspectos permite realizar un enfoque general y de alto nivel. También se analizaron sistemas de monitoreo, de modo de poder establecer sus ventajas y desventajas, para así determinar una referencia para el momento de la implementación. Y en las tecnologías principalmente tomamos como referencia a la infraestructura TI y la gestión de incidencias.

2.1. Antecedentes Teóricos

Víctor Arrebola Real (2013) en su proyecto "Sistema de monitorización de servidores Linux" se plantea como objetivo monitorizar los nodos de red en tiempo real, mediante la creación de un sistema de alertas que permita alertar mediante e-mail y/o sms cuando alguno de los aspectos parametrizados supere los rangos establecidos. Se utilizó la metodología de investigación cuantitativa para poder probar la hipótesis y los resultados fueron que durante la realización del proyecto se ha podido comprobar la dificultad de cumplir la planificación temporal prevista. Inicialmente se había previsto que el tiempo no sería un problema, pero la implicación en ciertos proyectos paralelos, no contemplados durante la planificación del proyecto ha complicado mucho la dedicación temporal. La tecnología de desarrollo de páginas Web ha crecido mucho durante los últimos años, haciendo que la programación de estas sea mucho más fácil

obteniendo resultados mucho más interesantes para el usuario final. Aun así, la linealidad aún es demasiado grande, aunque cada vez está más implantada la programación orientada a objetos, lo que nos aporta una mayor potencia y flexibilidad. La satisfacción una vez finalizado el mismo es indescriptible, tanto por el resultado, como por la cantidad de conocimientos adquiridos. Por lo tanto, la valoración final es muy positiva, dado que se han cumplido en mayor o menor medida todos los objetivos establecidos inicialmente, además de algunos que han ido surgiendo sobre la marcha durante el desarrollo del sistema.

Evelyn Valdez Zamora (2013) en su proyecto "Gestor automático de eventos en servidores mediante el uso de una matriz de escalamiento, propuesta basada en software open source" se plantea como objetivo automatizar el proceso de control de incidencias en servidores y la generación de sus alertas, manteniendo de esta forma la continuidad de las operaciones y acortando tiempos de respuesta ante fallos en los sistemas, así mismo, optimizar recursos de gestión de sistemas y automatizar los procesos de atención a eventualidades generando alertar por las vías de correo electrónico y/o llamada telefónica por medio de asterisk. Para llevar a cabo el desarrollo de este modelo de investigación es necesario realizar un diagnóstico de la situación planteada y, en segundo lugar, es describir y fundamentar con bases teóricas la propuesta, de la misma forma los procedimientos metodológicos, así como las actividades y los recursos necesarios, para llevar a delante la ejecución. Una vez culminado el diagnóstico y la factibilidad, se procede a la elaboración de la propuesta, lo que conlleva a desarrollar siguientes fases del proyecto. Se basa en proponer una solución a un problema práctico, con la finalidad de optimizar sus procesos y actividades, en la

que cada etapa aplica técnicas diferentes. Finalmente, los resultados fueron que mediante esta herramienta el usuario puede analizar el comportamiento de cada uno de los servidores, desde cualquier lugar, ya que puede acceder desde su celular o recibir alertas por el mismo medio, sin necesidad de estar todo el tiempo observando la pantalla de su monitor. De esta manera nos ayuda a atender en el menor tiempo posible los incidentes y nos evita que las operaciones y los procesos normales de nuestra empresa se detengan, ahorrando grandes cantidades de recursos como económicos, humanos y de tiempo.

Daniel Napoleón Vargas Collaguazo y Alex Manuel Loaiza Carpio (2014) en su proyecto “Instalación y configuración de Software Open Source para monitorear el servicio y la carga de un sistema Asterisk”, se plantearon como objetivo de desarrollar una solución tecnológica basada en el estudio, uso y manejo de un software de monitoreo open source con la cual se pueda llevar un control permanente sobre un servidor de central telefónica Asterisk del rendimiento de la plataforma, así como de todos los servicios de la misma a fin de evitar posibles errores y establecer mejoras en el sistema VOIP. Se utilizó la metodología de investigación experimental. Finalmente, los resultados fueron que el software Nagios tiene las mejores características para monitorear un Servidor Asterisk, además, la instalación y configuración de Nagios son procedimientos muy complejos pero necesarios para tener un buen sistema de monitoreo Voip Los reportes de Nagios son precisos y nos dan claramente la información de lo que está ocurriendo en el servidor Asterisk.

Barriga Martinez Edison Lennin (2013) en su proyecto “Análisis e implementación de un sistema de manejo de incidentes con funcionalidad extendida notificación de correo electrónico bajo gnu/Linux aplicado a los servidores y enlaces LAN y WAN de la empresa Edesa S.A.” se plantea como objetivo implementar y configurar un sistema de manejo de incidentes en un servidor Linux para el monitoreo de servidores y enlaces, garantizando el servicio de la red WAN de la compañía, analizando los servicios requeridos por EDESA para diagnosticar posibles fallas. La metodología de investigación que se utilizó es cuantitativa, no experimental. Finalmente, los resultados fueron que la implementación y configuración de un servidor de monitoreo mantiene al administrador de red informado del comportamiento de los enlaces de la red tanto LAN como WAN, además de tener un histórico de los trabajos realizado como memoria para solventar futuros problemas de manera rápida y efectiva, garantizando el servicio de la red. Nagios permite al administrador mantenerse informado del estado de los enlaces y servidores mediante el envío de alertas por correo electrónico a los miembros del departamento de Tecnologías de la Información (TI).

2.2. Fundamentos Conceptuales.

2.2.1. Importancia actual de la Infraestructura TI en las organizaciones

A lo largo de la historia se han dado muchos cambios en el funcionamiento de las organizaciones y en la mayoría de los casos estos han estado impulsados por novedades tecnológicas. Durante la revolución industrial, las tecnologías de producción permitieron pasar de una manufactura casi artesanal a la producción

mecanizada y masiva, de modo de satisfacer de la demanda de bienes de consumo esenciales y no esenciales. Además de crear nuevos paradigmas de producción, la revolución industrial influyo la ocurrencia de dos fenómenos interesantes:

- Las organizaciones empezaron a tener un enfoque donde el objetivo principal es el "negocio", es decir, que la ganancia de la organización sea rentable con respecto a los costos de producción y operación. Tal vez pueda parecer obvio, sin embargo, muchas organizaciones centran su funcionamiento en este concepto.
- Las maquinas que integraban la línea de producción o ensamblaje se volvieron el corazón de las organizaciones y, por lo tanto, mantener su operatividad y niveles de calidad del producto generado se volvió fundamental para el negocio.

Las líneas de producción iniciales estaban conformadas por maquinas mecánicas, las cuales se iban desgastando por su funcionamiento continuo. Este desgaste podía reflejarse en la calidad del producto o hasta en periodos indeterminados de tiempo que la producción se detenía, generando pérdidas al negocio. Es por esto que fue necesario realizar revisiones periódicas de las piezas y el producto terminado, así como también tareas de reparación y ajuste para garantizar el cumplimiento de los estándares y la mínima interrupción en la producción. Estas tareas periódicas de revisión, reparación y ajuste posteriormente fueron formalizadas en la disciplina conocida como control de procesos.

Posterior a la tendencia de producción masiva, empezaron a surgir nuevas empresas que centrarían su negocio en la prestación de servicios. Al igual que las

empresas de producción masivas, las empresas de prestación de servicios utilizarían la tecnología como línea de producción para entregar a sus clientes los servicios acordados. Luego, al introducirse las computadoras y sus redes e irse haciendo más accesible a las empresas, empezaron a integrarse a la infraestructura de producción para automatizar tareas y en el caso de ciertas organizaciones, las computadoras y sus redes se convertirían en la línea de producción.

Hoy en día, la gran mayoría de las organizaciones manejan sus operaciones a través del uso de la información electrónica, a diferencia de cómo se hacía en los inicios de la era de industrial. Los bancos y otras organizaciones financieras, las compañías de servicios como operadoras de telecomunicaciones, los sitios de comercio electrónico, por mencionar algunos, dependen críticamente de los sistemas de información que se apoyan en computadoras y redes, siendo esto la nueva línea de producción para sus respectivos objetivos de negocio.

Aun mas, la rápida evolución de las tecnologías de la información (TI) ha cambiado la visión del marco competitivo de las organizaciones, tal como lo expresan (Markus y Soh, 1993) debido a que les ha ocasionado, en algunos casos, tensiones por la necesidad de adquirir las tecnologías más recientes con el fin mantener su competitividad “. La visión tecnológica en las organizaciones se ha vuelto consciente de la importancia y tratamiento que requiere la infraestructura de TI, en cuanto a su inversión y mantenimiento; ya que, del buen desempeño y disponibilidad de estos recursos críticos, dependerá la mejora continua de la operatividad, productividad y de los productos finales generados.

2.2.2. Gestión de incidencias

La Gestión de Incidentes tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible, esto no debe confundirse con la Gestión de Problemas, pues a diferencia de esta última, no se preocupa por encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente en restaurar el servicio. Sin embargo, es obvio, que existe una fuerte interrelación entre ambas.

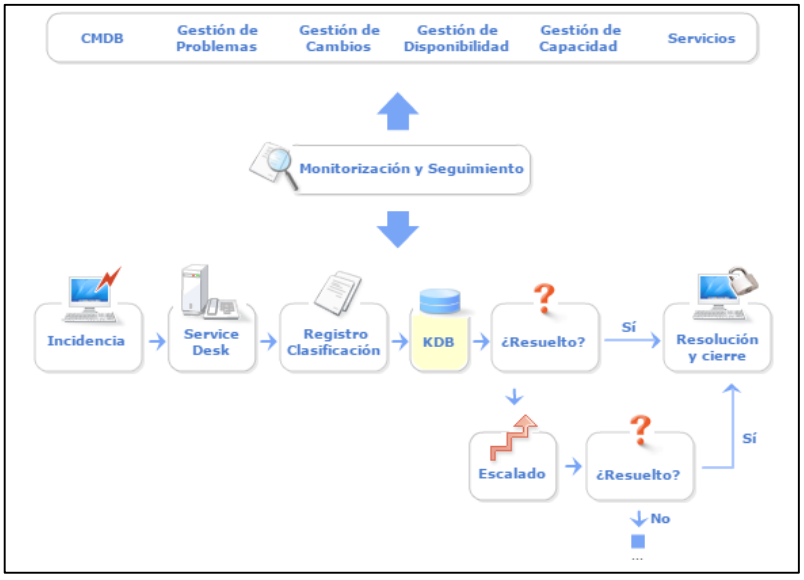


Figura 1. Gestión de incidentes

Fuente: http://itil.osiatis.es/curso_itil/gestion_servicios_ti/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php

Aunque el concepto de incidencia se asocia con cualquier mal funcionamiento de un sistema ya sea en hardware o en software según el libro de Soporte de servicio de ITIL un incidente es: “Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una

reducción de calidad del mismo". Por otro lado, una incorrecta Gestión de Incidentes puede acarrear efectos adversos tales como:

- Reducción de los niveles de servicio.
- Se dilapidan valiosos recursos: demasiada gente o gente del nivel inadecuado trabajando concurrentemente en la resolución del incidente.
- Se pierde valiosa información sobre las causas y efectos de los incidentes para futuras reestructuraciones y evoluciones.
- Se crean clientes y usuarios insatisfechos por la mala y/o lenta gestión de sus incidentes.

Las principales dificultades a la hora de implementar la Gestión de Incidentes se resumen en:

- No se siguen los procedimientos previstos y se resuelven las incidencias sin registrarlas o se escalan innecesariamente y/o omitiendo los protocolos preestablecidos.
- No existe un margen operativo que permita gestionar los "picos" de incidencias por lo que éstas no se registran adecuadamente e impiden la correcta operación de los protocolos de clasificación y escalado.
- No están bien definidos los niveles de calidad de servicio ni los productos soportados. Lo que puede provocar que se procesen peticiones que no se incluyen en los servicios previamente acordados con el cliente.

Por el nivel de prioridad los Incidentes se puede clasificar en:

- **IMPACTO:** determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o el número de usuarios afectados.
- **URGENCIA:** depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el SLA.

También se debe tomar en cuenta el tiempo de resolución y los recursos necesarios para resolverlos con los cuales los servicios "sencillos" se tramitan de inmediato.

2.2.3. Estructura

A diferencia de la versión 2 de ITIL la versión 3 establece una diferencia entre los Incidentes (interrupción de servicios) y Solicitudes de Servicio (consultas estándar de los usuarios), ya que, en esta versión la gestión de incidentes ya no se encarga de las solicitudes de servicio sino del cumplimiento de las mismas, además añade un proceso para tratar los casos urgentes llamados incidentes graves, así como una interfaz de procesos entre la gestión de eventos y la gestión de incidentes. La gestión de incidentes abarca los siguientes subprocesos**:**

- Soporte a Gestión de Incidentes.
- Registro y categorización de Incidentes.
- Resolución de Incidentes por el Soporte de Primera Línea.
- Gestión de Incidentes por el Soporte de Segunda Línea.
- Gestión de Incidentes Graves.
- Monitorización y Escalado de Incidentes.

- Cierre y Evaluación de Incidentes.
- Información Pro-Activa a Usuarios.
- Informes de Gestión de Incidentes.

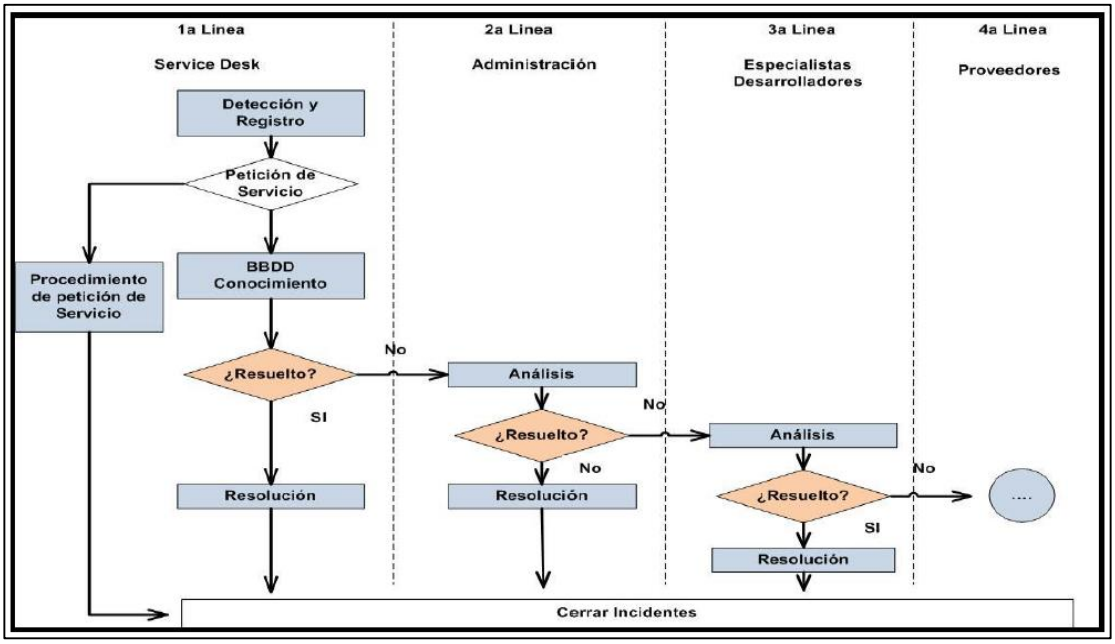


Figura 2. Diagrama gestión de incidencia

Fuente: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php

La consultora Pink Elephant (2008) publico diferentes encuestas realizadas a empresas de TI, gubernamentales, de finanzas, de fabricación y de salud que obtuvieron mejoras significativas en la gestión de los servicios de TI al implementar la filosofía gestión de incidencias de ITIL, tal es el caso de la empresa Procter & Gamble:

> Empezó con ITIL en 1999 y ha alcanzado recortar sus costos de operación en un 6% al 8%. Otro de los proyectos ITIL ha reducido las llamadas al centro de servicio de atención en un 10%. En cuatro años, la compañía reporto un ahorro total de cerca de $ 500 millones. (Pág. 7).

Otro caso significativo referenciado por Pink Elephant (2008) es de la empresa Visa:

> Visa: comenzó a introducir las directrices de administración de incidentes en el 2002, lo cual permitió mejorar el monitoreo de los cortes de servicios de las redes y los sistemas, y lograr una reducción en el tiempo para solventar los incidentes de hasta un 75%. (Pág. 6).

Estos y otros casos, reflejan los beneficios tangibles que proporciona ITIL.

ITIL define e incorpora en sus procesos tareas de monitoreo constante como parte de ciclo de mejora continua de los servicios de TI.

2.2.4. Modelo PDCA o Ciclo de Deming

Debido al entorno cambiante y competitivo de las empresas de hoy en día, y a la creciente exigencia de los usuarios en recibir servicios de alta calidad y disponibilidad, las organizaciones se han visto obligadas a optimizar el manejo de sus procesos y recursos, a través de la implementación de modelos que permitan ejecutar tareas planificadas en forma recurrente y constante para el cumplimiento de los objetivos previstos.

Uno de los modelos empleados para alcanzar la mejora continua en los procesos y servicios, es el ciclo de vida PDCA. Sus acrónimos en ingles hacen referencia a Plan, Do, Check y Act (ITIL, 2007). Originalmente fue desarrollado por Walter Shewart, no obstante, este fue popularizado por Edward Deming por lo que es conocido como ciclo de Deming (Janakiraman y Gopal, 2006).

Las etapas del ciclo PDCA consisten en (Janakiraman y Gopal, 2006) ver la figura 3:

- Planear (P): es la primera etapa del ciclo de Deming, llamada en ingles Plan. En esta se “establecen los objetivos y procesos necesarios para entregar resultados de acuerdo a los requerimientos del cliente y la organización” (Pág.104).
- Hacer (D): en esta etapa se lleva a cabo lo planificado de manera de “Implementar los procesos” (Pág. 104).
- Verificar (C): en ingles su sigla significa Check, etapa que consiste en “Monitorear y medir, procesos y productos contra las políticas, objetivos y requerimientos por producto, y reportar resultados” (Pág. 104).
- Actuar (A): su sigla en inglés significa Act. “Tomar medidas para mejorar continuamente el proceso, y desempeño” (Pág. 104).

Entre los beneficios de poner en práctica el ciclo de Deming están proveer efectivas y rápidas soluciones a diversos problemas, y documentar los procesos antes y después de la solución de los mismos, información que podrá ser utilizada en el siguiente ciclo de mejora continua (Janakiraman y Gopal, 2006).

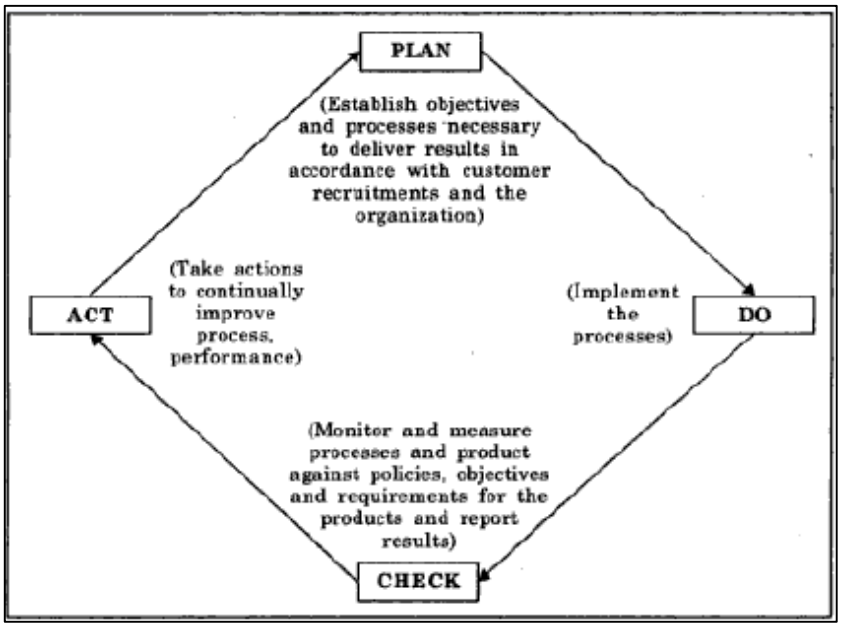


Figura 3. Etapas del marco de gestión continúa Deming.
Fuente: Janakiraman y Gopal (2006). *Total quality Management: Text and cases*. New Delhi: Prentice- Hall of India Private Limited

El PDCA es definido en el contexto del marco de gestión de TI por ITIL como un ciclo de gestión de procesos, que permite medir continuamente el desempeño de los proveedores de los servicios TI, y además de aplicar mejoras a los procesos, servicios e infraestructura TI, con el fin de incrementar la eficiencia, efectividad y rentabilidad. (ITIL, 2007).

Básicamente ITIL define el modelo PDCA de la siguiente forma:

- Planificar: diseñar o revisar los procesos que dan soporte a los servicios de TI.
- Hacer: implantar el plan y gestionar los procesos.
- Verificar: medir los procesos y servicios de TI, y compararlos con los objetivos y producir informes

- Actuar: planificar e implementar cambios para perfeccionar los procesos. (Pág. 34)

Diversas funciones y procesos de ITIL aplican explícitamente las etapas del PDCA. Entre las cuales están (Van Bon y Dyer, 2009)

> … la implantación de la mejora continua del servicio (CSI, Continual Service Improvement), en la función de seguridad de información en la fase del diseño del servicio y para la continua mejora de servicios, procesos y funciones en todo el ciclo de vida del servicio (Pág. 15)

La metodología PDCA es empleada como guía para el desarrollo del marco metodológico del presente proyecto por tratarse de un modelo de mejoramiento continuo de la calidad que permite rediseñar los procesos que posee un sistema de monitoreo de los recursos críticos de TI.

2.2.5. Componentes de monitorización remota

Son herramientas de monitoreo estandarizadas, que ayudan a los administradores de red a determinar en donde se encuentra un problema mediante el acceso remoto a los equipos.

En la actualidad existen diversas herramientas de apoyo al monitoreo remoto tales como WMI (Windows Management Instrumentation), RPC (remote procedure calls), RMI, ICMP, SMNP entre otros. Existen dos tipos de comunicación remota como la comunicación remota directa y la comunicación remota indirecta.

- La primera se refiere al uso de los componentes locales de monitoreo del equipo, por ejemplo, ICMP, traceroute o tracert y SNMP.
- La segunda requiere la instalación local de programas llamados agentes que se encargan de establecer la comunicación del equipo con el repositorio de monitoreo.

A continuación, se definirán algunos componentes de monitoreo remoto utilizados por los administradores de red para verificar el estado de los dispositivos.

2.2.6. Windows Management Instrumentation

Según AJPDSoft (2010), Windows Management Instrumentation (WMI o Instrumental de administración de Windows) es una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa. WMI incluye un repositorio de objetos, a modo de base de datos de definiciones de objetos, y el administrador de objetos CIM, que controla la recopilación y manipulación de objetos en el repositorio y reúne información de los proveedores de WMI. Los proveedores de WMI actúan como intermediarios entre los componentes del sistema operativo, las aplicaciones y otros sistemas.

El Windows Management Instrumentation (WMI) es la implementación de Microsoft del Web Based Enterprise Management (WBEM) que es una iniciativa de la industria para desarrollar un estándar de tecnología para acceso a información de administración. WMI usa el Common Information Model (CIM) que es un estándar de la industria para representar sistemas, aplicaciones, redes,

dispositivos y otros equipos administrados. CIM es desarrollado y mantenido por el Distributed Management Task Force (DMTF).

WBEM trabaja independientemente del vendedor, protocolo y del estándar de administración, sin reemplazar a estándares de administración como SNMP. Esta tecnología realiza la gestión de recursos como registros, hardware, software, dispositivos, aplicaciones, etc.

La arquitectura de WMI posee tres capas: capa de recursos administrados, capa de aplicaciones consumidoras y capa de infraestructura WMI, como se puede observar en la Figura 4.

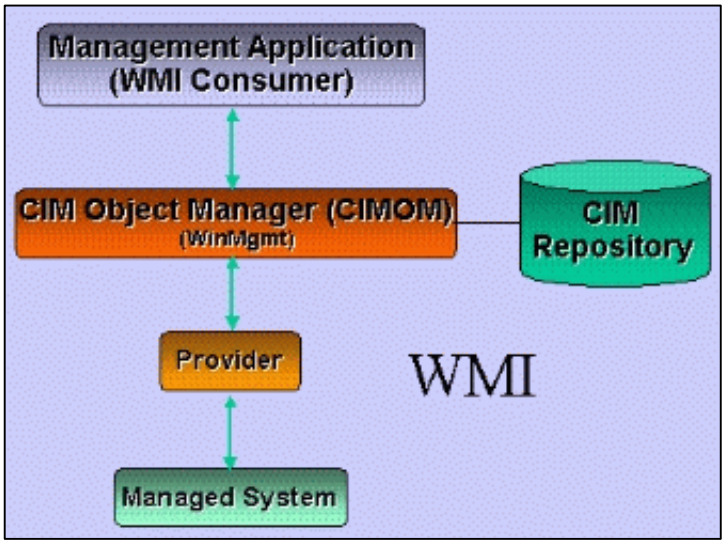


Figura 4. Arquitectura WMI
Fuente: https://msdn.microsoft.com/en-us/library/bb742445.aspx?f=255&MSPPError=-2147217396

Recursos Administrados: es cualquier componente físico o lógico, el cual es expuesto y administrado mediante WMI.

Aplicación consumidora: es una aplicación basada en Windows o un servicio de Windows que procesa los datos solicitados a un objeto administrado, o información provista por el objeto sin ningún tipo de solicitud. Esta aplicación puede realizar diferentes tipos de tareas como: medida de rendimiento, inventario de componentes de equipos, eventos, etc. Una solicitud a un objeto administrado puede ser realizada usando una consulta mediante el lenguaje WQL.

Infraestructura WMI: está compuesto de tres elementos: el CIMON (Administrador de objetos CIM), el repositorio CIM, y los proveedores. Mediante esta infraestructura los datos de configuración y administración se pueden definir, exponer, acceder y obtener su información

- CIMON (Administrador de objetos CIM): Es el componente principal de la infraestructura WMI porque maneja las interacciones entre las aplicaciones consumidoras y los proveedores. Las aplicaciones consumidoras, proveedores de objetos y extensiones de esquema interactúan con el CIMON por medio de cualquier lenguaje de programación que pueda registrar objetos COM, como C, C++, debido a que CIMON provee una interfaz de programación basada en COM.
- Repositorio CIM: (CIM o Modelo de Información Común) es un esquema orientado a objetos, y no depende de la implementación para describir la información de gestión de la red. La función del repositorio es almacenar datos estáticos, que generalmente son los datos operacionales de WMI como información del contenedor, y almacenar los identificadores de los

recursos administrados. Dentro de la información del repositorio CIM constan las clases a las que se accede mediante consultas WQL.

En resumen, WMI es un protocolo con características similares a SNMP, pero a diferencia del mencionado, es propiedad de Microsoft y solo es utilizado para plataforma Windows.

2.2.7 Simple Network Management Protocol

El protocolo SNMP se originó en 1988 a partir del protocolo SGMP (Simple Gateway Monitoring Protocol). Definido en RFC-1098, SNMP fue diseñado para optimizar el procesamiento de funciones simples sobre las que se construye el manejo de la red.

SNMP (Simple Network Management Protocol) es un protocolo estándar para la gestión y monitoreo de red. SNMP tiene la capacidad de permitirles a los administradores gestionar el rendimiento de la red y localizar problemas.

CISCO (2004) define en el Internetworking Technologies Handbook:

> El Simple Network Management Protocol (SNMP) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte del conjunto de protocolos Transmission Control Protocol/Internet Protocol (TCP / IP) SNMP permite a los administradores de red para gestionar el rendimiento de la red, encontrar y resolver problemas de red, y el plan de crecimiento de la red (pág. 1).

SNMP fue desarrollado para gestionar los dispositivos IP de la infraestructura TI, y reducir la complejidad que se torna la administración y monitoreo de los estados de sus variables de forma manual. Por estas razones, los fabricantes como CISCO e IBM, entre otros, incorporan en sus dispositivos este estándar de gestiona, además de desarrollar herramientas centralizadas que recolectan el estado de sus dispositivos. Sin embargo, en el mercado existen sistemas de monitoreo que pueden gestionar los estados de diferentes marcas y tipos de dispositivos IP.

Es importante conocer los elementos que se requieren para implementar la gestión SNMP. En el Internetworking Technologies Handbook CISCO (2004) se establecen tres componentes fundamentales para el funcionamiento de este protocolo.

- Los dispositivos administrados o elementos de red compatibles con SNMP.
- Los agentes.
- Los sistemas de gestión de red centralizado (NMS, sus acronimos en ingles significan Network Management System).

Asimismo, CISCO (2004) conceptualiza estos componentes de la siguiente manera:

> Un agente SNMP es un módulo de software de los dispositivos de red administrados que reside en el dispositivo administrado. Un agente tiene conocimiento local la información de gestión y convierte en el formato SNMP, para que luego esta sea

> transportada al NMS a través de SNMP Un NMS es una herramienta de software que monitorea y controla los dispositivos de red administrados por SNMP. Los NMS consumen en gran medida los recursos de procesamiento y de memoria (pág. 898).

Lo anterior pone de manifiesto la importancia de implantar un sistema de gestión y monitoreo que actúe en conjunto con el protocolo SNMP en dispositivos IP para obtener un preciso y detallado control de los estados y desempeño de los mismos.

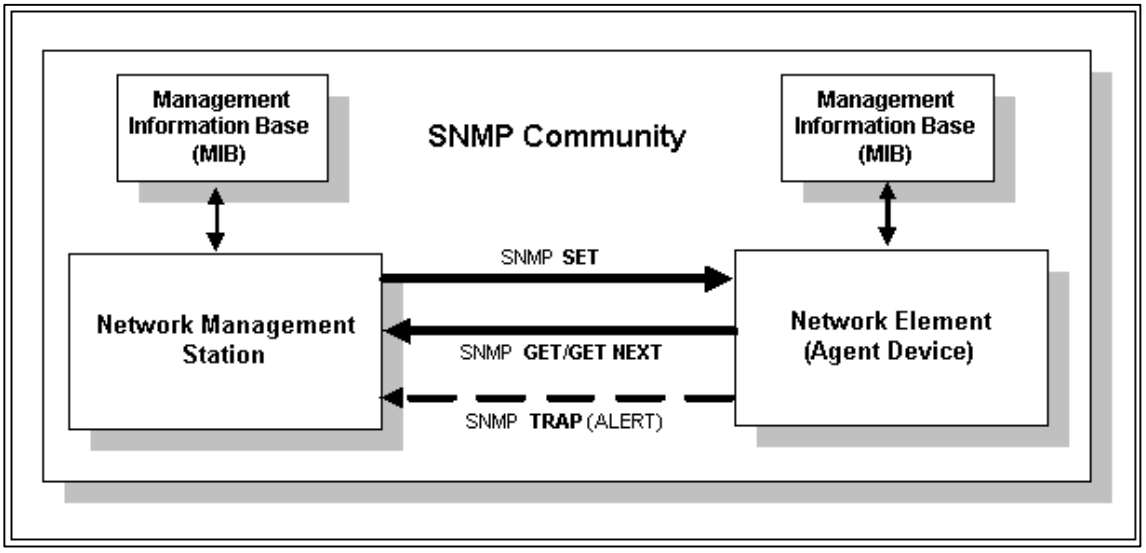


Figura 5. Protocolo SNMP

Fuente: http://www.keil.com/support/man/docs/rlarm/rlarm_tn_using_snmp.htm

2.2.8 Internet Control Message Protocol

ICMP es un protocolo de intercambio de mensajes de control perteneciente al conjunto de protocolos de TCP/IP, creado por el RFC 792, y es utilizado para detectar errores, realizar pruebas, diagnosticar y aislar problemas en una red.

ICMP es definido por Postel (1981) en el documento RFC 792 de la siguiente forma:

> Los mensajes ICMP son enviados en varias situaciones: por ejemplo, cuando un datagrama no puede alcanzar su destino, cuando el gateway no dispone de capacidad de almacenamiento temporal para reenviar el datagrama, y cuando el gateway puede dirigir al "host" para enviar el tráfico por una ruta más corta. El Protocolo Internet no está diseñado para ser absolutamente fiable. El propósito de estos mensajes de control no es hacer a IP fiable, sino suministrar información sobre los problemas en el entorno de comunicación. Sigue sin garantizarse que un datagrama sea entregado o que se devuelva un mensaje de control. Existe la posibilidad de que algunos datagramas no sean entregados, sin ningún informe sobre su perdida. Los protocolos de nivel superior que usen IP deben implementar sus propios procedimientos de fiabilidad en caso de que requieran comunicación fiable. Típicamente, los mensajes ICMP informan de errores en el procesamiento de datagramas. Para evitar la generación sin fin de mensajes acerca de mensajes, etc.; no se envían mensajes ICMP acerca de mensajes ICMP (pág. 1).

Citando lo anteriormente expuesto por RFC 792, ICMP es un protocolo de control, que colabora en gran medida con los procesos de los equipos de comunicaciones, tales como los routers y switches, y también ayuda a detectar

errores de red, congestión de la misma y calcula los tiempos de respuesta en el envío/ recepción de los paquetes IP.

En CISCO (2008), describe a ICMP como un protocolo que ayuda a seleccionar las mejores rutas disponibles para direccionar el trafico IP hacia un destino.

ICMP no proporciona información exacta de los problemas de la red, más bien este protocolo es utilizado como herramienta para apoyar el análisis que realizaran los administradores, suministrándole información suficiente para conocer el camino que deberán tomar para solventar los problemas.

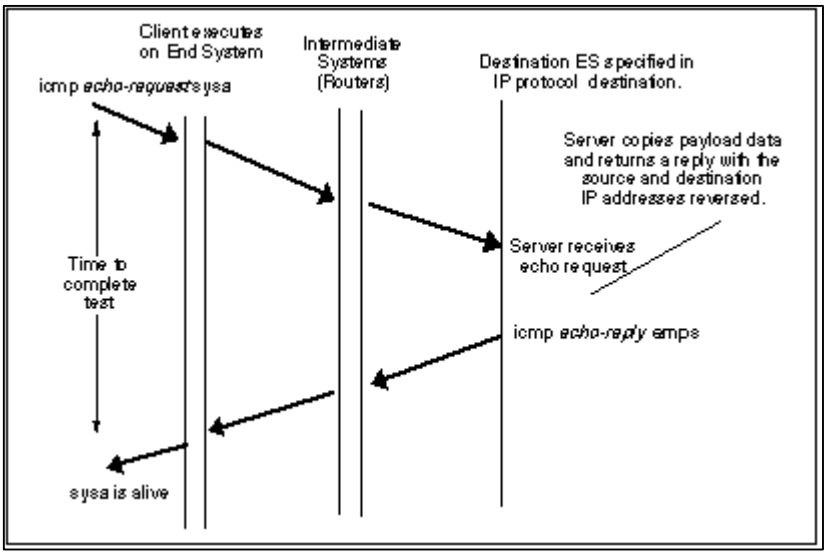


Figura 6. Formato del protocolo ICMP

Fuente: http://www.erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/icmp.html

2.2.9 Parámetros críticos de monitoreo

Los parámetros críticos son métricos o variables del hardware o software que forman parte de la infraestructura de TI y que al variar su estado impactan significativamente el cumplimiento de los objetivos de la organización, por ello es

importante identificarlos y medirlos constantemente, ya que son consideradas fundamentales para el buen funcionamiento de la organización.

La selección de los parámetros críticos varía de una organización a otra, dependiendo de los tipos de dispositivos que soportan la operación de la organización en la infraestructura de TI. Sin embargo, existen parámetros críticos comunes entre los dispositivos de TI que apoyan los servicios de la organización. Estos parámetros se relacionan con los componentes de temperatura, utilización de la memoria de almacenamiento y utilización del procesador o CPU, los cuales al variar sus valores fuera de los umbrales de funcionamiento normal alteran el desempeño del dispositivo. La identificación de los parámetros críticos de los dispositivos TI, forma parte del diseño inicial para la implementación de un sistema de monitoreo de la infraestructura de TI.

Técnicamente se consideran como parámetros críticos todas aquellas variables del hardware que, al variar de manera negativa, afectan el desempeño de un servicio de TI. Estos parámetros deben ser medibles, de modo que puedan incorporarse al monitoreo de los dispositivos de TI. Así, los administradores de TI podrán establecer umbrales de buen desempeño, según sea la demanda normal de los recursos y servicios utilizados, con el propósito de que al detectarse algún valor fuera de rango, se generen las alertas que notifiquen el surgimiento de algún problema; identificando los dispositivos afectados para que se ejecuten las acciones correctivas necesarias.

2.2.10 Parámetros críticos y comunes en los dispositivos TI

Independientemente de cual sea el modelo o marca de los dispositivos de TI, se pueden encontrar parámetros críticos comunes, tales como: uso del CPU, estado del funcionamiento del ventilador (fan), uso de la memoria de almacenamiento y medición de la temperatura, entre otros componentes.

CISCO (2009), en el manual de mejores prácticas para el monitoreo a través de la herramienta propietaria CISCO Unified Contact Center Enterprise with CISCO Unified Operations, se proponen recomendaciones sobre la supervisión básica del estado (Basic Health Monitoring) de los dispositivos de esta marca, entre las cuales clasifican los siguientes parámetros: de sistema (system) y de entorno (environment). Estos componentes se detallan en la tabla 1, la cual proviene de la fuente CISCO (2009).

Tabla 1: Monitoreo básico CISCO (2009)

Parámetros	Descripción
Sistema (system)	Incluye el uso de procesador y de la memoria del dispositivo junto con el estado de las interfaces en el dispositivo.
Entorno (environment)	Estado del ventilador del sistema(Fan), del sensor de temperatura del sistema, del sensor de voltaje y el suministro de energía del sistema del dispositivo.

Nota. Fuente: Cisco (2009) *Best Practices for Monitoring Cisco Unified Communications Manager with Cisco Unified Operations Manager.* Cisco Public Information.

Es importante destacar que las recomendaciones de CISCO son aplicadas para los dispositivos de comunicaciones de su marca. Sin embargo, en este proyecto de investigación, además de tomar como referencia esta clasificación básica de los parámetros de monitoreo (sistema y entorno), se propone incorporar a la misma parámetros críticos de conectividad de red para monitorear el estado de las

interfaces y la disponibilidad de los dispositivos IP, para de esta manera constituir un primer nivel de monitoreo. El propósito es definir un estándar de parámetros básicos y comunes entre los diferentes dispositivos IP de una plataforma TI (servidores, router y switch), que sirva para la configuración de las métricas en un sistema de monitoreo.

Tabla 2: Parámetros básicos de monitoreo.

Parámetros	Descripción
Sistema	1. Uso de procesador(es). 2. Uso del disco duro (aplica solo para servidores). 3. Utilización de la memoria RAM.
Entorno	1. Estado del ventilador (Fan). 2. Estado del sensor de temperatura. 3. Estado del sistema de suministro de energía
Red	1. Interconectividad entre los dispositivos (disponibilidad de las Interfaces). 2. Utilización de las interfaces de red 3. Tiempo de respuesta

Nota. Fuente: Los autores

2.2.11 Parámetros críticos de monitoreo de un conmutador

Los conmutadores o también llamados switch, son los dispositivos que se encargan de transportar la información en la red local de las organizaciones (LAN). Los problemas en los switchs afectan en gran medida a los usuarios de la red LAN. La detección de los problemas a tiempo en la red y el monitoreo proactivo de los parámetros críticos ayuda a evitar problemas potenciales. A continuación, en la tabla 3 se establece una clasificación de segundo nivel de monitoreo con ciertos parámetros críticos específicos de estos dispositivos.

Tabla 3: Parámetros críticos de monitoreo de un switch

Parámetros	Descripción
Red	1. Disponibilidad del switch. 2. Disponibilidad de los puertos del switch. 3. Utilización de ancho de banda por puerto del conmutador

Nota. Fuente: Los autores.

2.2.12 Parámetros críticos de monitoreo de un enrutador

Los enrutadores o también conocidos routers se encargan del transporte del tráfico de información entre la red LAN y WAN. Por ello se deben monitorear los parámetros críticos de desempeño básicos mencionados anteriormente. Los siguientes parámetros, son propios de estos dispositivos**:**

Tabla 4: Parámetros críticos de monitoreo de un router

Parámetros	Descripción
Red	1. Disponibilidad del router. 2. Disponibilidad de los puertos del router. 3. Utilización de ancho de banda por puerto

Nota. Fuente: Los autores.

2.2.13 Rol de un sistema de monitoreo de una infraestructura TI

Según, Mendillo (2009) el apropiado uso de las herramientas de apoyo para la gestión de redes, incrementa la satisfacción de los usuarios finales, garantizándoles disfrutar de servicios con mayor disponibilidad disponibles independientemente de la complejidad, crecimiento o cambios que tenga la red. Por lo que, se concluye que un sistema de monitoreo es una herramienta de apoyo para la gestión de incidencias en los dispositivos críticos de la infraestructura TI. A través del correcto uso de ésta, los administradores de red mejoran su desempeño y aseguran por mayor tiempo la disponibilidad de los servicios de la

plataforma de TI, debido a que podrán visualizar con mayor precisión las causas de las fallas, lo que les permitirá brindar soluciones en menor tiempo. Por otro lado, los administradores de red también podrán delegar en un sistema de monitoreo las funciones de supervisión y notificación de fallas, con el fin de concentrar sus esfuerzos en realizar otras funciones de igual importancia para la infraestructura TI, ahorrando a la organización los costos de contratar personal adicional.

2.2.14 Beneficios de implementar un sistema de monitoreo para la infraestructura TI.

- Permite la planificación de las capacidades de los recursos, mediante el conocimiento del uso de los recursos de hardware, software y ancho de banda.
- El desempeño de la red puede ser optimizado a través del uso adecuado de los recursos de la infraestructura TI.
- La detección y solución de los problemas se torna más rápido abordando problemas específicos.
- El conocimiento del estado de la red les permitirá a los administradores planificar mantenimientos preventivos y correctivos a la infraestructura de TI, para prever indisponibilidades del servicio.
- El tiempo de los administradores es empleado en atender otros requerimientos.
- Con la información de las tendencias de consumos de los servicios permite conocer la tendencia del uso normal, ayudando a configurar la calidad de

servicio (QoS) que garanticen la cuota de recursos para los servicios prioritarios. En estas tendencias se pueden detectar problemas

2.2.15 Análisis de sistemas de monitoreo

Actualmente en el mercado existen diversas herramientas de monitoreo para la infraestructura de TI, que han sido implementadas como software. Estas aplicaciones básicamente son capaces de automatizar la captura, registro y entrega de información sobre la actividad de la red, además de notificar fallas por medio de diferentes mecanismos de alertas, que facilitan el análisis y la toma de decisiones al momento de aplicar eficientes soluciones en menor tiempo, y que permitan mejorar y mantener la calidad en la prestación de los servicios TI. Algunas de estas aplicaciones de monitoreo son propietarias y otras son Open Source (software libre), así como también pueden ser multiplataforma o capaces de incluir equipos de un solo fabricante.

Cada herramienta de monitoreo provee funciones específicas, por ello es importante conocer las características y limitaciones de las mismas a la hora de seleccionar una solución que apoye a la gestión de la infraestructura TI, tomando en cuenta que estas características deberán de satisfacer los requerimientos de la organización.

Para la selección de un sistema de monitoreo, se debe considerar, además del cumplimiento de las funcionalidades técnicas, la relación costo/beneficio, a través del estudio del ahorro por reducción del tiempo de fallas, disminución de

esfuerzos de monitoreo y mejoramiento de la calidad de los servicios, para llevar a cabo su adquisición, implementación y mantenimiento.

Por lo anterior, se consideraron definir las herramientas y sistemas de monitoreo de redes código abierto (Open Source Software) que fueron reconocidas y premiadas con el Bossie Awards: The Best Open Source Networking Software de los años 2013 y 2014, premio que es otorgado por los editores del grupo INFOWORLD Test Center (InfoWorld, 2014). El grupo INFOWORLD es una división de IDG (InfoWorldAbout, 2010), siendo ésta una consultora reconocida por su trayectoria en cuanto al asesoramiento, análisis, evaluación y publicación de los resultados obtenidos en estudios realizados a productos, soluciones y tecnologías de redes. (IDG, 2010). En referencia al premio, la consultora selecciona las herramientas y soluciones de código abierto basado en lo siguiente:

> Cada año, Bossies de InfoWorld (Best of Open Source Software awards) reconoce el mejor software de código abierto para los negocios. La misión central de INFOWORLD Test Center ha sido siempre identificar los productos más prometedores y rentables a disposición de las organizaciones de TI. (Bossie, 2014).

Basado en lo previo, las herramientas y software de redes de código libre ganadoras del Bossie Awards del año 2013 fueron: Pandora FMS, Nagios y Zabbix. Mientras que, en el año 2014, las ganadoras fueron, por segundo año consecutivo, Pandora FMS y Zabbix, las cuales a continuación se describirán sus características, ventajas y desventajas.

2.2.16 Pandora FMS

Pandora FMS es un software de monitorización para todo tipo de empresas, pero especialmente diseñado para grandes entornos, que le ayuda a detectar problemas antes de que ocurran mediante la gestión de servidores, comunicaciones y aplicaciones. Además, Pandora FMS cuenta con un sistema de informes configurable que evaluará el nivel de cumplimiento de sus sistemas y reportará la información a sus clientes (Pandora FMS, 2014).

Es una herramienta de código abierto que permite y proporciona las funcionalidades necesarias para realizar un monitoreo exhaustivo y análisis de nuestra infraestructura de red, mediante este sistema de monitoreo podemos gestionar diversos entornos, tales como, aplicaciones, servidores, plataformas virtualizadas y entornos web.

Otro tipo de detecciones que realiza pandora, son la carga del procesador, el uso de disco y memoria, procesos ejecutados en un sistema, eventos de log, temperatura, luz, humedad. Pandora FMS es una herramienta muy variable y modular, que nos permite trabajar de distintas formas y con la combinación de diferentes tipos de monitorización.

2.2.16.1 Características

Las principales características de Pandora FMS, son las siguientes:

- Autodescubrimiento y detección automática de la topología de red.
- Gestión de Eventos y fallos.

- Agentes multiplataforma para Windows, HP-UX, Solaris, BSD, AIX y Linux.
- Virtualización y cloud computing.
- Monitorización de disponibilidad y rendimiento.
- Consola visual personalizable.
- Agentes para android y dispositivos empotrados.
- Alta disponibilidad.
- Monitotización de red (SNMP, WMI, TCP, ICMP), IPv4 e IPv6.
- Niveles de control de acceso basados en roles.
- Monitorización de SNMP mediante polling y traps.
- Monitorización de servicios.
- Interfaz 100% web con niveles de acceso totalmente personalizables.
- Mapas topológicos de la monitorización personalizables.
- Conexión SSH/Telent a dispositivos desde el interfaz web.
- SLA y Elaboración de Informes, con ITIL v3 métricas.
- Monitorización de experiencia de usuario.
- Alta escalabilidad (monitorización delegada con múltiples instancias y gestión centralizada).

Este sistema de monitoreo dispone de un dashboard o también conocido como cuadro de mandos, por medio de esta interfaz gráfica se puede realizar configuraciones completamente personalizadas con diferentes pantallas y marcos.

Cada cuadro de mando contiene varias partes, como informes, gráficas, mapas, métricas, esto con la finalidad de ajustarlo de manera que sea claro para cada usuario.

Entre las tecnologías soportadas:

Sistemas Operativos: Linux, Windows, Solaris, AIX, HP-UX, BSD, MacOS

Aplicaciones: SAP, Tomcat, Weblogic, JBoss, IIS, Exchange, WebSphere, Apache

Comunicaciones: Cisco, Juniper, 3com, Teldat, Huawei, D-link, etc.

Bases de datos: Oracle, DB2, Microsoft SQL Server, MySQL, PostgreSQL

Protocolos soportados: SNMP v1, v2c, v3, HTTP, LDAP, ICMP, TCP, UDP, WMI, DNS

Virtualización: VMware vSphere, Xen VM, Amazon, EC2, RHEV

Sensores hardware: Temperatura, humedad, inundación, consumo eléctrico, luz, etc.

Experiencia de usuario: Latencias, comprobación contenido, login, proceso de compra.

2.2.16.2 Ventajas

- Misma herramienta para varios entornos

- Acceso al código fuente para personalizaciones
- Administración simple mediante interfaz web
- Escalabilidad extrema (miles de servidores y dispositivos)
- Rápida puesta en marcha
- Soporte internacional
- Gran comunidad de usuarios

2.2.16.3 Desventajas

- El tiempo de respuesta para la comunidad open source no es tan rápida

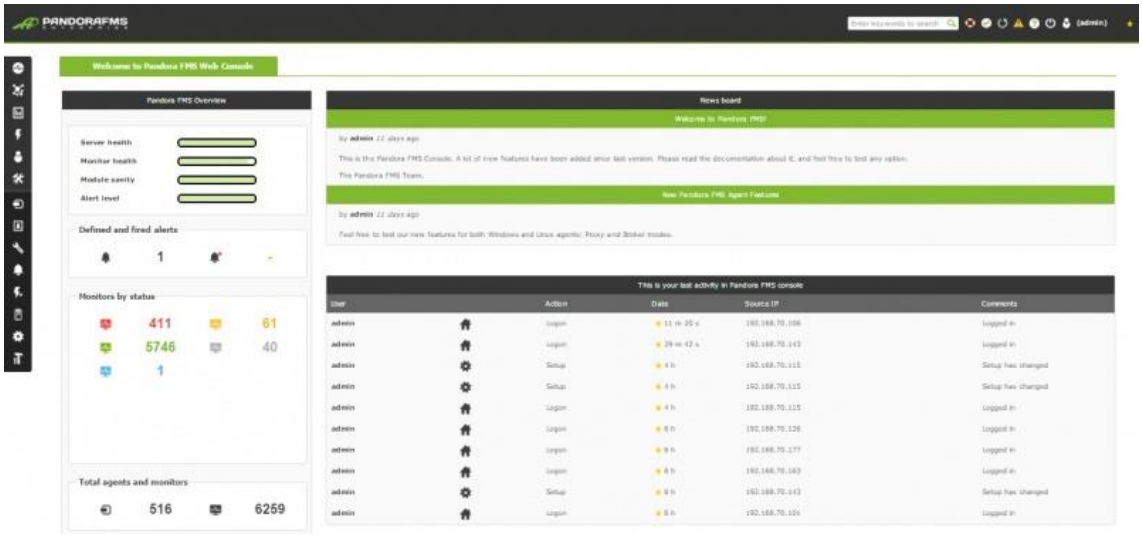


Figura 7. Interfaz de Pandora FMS

Fuente: http://wiki.pandorafms.com/images/thumb/b/bb/Pagipal.jpg/800px-Pagipal.jpg

2.2.17 Zabbix

Empresa Lituana trabajando en Zabbix desde el 2005. Fácil configuración y potente interfaz gráfico. Es un sistema de monitorización centralizado permite almacenar toda la información (datos de configuración y rendimiento), en bases de datos relacionales para facilitar el procesamiento y reutilización de datos. Zabbix ofrece la libertad sin lock-in y la seguridad a través de la disponibilidad del código fuente mediante componentes necesarios (Linux, Apache, MySQL/ PostgreSQL, PHP). (ZABBIX, 2014)

2.2.17.1 Características

- Chequeos simples que pueden verificar la disponibilidad y el nivel de respuesta de servicios estándar como SMTP o HTTP sin necesidad de instalar ningún software sobre el host monitorizado.
- Un agente Zabbix puede también ser instalado sobre máquinas UNIX y Windows para monitorizar estadísticas como carga de CPU, utilización de red, espacio en disco, etc.
- Como alternativa a instalar el agente sobre los hosts, Zabbix incluye soporte para monitorizar vía protocolos SNMP, TCP y ICMP, como también sobre IPMI, JMX, SSH, telnet y usando parámetros de configuración personalizados. Zabbix soporta una variedad de mecanismos de notificación en tiempo real, incluyendo XMPP

2.2.17.2 Ventajas

- Su comunidad es bastante activa.

- Es potente a bajo nivel.

2.2.17.3 Desventajas

- Aunque se ha utilizado en grandes instalaciones, a partir de 1000 nodos puede disminuir su rendimiento.
- Difícil crear y definir plantillas de informes y alertas. Las configuraciones pueden requerir muchos clics y pasos para completarlas.
- No posee informes en tiempo real.
- Es difícil de depurar cuando hay errores.
- Pobre tratamiento de traps.

Nuestra sensación es que muchos usuarios de Nagios se están moviendo a Zabbix por que ha recogido el guante de Nagios y empieza a tener la visibilidad que tenía antes Nagios. (Zabbix 2014)

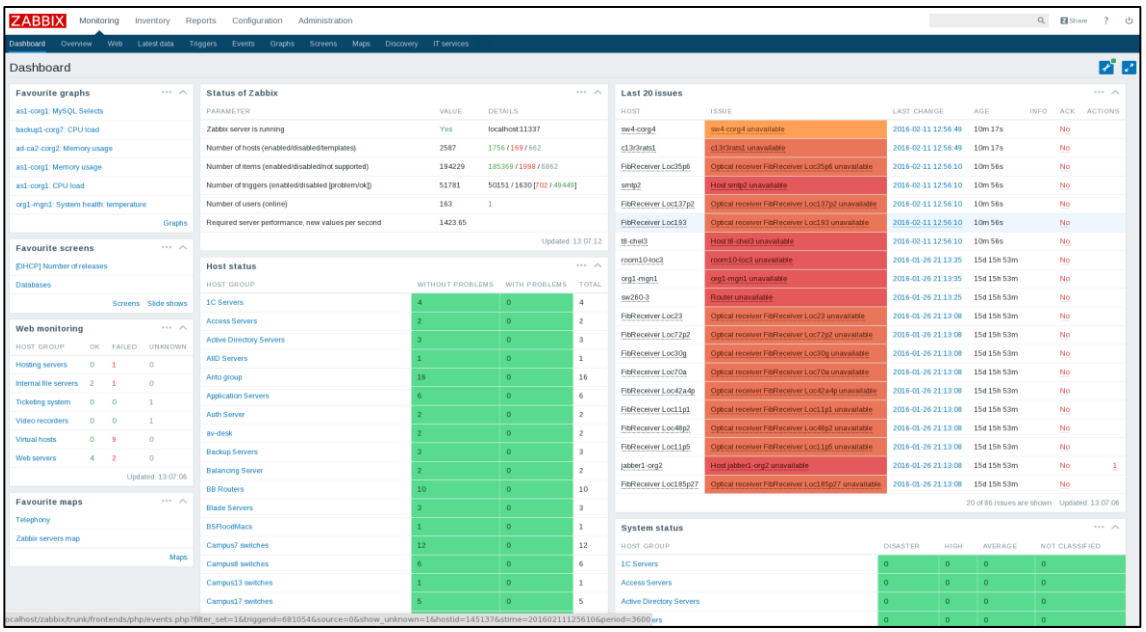


Figura 8. Interfaz de Zabbix
Fuente: http://www.zabbix.com/img/3.0/whatsnew/zabbix-whats-new-3.0-dashboard.png

2.3. Definición De Terminos Basicos

2.3.1. Monitoreo

El monitoreo no es una tarea exclusiva de la tecnología de información. Otras áreas como la medicina y el sector automotriz, supervisan el estado de sus componentes críticos. Los médicos utilizan monitores de signos vitales, tal como es el caso del electrocardiograma que mide, registra, alerta y grafica la actividad eléctrica del corazón. Mientras que los vehículos y maquinarias industriales, poseen mecanismos de medición de los parámetros críticos (temperatura, presión de aceite, entre otros) y tienen la capacidad de alertar anomalías con el fin de preservar la vida útil de estos.

2.3.2 Infraestructura TI

Se define este término a través de su interpretación etimológica, ya que aún no hay interpretación validada por parte de un autor.

Según el Diccionario de la Real Academia Española, se define Infraestructura como: “conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una organización cualquiera.” Mientras que, tecnología, se define en la misma fuente, como: “conjunto de los conocimientos, instrumentos y métodos técnicos empleados en un sector profesional: tecnología de la información”. Esta definición es amplia y sujeta a interpretación, según la práctica y dependiendo en gran medida del contexto en el que se utiliza el término.

Otra fuente de referencia para este concepto, pero no tan públicamente disponible, es el glosario de términos de ITIL (2007), que se incluye en el marco referencial Librería de la Infraestructura de Tecnología de Información (ITIL), por sus siglas en inglés (Information Technology Infrastructure Library). Este glosario define que la infraestructura de TI es:

> Todo el hardware, software, redes, instalaciones etcétera que son requeridas para desarrollar, probar, proveer, monitorear, controlar o soportar los servicios de TI. El termino Infraestructura de TI incluye todas las tecnologías de la información, pero no lo asociado a las personas, procesos y documentación. (Pág. 26).

Sin embargo, Weill y Broadbent (1998) definen una estructura de componentes que incluye al personal de TI como parte de los elementos que conforman la infraestructura tecnológica de información; de manera contraria a lo expresado en ITIL.

De acuerdo a lo anteriormente mencionado, y a pesar de las contradicciones, es posible afirmar que la infraestructura tecnológica de información es el conjunto de herramientas o dispositivos tecnológicos que soportan servicios, los cuales mantienen la operatividad de los procesos de la organización.

La importancia de este concepto para la presente investigación, es poder establecer y delimitar los elementos que se tomaran en cuenta para el desarrollo de la propuesta de monitoreo de infraestructura tecnológica, de una manera formal.

2.3.3 Servicios TI

En glosario de términos de ITIL (2007), servicio (service) se define como "una manera de ofrecer valor a los clientes, facilitándoles a estos el cumplimiento de los resultados sin ser responsables de los costos y riesgos específicos". (Pág. 42).

Igualmente, en el glosario de términos de ITIL (2007), se conceptualiza servicio de TI (IT Service) como:

> El uso de tecnologías de la información y apoyo a los procesos de negocio del cliente. Un servicio de TI se compone de una combinación de personas, procesos y tecnología, y podrían definirse en un Acuerdo de Nivel de Servicio (SLA, Service Level Agreement). (Pag. 26).

Los acuerdos de niveles de servicios o también conocido por las siglas SLA en inglés (Service Level Agreement) son definidos en el glosario de (Rance y Hanna, 2007) como:

> Un acuerdo entre un proveedor de servicios de TI y un cliente. En el SLA se describen los servicios de TI, con los objetivos a nivel de servicio, y se especifican las responsabilidades del proveedor de servicios de TI y el cliente. Un único SLA puede cubrir múltiples servicios de TI o varios clientes. (Pag. 44).

Partiendo de la definición establecida por ITIL, se tiene que el SLA especifica detalladamente en un documento los aspectos de los servicios TI ofrecidos por el proveedor a un cliente. Estos acuerdos de servicio desempeñan un papel

importante para mantener la calidad de los servicios de TI, ya que en estos se establecen las responsabilidades y/o penalizaciones de cada uno de los involucrados. En los SLA se describen previamente aspectos que definen la prestación de servicios, tiempo de atención, calidad, disponibilidad y recuperación de los mismos. El incumplimiento de los SLA por parte del proveedor, pueden generarles multas, debido a que las fallas de los servicios pueden afectar el prestigio y confianza de los clientes, lo que se traduce en perdida de dinero. Para verificar el cumplimiento de los SLA y la calidad de los servicios, es imprescindible realizar tareas de monitoreo constantemente.

Para gestionar estos servicios, en el glosario de términos de ITIL (2007), la gestión de servicios TI (IT service management) está definida como:

> Implantación y gestión de servicios de TI de calidad que cumplan con las necesidades de la organización. La gestión de los servicios de TI es llevada a cabo por los proveedores de servicios de TI a través de la combinación apropiada de personas, procesos y tecnologías de la información. (Pag. 27).

Los procesos de la organización dependen en gran medida de la gestión de la infraestructura tecnológica, y el desempeño de esta en la misma forma depende de la estabilidad y disponibilidad de la prestación de servicios tecnológicos, de aquí la importancia de monitorear tanto los recursos de la red como los dispositivos por los cuales transportan y procesan los servicios que se prestan a los clientes.

La importancia que tienen los servicios tecnológicos para el negocio, se basa en que estos, como su definición lo indica, apoyan los procesos de la organización y permiten a los usuarios el logro de sus funciones y operaciones, para alcanzar los objetivos de la organización.

2.3.4 Dispositivos TI

Según Laudon y Laudon (2000) conceptualizan que "Técnicamente, podemos definir un sistema de información como un conjunto de elementos interconectadas que capturan, (o recuperan), procesan, almacenan y transmiten información en orden para apoyar la toma de decisiones y control de procesos en la organización " (Pag.8). En tal sentido, se puede considerar de manera general que las funciones esenciales en estos sistemas son el transporte, procesamiento y almacenamiento de los datos. Dentro de los componentes de infraestructura de TI, las funciones de procesamiento y almacenamiento son soportadas por los servidores, mientras que el transporte de los datos se realiza a través de los dispositivos y enlaces de red. En analogía a la definición de sistema de información con las funciones esenciales del mismo, se hace evidente que los servidores y dispositivos de red que intervienen en un servicio, tienen una importancia fundamental para el funcionamiento de dicho servicio.

Para gestionar estas redes y dispositivos, según Mendillo (2009):

> Se trata de una amplia gama de actividades de índole técnica, administrativa y gerencial que se puede resumir en coordinar recursos para: planificar, organizar, diseñar, operar, contabilizar, controlar, analizar, evaluar y expandir las redes de comunicaciones con el objetivo de lograr

> niveles de servicio óptimos, a un costo razonable y con la máxima eficiencia en el uso de la red y sus recursos (Pág. 11).

A través de la gestión de redes y dispositivos de las organizaciones podrán controlar los recursos estratégicos, controlar la complejidad del diseño de la red, ofrecer mejor prestación de servicios a los usuarios, reducción de fallas, congestión y tiempos de caídas del servicio y controlar los costos de los recursos que se consumen en la red.

Por otra parte, Mendillo (2009) describe que la gestión de redes en un principio se enfocaba en administrar los dispositivos de red (switch, router, firewall, enlaces de conexión WAN entre otros), luego evoluciono para abarcar la gestión de la red completa, sin embargo, hoy en día el enfoque está dirigido a la gestión de servicios que toma en cuenta la tecnología y el mantenimiento de los equipos que operan en la red, derivándose en la gestión de dispositivos y la gestión de la red.

El enfoque mencionado anteriormente proporciona una guía inicial. Sin embargo, en el marco metodológico se propone un método para la implementación de un sistema de monitoreo, que, entre otros aspectos, permita definir la criticidad de los dispositivos TI de una manera más precisa, ajustado al contexto de una determinada organización.

2.3.5 Monitoreo de TI

En la infraestructura TI de las organizaciones, se necesita emplear herramientas automatizadas para supervisar el uso de sus recursos y componentes críticos tecnológicos de información. Con el propósito de detectar problemas o situaciones

anómalas. La diversidad de recursos, el número de usuarios y la demanda de estos, aumentan la vulnerabilidad de la infraestructura tecnológica, por lo que es necesario implantar herramientas automatizadas de apoyo a la gestión de monitoreo.

Estas herramientas generalmente están conformadas por aplicaciones informáticas y bases de datos, capturan el comportamiento de los dispositivos y recursos de la infraestructura TI y determinan la utilización y otros indicadores críticos de desempeño. La información obtenida de la red, se podrá presentar en estadísticas y representaciones graficas que facilitaran el análisis de los eventos.

El termino monitoreo no está definido por la Real Academia Española, sin embargo, es utilizado para describir todo proceso de supervisión y observación. Por su parte (Rance y Hanna, 2007) define monitoreo (monitoring) como "la observación repetida de un elemento de configuración, servicio o proceso para detectar eventos y asegurarse de que se conoce el estado actual" (Pág. 31).

(Rance y Hanna, 2007) en el glosario de términos ha definido cuatro tipos de monitoreo, los cuales forman parten de los objetivos de mantenimiento del servicio. A continuación, se describen las definiciones de ITIL:

- Monitoreo activo (Active Monitoring), es "el monitoreo de un elemento de configuración o de un servicio TI que utiliza de forma regular revisiones automatizadas para descubrir el estado actual" (pág. 2).

- Monitoreo pasivo (passive monitoring). “el monitoreo de un elemento de configuración, un servicio TI o un proceso que depende de una alerta o notificación para la identificación de su estado” (pág. 34).
- Monitoreo proactivo (proactive monitoring), es “el monitoreo que trata de encontrar patrones, a partir de eventos, para predecir posibles futuros fallos” (pág. 35).
- Monitoreo reactivo (reactive monitoring), es “accionado en función a una respuesta de un evento”.

3. Hipótesis

El sistema de monitoreo de infraestructura TI influye de manera positiva en la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca.

3.1. Operacionalización de Variables

Las variables de investigación son:

Variables Independientes

Sistema de monitoreo de Infraestructura TI

Variables Dependientes

Gestión de incidencias.

Tabla 5: Operacionalización de Variables

VARIABLE	DEFINICIÓN	INDICADOR(ES)	ÍTEM	INSTRUMENTO
Independiente: Sistema de monitoreo de Infraestructura TI	Una gestión de eventos efectiva depende del conocimiento del estado de la infraestructura de TI a través de la detección oportuna de cualquier desviación de la operación normal o esperada, para lo cual existen en el mercado sistemas de control y monitoreo. (ITIL, 2013)	Tiempo empleado en la respuesta de incidencias Exactitud al encontrar el fallo Nivel de satisfacción del cliente.	¿Hay algun dispositivo o servicio que necesita atención? ¿Cuándo se tarde en encontrar el fallo?	Reportes del servidor de monitoreo / Encuestas/ Gráficas
Dependiente: Gestión de incidencias	Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo (ITIL, 2011)	Índice de Producción Confiabilidad del sistema. Índice de quejas. Nivel de aceptación por parte del usuario final.	¿Confía en la eficiencia en la gestión de incidencias del sistema de monitoreo? ¿En qué porcentaje han disminuido las quejas por parte de los clientes de la red LAN?	Entrevistas a personal de sistemas / encuestas

Nota. Fuente: Los autores.

CAPITULO III

METODOLOGÍA

Este capítulo está orientado a ofrecer detalles sobre la metodología empleada para determinar la influencia de la implementación de un sistema de monitoreo de infraestructura TI para gestionar las incidencias en la red LAN del Hospital Regional de Cajamarca.

- Se determinó que el enfoque de la presente investigación fue CUANTITATIVO porque (Sampieri, 2007) establece que se utiliza secundariamente la recolección de datos fundamentada en la medición, posteriormente se lleva a cabo el análisis de los datos y se contestan las preguntas de investigación, de esta manera probamos las hipótesis establecidas previamente, confiando en la medición numérica, el conteo, y en el uso de la estadística para intentar establecer con exactitud patrones en una población.
- Se determinó que el tipo de investigación fue APLICADA de acuerdo con Murillo (2008) la investigación aplicada recibe el nombre de "investigación práctica o empírica", que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación.
- Se determinó que el diseño de la investigación fue NO EXPERIMENTAL la que es también conocida como investigación Ex Post Facto, término que proviene del latín y significa después de ocurridos los hechos. De acuerdo con Kerlinger (1983) la investigación Ex Post Facto es un tipo de "... investigación sistemática en la que el investigador no tiene control sobre

las variables independientes porque ya ocurrieron los hechos o porque son intrínsecamente manipulables," (p.269).

- Se determinó que la dimensión temporal de la investigación fue TRANSECCIONAL de acuerdo con Hernández, Fernández y Baptista (2003) en la investigación transeccional se recolectan datos en un solo momento, su propósito es descubrir variables y analizar su incidencia e interrelación en el momento dado.

4.1.Unidad de análisis, universo y muestra

4.1.1 Unidad de análisis

La unidad de análisis estuvo conformada por los trabajadores del área de Estadística e Informática y personal del Hospital Regional de Cajamarca que utilizan a diario la infraestructura TI.

4.1.2 Universo

El universo estuvo conformado por la totalidad de las personas que integran el área de estadística e informática y trabajadores de las diferentes áreas del Hospital Regional de Cajamarca, los cuales interactuaron con las incidencias de la infraestructura TI.

4.1.3 Muestra

Se utilizó un muestreo de tipo NO PROBABILISTICO – INTENCIONAL ya que se realizó considerando el conocimiento y los criterios de quien efectuó la investigación.

Los criterios de inclusión y exclusión considerados para la delimitación poblacional son los siguientes:

- Trabajadores con experiencia mayor a 3 años.

Considerando estos criterios se tiene:

Tabla 6: Muestra del proyecto de investigación

Nombre y Apellidos	**Cargo**	**Tiempo de Servicio**
Manuel Cruz Malca	Jefe del área	3 años
Susana Tantalean Odar	Análista de Base de Datos	5 años
Larissa Ruiz.	Análista de Base de Servidores	5 años
Carlos Hoyos Chaves	Encargado del Sub-área de Telecomunicaciones	4 años
Christian Abanto Segura	Programador	4 años
Miguel Coba Uriarte.	Soporte Técnico	4 años
Personal del HRC	Diferentes áreas y cargos.	> a 3 años.

Nota. Fuente: Elaborado por los autores.

- Muestra: se considera a todo el universo como muestra (6 trabajadores y a 80 trabajadores a los que se les presentaron las incidencias) para la evaluación de variables, por ser un número reducido y por tener acceso a los trabajadores que componen dicho universo.

4.1.4 Técnicas e instrumentos de recolección de datos

Para el trabajo de recolección de información se utilizaron las siguientes técnicas:

ENTREVISTAS

Esta técnica fue utilizada para poder conseguir la información necesaria para determinar los casos comunes de incidentes en la infraestructura de TI y cuál fue el tiempo en que se solucionaban. Para establecer soluciones oportunas en menor tiempo con una base de incidentes ya definida.

ENCUESTAS

Estuvo enfocada a las personas que conforman la muestra, quienes están diariamente atendiendo las incidencias y a los trabajadores que se les presenta los incidentes.

LA OBSERVACIÓN

Se realizó la utilización de esta técnica con el fin de verificar la interacción de las personas encargadas de la administración de la red con el aplicativo y si se adaptan a las interfaces del mismo con el fin de que sea amigable y puedan hacer uso de el sin ningún inconveniente.

Para la presente investigación se utilizaron los siguientes instrumentos:

CUESTIONARIO ESTRUCTURADO

Se elaboró un cuestionario para las personas o responsables técnicos encargados de la administración de la red, para determinar las expectativas del aplicativo y que este ajustado a sus necesidades.

Elaboramos cuestionarios estructurados para recolectar datos sobre: Tiempo de respuesta, exactitud al encontrar el fallo, nivel de satisfacción del cliente y confiabilidad. Todos estos cuestionarios referentes al mecanismo de atención de incidencias.

GUIA DE OBSERVACIÓN ESTRUCTURADA

Este tipo de instrumento nos sirvió para evaluar nuestra técnica de observación.

Utilizamos la guía de observación estructurada para identificar los posibles cambios y/o atajos que tuvimos que añadir para que el sistema de monitoreo sea amigable y entendible para el encargado de TI.

CHECKLIST

Utilizamos esta herramienta para verificar el resultado de nuestro aplicativo, comprobando que esté acorde a los objetivos y alcances planteados inicialmente.

INTERNET

Fue una herramienta principal para nuestra investigación al momento de despejar ciertas dudas, con sitios confiables, nos permitió aclarar muchas interrogantes con respecto a la configuración e implementación de ciertas aplicaciones utilizadas en nuestra tesis de grado.

4.1.5 Técnicas para el procesamiento y análisis de datos

Las técnicas de análisis de datos consistieron en la realización de las operaciones en las que el investigador sometió los datos, con la final de alcanzar los objetivos del estudio.

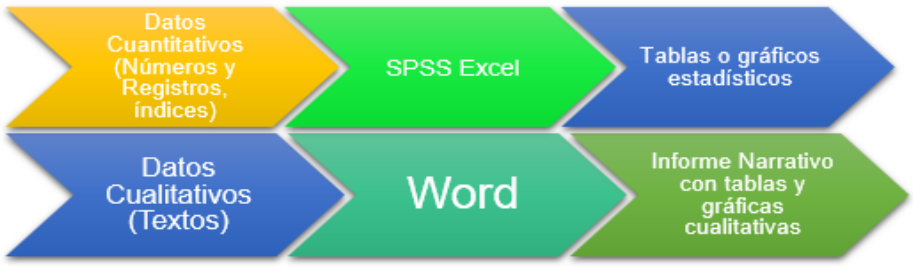


Figura 9. Proceso de organización y análisis de datos en función de los datos
Fuente: Aristides Vara

Procesamiento para organizar datos cualitativos (entrevistas)

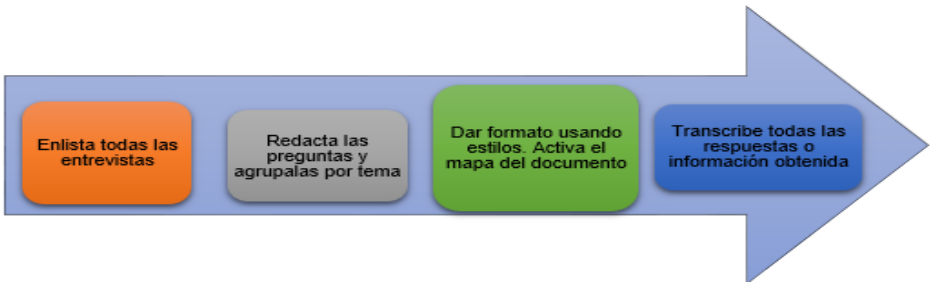


Figura 10. Pasos para crear el organizador cualitativo
Fuente: Aristides Vara

En el caso de las entrevistas se procesaron mediante técnicas de análisis cualitativo empleadas para resumir analizar e interpretar la información obtenida. En este caso se utilizó las técnicas de análisis de contenido. Mediante tablas de origen en donde se agruparon las entrevistas en tablas de doble entrada. En estas tablas, cada columna fue un entrevistado y cada fila una pregunta o categoría de interés. Hecha la tabla, se transcribió la información tal cual había sido obtenida, distribuyéndola por cada categoría y entrevistado. Se llama tabla se origen porque los datos son ingresados tal cual, sin modificaciones ni resúmenes. Adicionalmente se utilizaron las tablas de resumen codificadas, ya que, estas se enfocan en las palabras e información clave y eliminan todo lo que sea innecesario de las tablas origen. En estas tablas, se usaron viñetas para organizar las ideas, mediante códigos que faciliten y uniformicen el lenguaje entre los entrevistados. Seguido se analizó el contenido de las tablas en función de los patrones de semejanza/desemejanza, coherencia y fiabilidad y por último se elaboraron los gráficos o mapas conceptuales o esquemas explicativos para resumir o presentar los resultados del análisis de contenido de las tablas que se emplearán.

Procesamiento para organizar datos cuantitativos (encuestas y cuestionarios estructurados)

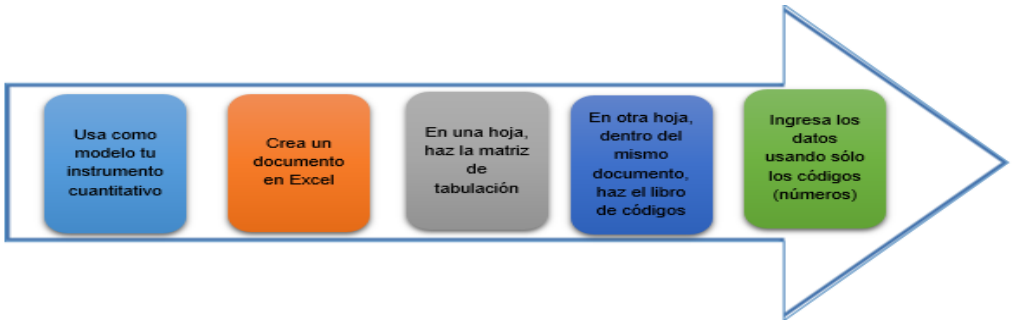


Figura 11. Pasos para crear una matriz de tabulación para analizar datos cuantitativos.
Fuente: Aristides Vara

En el caso de las encuestas utilizamos las técnicas de análisis cuantitativo las cuales sirven para describir, graficar, analizar, comparar, relacionar y resumir los datos obtenidos con los instrumentos cuantitativos, en este caso se realizó diversas técnicas de estadística descriptiva, tales como tablas de frecuencia e histogramas. Sin importar la técnica o técnicas escogidas hay una secuencia básica que se tiene que seguir para analizar nuestros datos estadísticos.

Procedimiento para el análisis cuantitativo de datos

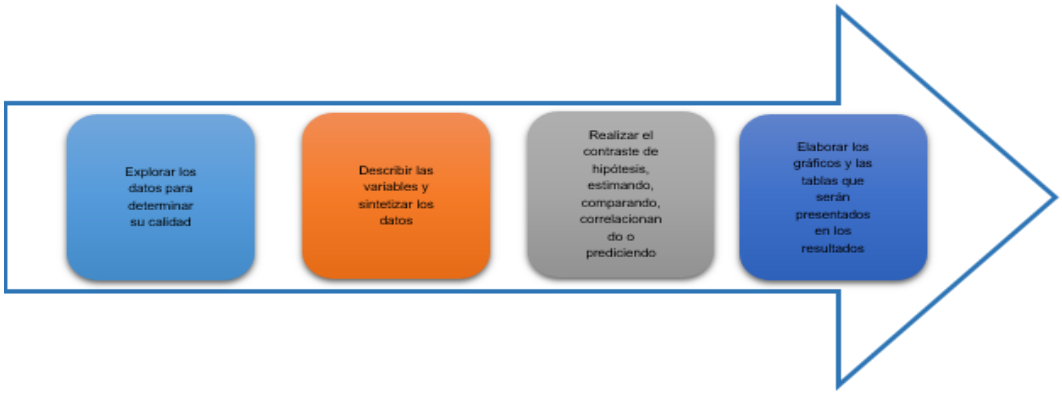


Figura 12. Procedimiento para el análisis cuantitativo de datos.
Fuente: Aristides Vara

4.1.6 Contrastación de Hipótesis.

Para contrastar la hipótesis involucró la realización de los siguientes pasos:

1. Se presentó una solicitud para el acceso y manipulación de las herramientas que necesitamos para la investigación (acceso a la infraestructura TI)
2. Se visitó el área de telecomunicaciones del Hospital Regional de Cajamarca.
3. Se seleccionó el hardware donde se realizaron las pruebas e implementación del sistema de monitoreo de infraestructura TI
4. Se aplicaron efectivamente las encuestas, cuestionarios estructurados y entrevistas para la recolección de datos.

5. Se identificó el problema y objetivos mencionados en la presente investigación con la participación del encargado de TI del Hospital Regional de Cajamarca – Ing. Carlos Hoyos Chavez.

6. Se recurrió a las teorías que sustentan la investigación y revisión de los estudios realizados para tener como base las recomendaciones.

7. Se implementó y probó dos de los más representativos sistemas de monitoreo del mercado sobre plataformas virtuales para elegir el que mejor se adecúe a los objetivos del Hospital Regional de Cajamarca – Se probaron los sistemas de monitoreo ZABBIX y PANDORA FMS.

8. Se implementó el sistema de monitoreo de infraestructura TI, que mejor estuvo alineado a los objetivos del Hospital Regional de Cajamarca, siendo Pandora FMS, el elegido. Sobre el hardware establecido anteriormente.

9. Se instalaron los agentes en los dispositivos y servicios de la infraestructura TI.

10. Se establecieron los parámetros críticos a ser medidos en la infraestructura TI, de acuerdo a los objetivos del Hospital Regional de Cajamarca

11. Se generaron las alertas de acuerdo a los parámetros críticos establecidos para gestionar las incidencias por parte del encargado de TI del Hospital Regional de Cajamarca – Ing. Carlos Hoyos Chavez.

12. Se probó el sistema de monitoreo de infraestructura TI durante el periodo estipulado en el cronograma con el fin de corregir cualquier error o falla.

13. Después de haber cumplido la parte de la implementación y fase de prueba, se procedió con la fase de CHECK y ACT del modelo PDCA, además mediante encuestas, cuestionarios estructurados y entrevistas realizamos los indicadores de medición de nuestras variables identificadas en nuestra matriz de operacionalización, elaborando así, tablas para mostrar los resultados de los datos obtenidos.

14. Se recurrió a los procedimientos de análisis e interpretación de datos siguiendo los pasos establecidos en la metodología del proyecto, en el punto 4.1.5 Técnicas para el procesamiento y análisis de datos, pág. 82; con el objetivo de elaborar los resultados concernientes de la presente tesis de grado, Capítulo 6: Resultados y discusión pág. 146, los cuales, determinaron la influencia de la implementación de un sistema de

monitoreo de infraestructura TI sobre la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca.

15. Se formularon las conclusiones y recomendaciones.
16. Se elaboró el trabajo final y presentación a las autoridades universitarias.

4.2 Metodología PDCA

La metodología utilizada está basada en el ciclo de mejora continua de la calidad de los procesos de la organización de Shewhart PDCA o círculo de Deming, específicamente enfocada en el rediseño de los procesos de monitoreo de los recursos críticos de TI. PDCA está compuesta por cuatro fases, en donde cada sigla en inglés hace referencia a una etapa de la siguiente forma: Plan (P), Do (D), Check (C) y Act (A), cuya traducción significa planificar, hacer, verificar y actuar, respectivamente, las cuales se observan en la figura 9 según ITIL (2015) los detalles de cada etapa en el círculo de Deming.

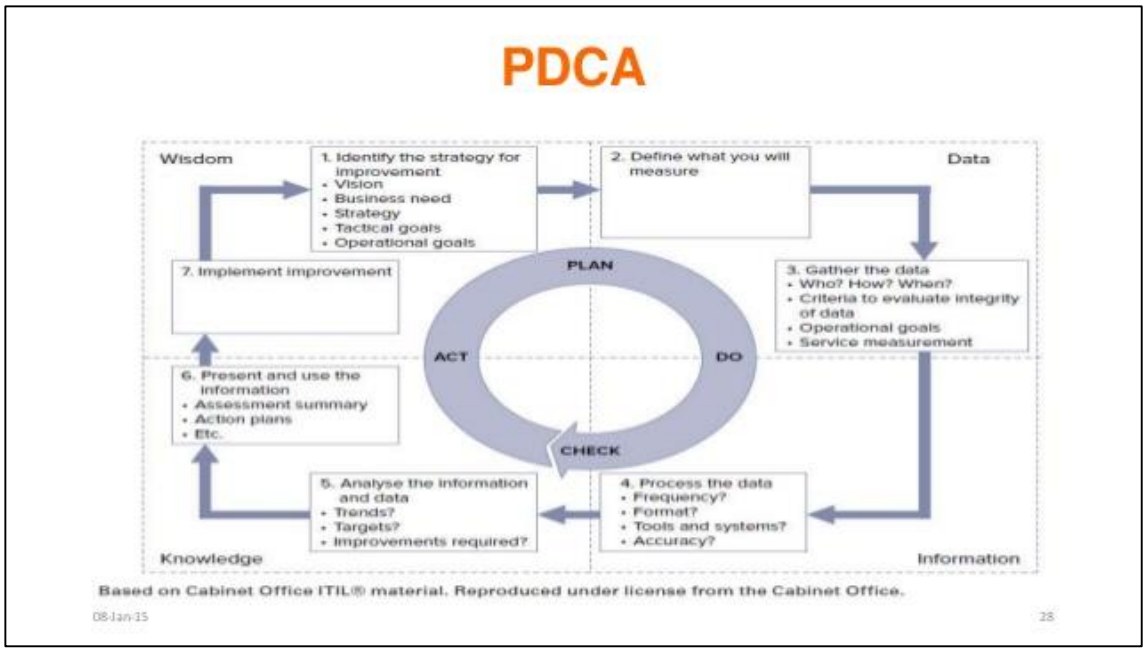


Figura 13. Ciclo de Deming
Fuente: ITIL® v3 (2015). *Mejora Continua del Servicio.* Cap.07.4. Itil - Information

Aunque el circulo de Deming o ciclo de Shewhart es una teoría empleada para mejorar la calidad de los procesos y servicios de forma general, en esta tesis de grado, se emplea como una guía para analizar, implementar, verificar y optimizar la calidad del proceso de monitoreo de la infraestructura TI del Hospital Regional de Cajamarca. Con el fin de mantener vigente el mecanismo de monitoreo, y éste sea consistente con los objetivos del Hospital, considerando que los servicios de tecnología apoyan operativamente al negocio.

El ciclo de monitoreo del presente proyecto, tiene como objetivo oriental al administrador de redes, en la realización de un proceso de monitoreo ordenado y constante, procurando el uso correcto de los recursos de red a disposición.

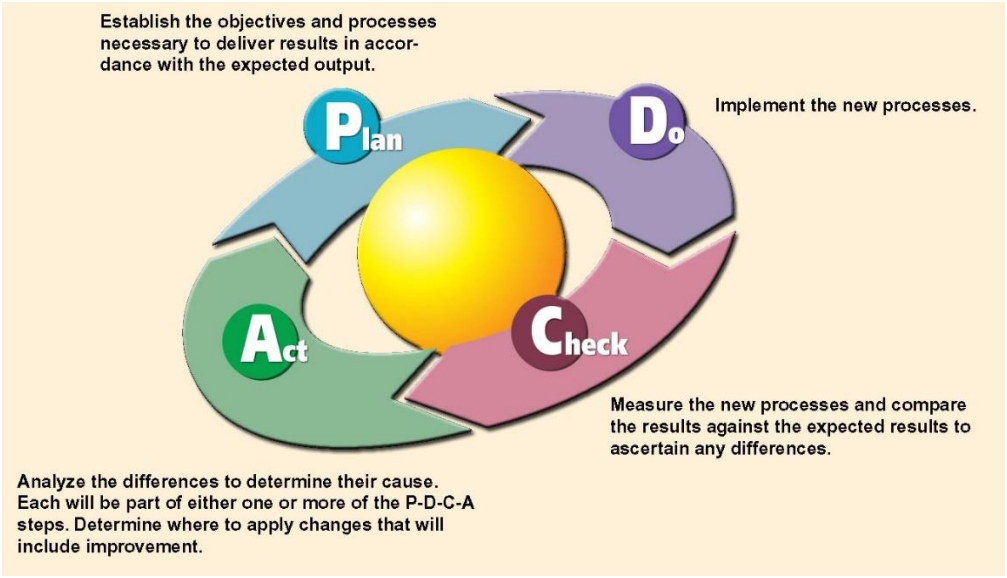


Figura 14. Ciclo de Deming
Fuente: ITIL (2008). *Importance of maturity models for implementing best practices.* Itil – Information

Figura 15. Representación gráfica de acuerdo a nuestro Proyecto
Fuente: Los autores.

A continuación, se describen brevemente las fases del modelo propuesto:

4.2.1 Fase Análisis

Esta etapa corresponde a la fase de Planing (P) del círculo de Deming. Esta fase describe el proceso que estudia los objetivos de la organización, la importancia y nivel de criticidad con los servicios de tecnología que hacen posible el cumplimiento de dichos objetivos. Estos servicios son descompuestos en lo siguientes componentes (dispositivos y servicios TI) que los integran. En esta fase se aplican las encuestas a detalle para recolectar datos sobre el estado actual de mecanismo de monitoreo de la infraestructura TI, seguidamente se tabulan los datos obtenidos y se generan gráficos entendibles a nivel usuario.

4.2.2 Fase de Implementación

Esta etapa corresponde a la fase DO (D) del círculo de Deming, y consta de implementar un sistema de monitoreo sobre la infraestructura TI (dispositivos y servicios) de acuerdo a los objetivos, la importancia y el nivel de criticidad en la

organización, determinada en la fase anterior. Seguidamente se instalan los agentes de acuerdo a los requisitos del Hospital y se generan las alertas correspondientes.

4.2.3 Fase de Verificación

Esta etapa se relaciona con la fase de Check del círculo de Deming. En esta etapa se comprueba que la implementación fue efectiva, de acuerdo a las expectativas establecidas en la fase de análisis. Se documenta toda desviación detectada, de modo de poder ser tratada en la fase de optimización o diferida a la próxima iteración del ciclo.

4.2.4 Fase de Optimización

Esta etapa corresponde a la fase Act (A) del círculo de Deming. En esta etapa, aquellas desviaciones que fueron detectadas en la fase anterior, serán analizadas y manejadas de la siguiente manera:

Se determinan los costos implícitos para corregir la deficiencia

En base a los costos determinados se puede tomar las siguientes acciones:

- Aceptación: Los costos de corrección son muy altos para el presupuesto disponible por lo tanto esta deficiencia será remitida a la próxima iteración del ciclo, de modo de ser considerada en la fase de análisis.
- Transferencia: en caso de existir recursos que permitan corregir la deficiencia a través de la contratación de un tercero al Hospital, puede considerarse esta acción.

- Evasión: no se lleva a cabo la tarea o implementación que genero la deficiencia. Todo adelanto en la implementación es reversado y documentado.

La ejecución de las cuatro etapas mencionadas se realiza con el objetivo de incorporar mejoras y actualizaciones al mecanismo de monitoreo del Hospital Regional de Cajamarca, manteniéndolo vigente y óptimo en el tiempo, y con esto alcanzar calidad en la entrega de toda la infraestructura TI.

4.3 Explicación detallada de la fase de análisis

En esta sección se describen y desarrollan en detalle los pasos de la fase de análisis.

Se conoce que, la infraestructura tecnológica de la información (TI) se encuentra expuesta a constantes cambios que, por lo general, son suscitados por la demanda de nuevos y/o más sofisticados componentes tecnológicos. Estos cambios están relacionados a las actualizaciones realizadas a la plataforma tecnológica, las cuales derivan en muchos casos en actividades tales como: incorporación, modificación, sustitución o desincorporación de sus componentes. Muchos de estos componentes deben ser monitoreados, sobre todo aquellos que soportan la operatividad de los servicios de TI que apoyan los procesos de gestión en el hospital.

Por lo anterior, es importante realizar periódicamente el análisis de los componentes tecnológicos que integran la infraestructura TI, mediante el cual se identifican, definen y planifican mejoras al proceso de monitoreo.

A continuación, se enumeran cada uno de los pasos que se llevan a cabo en la fase de análisis del modelo propuesto:

- Identificar los objetivos en el Hospital Regional de Cajamarca
    - Identificar los servicios críticos de TI.
    - Identificar los dispositivos críticos de TI.
    - Correlacionar los objetivos de la organización con los servicios críticos TI.
    - Identificar el mecanismo actual de monitoreo de la infraestructura TI.

Los pasos anteriores son definidos y detallados en forma general.

4.4 Identificar los objetivos del Hospital Regional de Cajamarca

En este paso, los objetivos de la organización son discutidos y verificados con el personal del área de estadista e informática, mediante un proceso de levantamiento de información que asegura que se tomen en cuenta las áreas que proporcionan productividad y competitividad al Hospital. También es importante tener en cuenta los objetivos del área de telecomunicaciones, el cual tiene como propósito proveer servicios altamente disponibles y eficientes a los usuarios, y principalmente al Hospital. Dado lo anterior, el área de telecomunicaciones a modo general es responsable de:

4.5 Identificar los servicios críticos de TI

La definición e importancia de los dispositivos y servicios TI fue mencionada en el marco teórico del presente proyecto, en donde se estableció que los mismos

hacen uso de la tecnología de información y soportan a los procesos de la organización permitiendo a los usuarios el logro de sus funciones y operaciones, para alcanzar los objetivos del Hospital Regional de Cajamarca. Estos servicios están compuestos por procesos y tecnología (dispositivos hardware, software u otros servicios).

Los servicios críticos de TI para efectos del presente proyecto se clasifican en dos niveles. En donde el primer nivel, se refiere a los servicios básicos comunes de TI, los cuales son la base operativa de comunicación, acceso y conectividad de la organización. Y el segundo nivel, se refiere a los servicios críticos de TI dedicados directamente al soporte de los procesos de la organización. Es importante destacar que muchos de los servicios del segundo nivel dependen operativamente del correcto funcionamiento y disponibilidad de los servicios del primer nivel.

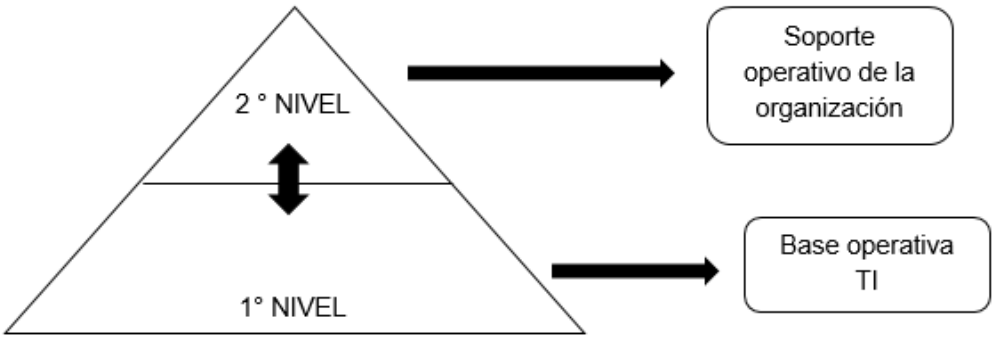


Figura 16. Niveles de servicios críticos
Fuente: Los autores

Como ejemplos de algunos servicios críticos básicos comunes de TI se observan en la siguiente tabla:

Tabla 7: Algunos servicios críticos comunes de TI

SERVICIO	DESCRIPCIÓN
Impresión	Provee a los usuarios capacidad para imprimir documentos.
Intranet	Les permiten a los usuarios acceder a la página Web interna de la organización
Correo electrónico	Les permiten a los usuarios hacer uso del correo electrónico para comunicarse con otros usuarios
DHCP	Les permiten a las estaciones de trabajo de los usuarios obtener una dirección IP (Internet Protocol) para conectarse a la infraestructura de red de la organización.
Dominio	Provee identificación a las estaciones de trabajo, servidores y demás dispositivos tecnológicos, para ser accedidos por medio de este.
Monitoreo	Suministra monitoreo de la actividad de la infraestructura tecnológica. Capturando el tráfico de la red, lo que puede identificar el uso que los usuarios demandan de los recursos TI, además de conocer problemas y eventos que puedan suceder.
Telefonía	Provee a los usuarios de la organización comunicación telefónica.
Antivirus	Provee protección ante virus a través de actualizaciones del mismo en las estaciones de trabajo de los usuarios y servidores de aplicación de la organización.
Internet corporativo	Provee acceso de la información de Internet a los usuarios de la organización
Seguridad	Proveer protección a los datos y confidencialidad de los usuarios

Nota. Fuente: Los autores.

4.6 Identificación de dispositivos y recursos críticos de TI que soportan la operatividad de los servicios críticos de TI definidos anteriormente.

Ejemplos de los servicios críticos de TI que se identifican en este paso, son todos aquellos dispositivos (hardware) tales como servidores, routers y switch que soportan la operación de los servicios críticos de TI. En este paso se genera una lista con los mismos. Elaborar cuadro dispositivo y descripción

4.7 Correlación de los objetivos de la organización a los servicios críticos TI

Como fue definido en el marco teórico del presente proyecto, en el Hospital Regional de Cajamarca, la tecnología de información tiene una directa relación de dependencia e importancia en el desempeño y soporte de las operaciones de la organización. Debido a lo anterior, este paso consiste en identificar la relación que poseen los objetivos de la organización con los servicios críticos de TI. Se toma como insumo la lista de servicios críticos de TI que apoyan directa e indirectamente al negocio, los cuales se correlacionan a los objetivos de la organización.

Se define el conjunto de objetivos de la organización como O, donde n ≥ 1 (n=número de objetivos de la organización). El conjunto On se relaciona al conjunto de servicios críticos de TI Sm, donde m ≥ 1 (m=número de servicios de TI). En la figura 13, se observa un ejemplo, en el cual se relaciona el objetivo O y los servicios S1.

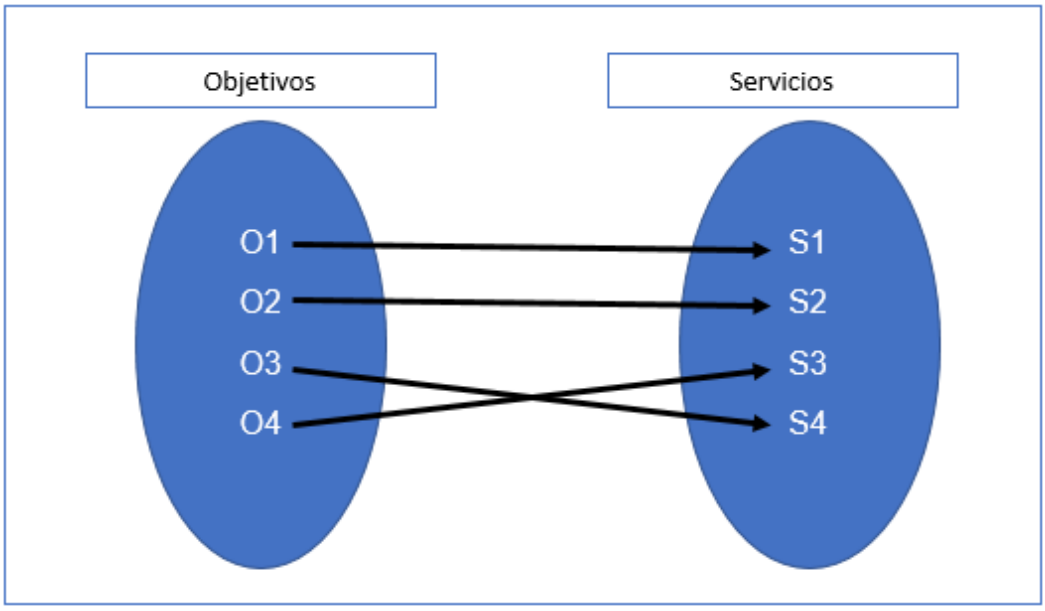


Figura 17. Correlación de objetivos con servicios
Fuente: Los autores

4.8 Identificar el mecanismo actual de monitoreo de la infraestructura TI.

Como fue definido en la problemática y marco teórico del presente proyecto, el mecanismo actual para monitorear la infraestructura TI es MANUAL, por lo que, no tiene o no usa ningún sistema automático que proporcione ayuda al administrador de redes.

4.9 Explicación Detallada de la Fase de Implementación

En este paso se empieza con el diseño e implementación de los mecanismos que permitan realizar el monitoreo de las métricas definidas para cada servicio y dispositivo TI.

- Analizar y seleccionar de herramienta de monitoreo de la infraestructura TI.
- Instalar y configurar el sistema de monitoreo.
- Incorporar los componentes críticos de TI y sus parámetros comunes.

4.10 Análisis de algunos sistemas de monitoreo existentes en el mercado

Este paso consiste en analizar las características de los diferentes sistemas de monitoreo estudiados, con el propósito de seleccionar un sistema que se adapte a las necesidades del Hospital y facilite la gestión de los recursos de la infraestructura TI.

Los sistemas presentados han sido seleccionados del universo de sistemas existentes, en base a análisis o revisiones realizadas por compañías dedicadas a la investigación y consultoría tecnológica, las cuales han sido definidas con más detalle en el marco teórico del presente proyecto.

A continuación, se presenta en las tablas, dos de los sistemas más representativos del mercado con algunas características pertenecientes al monitoreo de red.

Tabla 8: Comparación de sistemas de monitoreo.

CARACTERÍSTICAS	PANDORA FMS	ZABBIX
Administración		
Centralizada.	Si	Si
Con interfaz Web	Si	Si
Monitoreo: A (aplicaciones) e I (infraestructura)		
Enfoque	A-I	A-I
En tiempo real	Si	Si
Servidores	Si	Si
Routers y Switch	Si	Si
SNMP Y WMI	Si	Si
Con agentes	Si	Si
Manejador de Base de Datos		
Postgre SQL	Si	No
Oracle	Si	Si
MySql	Si	Si
RRDTool	Si	No
Instalación, configuración y Uso		
Auto detección de dispositivos	Si	Si
Vista gráfica de configuración	Si	Si
Fácil instalación y configuración	Si	No
Notificaciones		
Alertas visuales	Si	Si
Alertas audibles	Si	Si
Alertas por correo electrónico	Si	Si
Multiplataforma		
Linux	Si	Si
Windows	Si	No

Otros	Si	No
Informes y estadísticas		
Estadísticas	Si	Si
Predicción de estadísticas	Si	Si
Mapa de red	Si	Si
Informes SLA	Si	Si
Complementos y aplicaciones externas		
Complementos (pluggins)	Si	Si
Creación por el usuario	Si	Si
Integración con otras aplicaciones	Si	No
Scripts creados por el usuario	Si	No
Licencia		
Licencia	GNU GPL	GNU GPL
Acceso y seguridad		
Seguridad	Si	Si
Soporte y documentación		
Documentación	Si	Si
Soporte comercial	Si	No

Nota. Fuente: Los autores.

La información expuesta tanto en el marco teórico como en las anteriores tablas comparativas, sirven como base para seleccionar el sistema de monitoreo que posea las características que se adapte a los requerimientos establecidos por el Hospital Regional de Cajamarca.

4.11 Instalar y configurar el sistema de monitoreo

Se instala y configuran el sistema de monitoreo seleccionado. Este paso varía dependiendo de los requerimientos de instalación de cada sistema. Lo importante es tomar en cuenta las expectativas de monitoreo esperadas por el Hospital Regional de Cajamarca.

CAPITULO IV

IMPLEMENTACIÓN

DE LA PROPUESTA.

En esta etapa se implementaron las fases de la metodología del proyecto especificadas anteriormente. Para la realización de este proyecto se tomó como muestra la infraestructura TI del Hospital Regional de Cajamarca. Entre las fases de la metodología que se desarrollaron en la presente etapa, se encuentran la fase de análisis, implementación, verificación y optimización, las cuales se ejecutaron con el objetivo de determinar la influencia de la implementación de un sistema de monitoreo de infraestructura TI para gestionar las incidencias de la red LAN del Hospital Regional de Cajamarca.

5.1. ANÁLISIS DEL CASO DE ESTUDIO.

En esta fase se realizó el análisis al Hospital Regional de Cajamarca, en donde se aplicaron cada uno de los pasos definidos en la metodología, en el cual se describe la fase de análisis del proyecto de modo general. De la institución en estudio, se definieron los objetivos de la organización, así como también, la topología de la infraestructura tecnológica de información (TI). Esta información se analizó y proceso mediante el desarrollo de los siguientes pasos.

5.1.1. Identificación de los objetivos del Hospital Regional de Cajamarca

La Hospital Regional de Cajamarca, es una organización perteneciente al Estado, la cual se encarga de proveer servicios de salud a sus clientes haciendo uso de la tecnología de información (TI). Para efectos de la implementación del sistema de monitoreo en el presente proyecto, se identificaron y describieron los siguientes objetivos del Hospital Regional de Cajamarca, descritos en la siguiente tabla.

Tabla 9: Objetivos del área de estadística e informática

OBJETIVO	DESCRIPCIÓN
O1	Definir y establecer las responsabilidades, atribuciones, funciones, relaciones internas y externas y los requisitos de los cargos establecidos en el Cuadro para Asignación de Personal y contribuir al cumplimiento de los objetivos funcionales establecidos en el Reglamento de Organización y Funciones del Hospital Regional Cajamarca.
O2	Facilitar el desarrollo de las funciones operativas y administrativas, así como la coordinación y la comunicación de todos sus integrantes, eliminando la duplicidad de esfuerzos, confusión e incertidumbre para el cumplimiento de las funciones asignadas a los cargos o puestos de trabajo.
O3	Servir como instrumento de comunicación y medio de capacitación e información para entrenar capacitar y orientación permanentemente al personal.
O4	Establecer las bases para mantener un efectivo sistema de control interno y facilitar el control de las tareas delegadas.

Nota. Fuente: MOF Hospital Regional de Cajamarca.

Tabla 10: Objetivos del área de informática

OBJETIVO	DESCRIPCIÓN
OBI1	Lograr la provisión de servicios informáticos, sistemas de información, informática y telemática, en el ámbito institucional.
OBI2	Lograr que los usuarios internos y externos tengan disponibilidad de asesoría y asistencia técnica en el uso de aplicaciones informáticas y las nuevas tecnologías de la administración.
OBI3	Implantar proyectos de desarrollo tecnológico de información que se programen a nivel sectorial.
OBI4	Aplicar y mantener las normas y estándares de informática establecidas por el Ministerio de Salud.

Nota. Fuente: MOF Hospital Regional de Cajamarca.

Tabla 11: Objetivos del área de Telecomunicaciones

OBJETIVO	DESCRIPCIÓN
OBT1	Lograr la provisión de servicios de información de Telecomunicaciones
OBT2	Lograr que los usuarios internos y externos tengan la disponibilidad de asistencia técnica, en el uso de aplicación de Telecomunicaciones.
OBT3	Implantar los proyectos de desarrollo tecnológico de Telecomunicaciones establecidas por el Ministerio de Salud.

OBT4	Mantener comunicación permanente con las instituciones afines
OBT5	Coordinar y programar mantenimiento de los equipos de telecomunicaciones.

Nota. Fuente: MOF Hospital Regional de Cajamarca.

También se tomaron en cuenta los objetivos de las sub-áreas de Informática y telecomunicaciones visualizadas en las tablas anteriores, se tomó en cuenta las siguientes sub-áreas, ya que, son éstas las que se ven ligadas y están en constante comunicaciones con la infraestructura TI de la organización, además en una entrevista al administrador de redes del Hospital se estableció que el propósito del área de Telecomunicaciones, es brindar servicios de TI altamente disponibles, con el fin de apoyar los procesos operativos de los usuarios, basados en la comunicación, conectividad con los recursos de la infraestructura de TI y acceso seguro y confidencial a las áreas pertinentes de cada área. Esta información es importante tenerla presente para el paso posterior a este, en donde se seleccionarán lo servicios críticos de TI.

5.1.2. Identificación de los servicios críticos de TI del Hospital Regional de Cajamarca.

Este paso del análisis, se encarga de identificar los servicios críticos de TI, entre los cuales se definieron tanto los servicios críticos básicos comunes de TI y los servicios críticos de TI de la organización que provee el Hospital Regional de Cajamarca, y son observados en la siguiente tabla

Tabla 12: Servicios críticos de la infraestructura TI del Hospital Regional de Cajamarca

SERVICIO	DESCRIPCIÓN	TIPO
S1	Servicio de correo electrónico	Básico
S2	Servicio de impresión - Emisión de citas	Básico y Negocio
S3	Servicio de Telefonía	Básico
S4	Servicio de Base de datos - Servicio SIS Galen+ - SGBD: SQL 2008 - Servicio HIS – SGBD: POSTGRESQL - Servicio ARFSIS – SGBD: MySQL - Antivirus Kapersky – SGBD: SQL 2008	Negocio
S5	Servicio de DNS	Básico
S6	Servicio de Firewall	Básico
S7	Servicio de FTP	Básico
S8	Servicio de DHCP	Básico
S9	Servicio Active Directory	Negocio
S10	Servicio de Internet - Reniec - SIS - MAD	Negocio
S11	Servicio Network Time Protocol	Negocio

Nota. Fuente: MOF Hospital Regional de Cajamarca.

De la tabla 18, se toma a todos los servicios críticos de TI especificados los cuales nos servirán para lograr verificar la influencia de la implementación del sistema de monitoreo en la organización en estudio.

El presente proyecto de estudio y el Hospital Regional de Cajamarca no poseen acuerdos de niveles servicios SLA (Service Level Agreement). Pero para efectos de la aplicación del proyecto se utilizará los servicios críticos de TI seleccionados previamente. Ya que, es importante que las organizaciones mantengan monitoreados los servicios de TI que entregan los proveedores, con el propósito

de asegurar el cumplimiento de dichos acuerdos y vigilar la calidad de servicio que los proveedores está prestando.

5.1.3. Correlacionar los objetivos de la organización con los servicios tecnológicos de la infraestructura TI del Hospital Regional de Cajamarca

Una vez levantada la información de los servicios TI que soportan operacionalmente la gestión de la organización, se correlacionó los objetivos del Hospital Regional de Cajamarca con dichos servicios. Se tomaron en cuenta los objetivos más relevantes en cuestión a infraestructura TI, antes mencionados.

Recordando que los objetivos del Hospital Regional de Cajamarca son los siguientes:

- **O1**: Lograr la provisión de servicios informáticos, sistemas de información, informática y telemática, en el ámbito institucional.
- **O2:** Lograr que los usuarios internos y externos tengan disponibilidad de asesoría y asistencia técnica en el uso de aplicaciones informáticas y las nuevas tecnologías de la administración.
- **O3:** Lograr la provisión de servicios de información de Telecomunicaciones
- **O4:** Lograr que los usuarios internos y externos tengan la disponibilidad de asistencia técnica, en el uso de aplicación de Telecomunicaciones.
- **O5:** Mantener comunicación permanente con las instituciones afines

- **O6:** Brindar servicios de TI altamente disponibles, con el fin de apoyar los procesos operativos de los usuarios, basados en la comunicación, conectividad con los recursos de la infraestructura de TI y acceso seguro y confidencial a las áreas pertinentes de cada área

Y los servicios críticos de TI en estudio son:

- **S1:** Servicio de correo electrónico
- **S2:** Servicio de impresión
- **S3:** Servicio de Telefonía
- **S4:** Servicio de Base de datos
- **S5:** Servicio de Firewall
- **S6:** Servicio de FTP
- **S7:** Servicio de DHCP
- **S8:** Servicio Active Directory
- **S9:** Servicio de Internet
- **S10:** Servicio Network Time Protocol

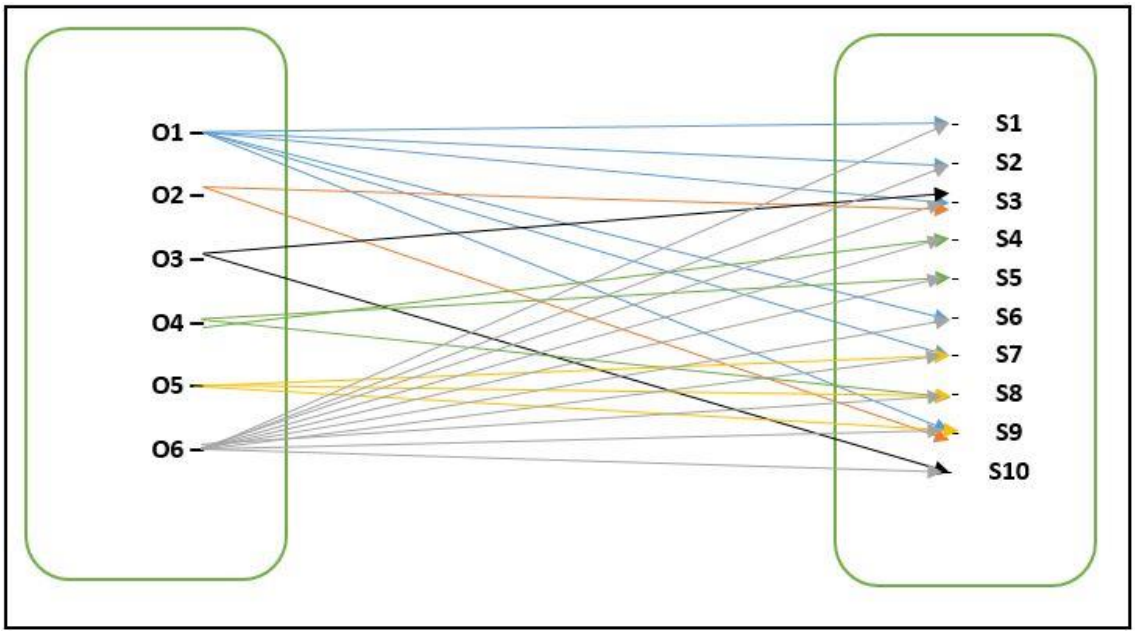


Figura 18. Correlación de objetivos con los servicios críticos TI del Hospital Regional de Cajamarca
Fuente: Los autores.

Identificar el mecanismo actual de monitoreo de la infraestructura TI.

Para definir el mecanismo actual de monitoreo y los indicadores para poder medir la influencia de la implementación de un sistema de monitoreo de infraestructura TI para gestionar las incidencias en la red LAN del Hospital Regional de Cajamarca, se recurrió a la elaboración de encuestas y cuestionarios estructurados para antes y después de la implementación, los siguientes resultados obtenidos son:

5.1.4. Validación de indicadores de medición

5.1.4.1. Tiempo de Respuesta

1. ¿Cuál es el tiempo promedio de atención a incidencias presentadas en la infraestructura TI?

Tabla 13: Tiempo de respuesta antes de la implementación

Pregunta	30 min	1 hora	3 horas	24 hrs
Tiempo de respuesta	68%	10%	20%	2%

Nota. Fuente: Los autores.

5.1.4.2. Exactitud al encontrar el fallo

1. ¿Cuál es el tiempo promedio que le toma encontrar con exactitud de que dispositivo TI o servicio proviene la incidencia?

Tabla 14: Exactitud al encontrar el fallo antes de la implementación

Pregunta	30 min	1 hora	3 horas	5 hrs
Exact. Al enc. La incidencia	5%	10%	70%	15%

Nota. Fuente: Los autores.

5.1.4.3. Satisfacción del cliente

1. ¿Cómo califica el mecanismo actual de monitorear la infraestructura TI de la organización?

Tabla 15: Satisfacción del cliente antes de la implementación

Pregunta	Excelente	Bueno	Regular	Malo	Pésimo
Satisf. Del cliente	1%	20%	70%	5%	5%

Nota. Fuente: Los autores.

5.1.4.4. Índice de producción

Antes de la implementación:

N° de incidencias promedio: 05

N° de incidencias atendidas promedio: 02

Tabla 16: Índice de producción antes de la implementación

Indicador	Medidor	Estado	Valor min	Valor max	Semáforo
ÍNDICE DE PRODUCCIÓN	Número de Incidencias / Número de incidencias atendidas	**BUENO**	**> 0**	**< 1.99**	
		REGULAR	**>2**	**<2.99**	
		MALO	**> 3**		

Nota. Fuente: Los autores.

Índice de producción = 2.5

5.1.4.5. Confiabilidad

1. ¿Confía en el mecanismo actual para monitorear la infraestructura TI de la organización?

Tabla 17: Confiabilidad antes de la implementación

Pregunta	Nunca	A veces	Casi siempre	Siempre	Totalmente
Confiabilidad	1%	20%	75%	3%	1%

Nota. Fuente: Los autores.

5.1.4.6. Índice de quejas

1. ¿Cuántas quejas se presentan por semana sobre la caída de un servicio o el mal funcionamiento de un dispositivo en la red?

Tabla 18: Índice de quejas antes de la implementación

Pregunta	1 semana	2 semana	3 semana	4 semana
Índice de quejas	4	8	3	7

Nota. Fuente: Los autores.

PROMEDIO: 5.5 al mes.

5.2.FASE DE IMPLEMENTACIÓN DEL PROYECTO

5.2.1. Identificación y correlación de los dispositivos críticos de TI con los servicios críticos del Hospital Regional de Cajamarca

Durante el proceso de implementación del proyecto, se identificaron los dispositivos de TI, considerados importantes por el proyecto para las operaciones del Hospital Regional de Cajamarca. Luego estos dispositivos fueron configurados en un sistema de monitoreo seleccionado durante la presente fase.

La idea de identificar los servicios críticos de TI, es disgregarlos en los dispositivos que los componen y soportan su operación, de forma de incorporarlos al proceso de monitoreo. En la figura 19, se presenta la topología de la infraestructura de tecnología de información (TI) del Hospital Regional de Cajamarca, la cual está encargada de prestar servicios tecnológicos a los usuarios. Estos servicios están compuestos por diversos dispositivos tales como routers, switches y servidores, encargados de apoyar la operatividad de los procesos del Hospital Regional de Cajamarca.

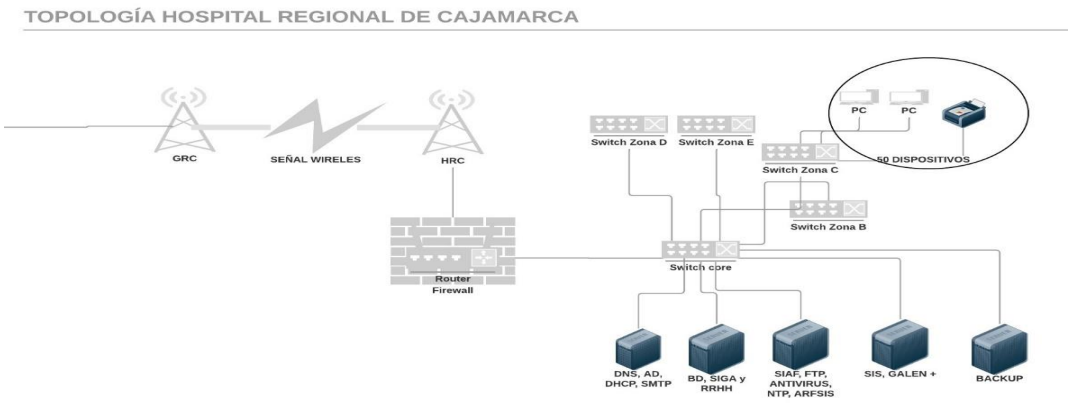


Figura 19. Topología de red del Hospital Regional de Cajamarca

Fuente: Los autores.

A continuación, se presenta en la siguiente tabla los dispositivos críticos de TI del Hospital Regional de Cajamarca:

Tabla 19: Dispositivos críticos del Hospital Regional de Cajamarca

Disp.	Dispositivo	Descripción
D1	Router Firewall	Sony Wall 3500 Router que funciona como firewall al mismo tiempo.
D2	Switch Core	Switch's CISCO conectado con Fibra Óptica con los switch's por zonas, está configurado en 4 VLAN'S, las cuales son para : VOIP, DATA, ADM y WLAN.
D3	Switch's por Zonas - Zona B - Zona C - Zona D - Zona E	Switch's CISCO, conectados por ethernet, categoría 6 establecido por el MINSA (Ministerio de Salud). Por cada zona tiene un determinado de dispositivos en oficinas (Computadoras de escritorio)
D4	Servidor DNS, AD, DHCP, SMTP.	Servidores de DNS (Domain Name System), AD (Active Directory), DHCP (Dynamic Host Configuration Protocol) y SMTP (Servidor de correo).

D5	Servidor de Base de Datos, SIGA, Personal	Servidor SQL SERVER 2000, Sistema de información gerencial y administrativa (proveedor MEF - Ministerio de Economía y Finanzas) y Software de registro de personal.
D6	Servidores SIAF, FTP, ANTIVIRUS, ARFSIS, NTP	SIAF (Sistema Integrado de administración Financiera), FTP (File Transfer Protocol), ARFSIS (Aplicativo de registro de formatos para el seguro integral de salud), NTP (Network Time Protocol).
D7	Servidores SIS, Galen+	SIS (Sistema Integral de Salud) y Galen+ (Aplicativo para gestión hospitalaria del Hospital Regional de Cajamarca)
D8	Servidores Backup	Respaldo de todos los servidores.

Nota. Fuente: Los autores

Se reiteran los servicios críticos de TI identificados en el presente proyecto, para facilitar la descripción presente:

- **S1:** Servicio de correo electrónico
- **S2:** Servicio de impresión
- **S3:** Servicio de Telefonía
- **S4:** Servicio de Base de datos
- **S5:** Servicio de Firewall
- **S6:** Servicio de FTP
- **S7:** Servicio de DHCP
- **S8:** Servicio Active Directory
- **S9:** Servicio de Internet
- **S10:** Servicio Network Time Protocol

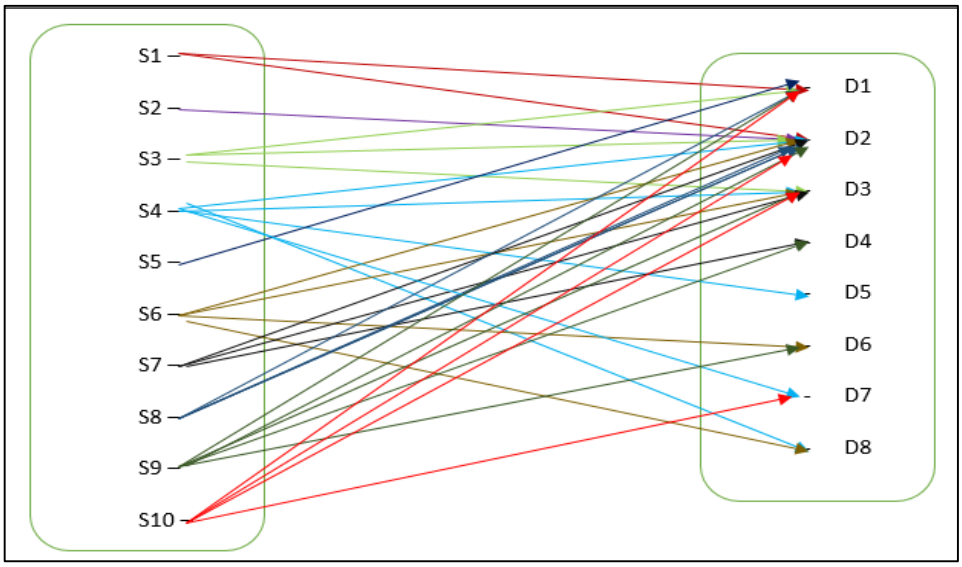


Figura 20. Correlación de los servicios TI con los dispositivos TI del Hospital Regional de Cajamarca

Fuente: Los autores.

Luego de haber identificado los dispositivos de TI que componen cada uno de los servicios críticos del proyecto, se construyó la tabla de inventario de dispositivos (ver tabla 26) que fueron posteriormente incorporados en el proceso de monitoreo en las siguientes etapas:

Tabla 20: Inventario de dispositivos críticos de la infraestructura TI del Hospital Regional de Cajamarca.

Sn	Servicio Crítico TI	Dn	Dispositivo TI
S1	Servicio de correo electrónico	D1	Router Firewall
		D2	Switch CORE
S2	Servicio de impresión	D2	Switch CORE
S3	Servicio de telefonía	D1	Router Firewall
		D2	Switch CORE
		D3	Switch por Zonas
S4	Servicio de Base de datos	D2	Switch CORE
		D3	Switch por Zonas
		D5	Servidor de base de datos
		D8	Servidor de Backup
		D7	Servidor Galen +
S5	Servicio de Firewall	D1	Router Firewall

S6	Servicio FTP	D2	Switch CORE
		D3	Switch por zonas
		D6	Servidor FTP
		D8	Servidor de Backup
S7	Servicio DHCP	D2	Switch CORE
		D3	Switch por Zonas
		D4	Servidor DHCP
S8	Servicio Active Directory	D1	Router Firewall
		D2	Switch CORE
		D3	Switch por Zonas
		D4	Servidor AD
S9	Servicio de Internet	D1	Router Firewall
		D2	Switch CORE
		D3	Switch por Zonas
		D4	Servidor de DNS, AD y DHCP
		D6	Servidor SIAF, antivirus, SIS
S10	Servicio Network Time Protocol	D1	Router Firewall
		D2	Switch Core
		D3	Switch por zonas

Nota. Fuente: Los autores.

5.2.2. Identificación de los parámetros críticos de monitoreo de los Dispositivos de TI.

La clasificación de parámetros críticos de monitoreo utilizada en el presente proyecto, es una guía que facilita su incorporación a los sistemas de monitoreo de infraestructura de TI. Estos parámetros deben ser medidos constantemente, para mantener la mayor disponibilidad y operatividad de los servicios de TI y poder gestionar las incidencias presentadas. La clasificación de los parámetros críticos comunes de monitoreo que propone el proyecto, esta descrita de igual forma en el marco teórico. En donde se definió un nivel de parámetros de monitoreo del hardware, siendo estos comunes entre los diferentes dispositivos TI, tales como los equipos de comunicaciones (routers y switches) y los equipos de

procesamiento de datos (servidores). Estos parámetros comunes se dividen en tres tipos entre los cuales son: de sistema, de entorno y de red, en la tabla 27 se describen en detalle.

Tabla 21: Parámetros críticos de monitoreo

Parámetros	Descripción
Sistema	Uso de procesador
	Uso de disco
	Utilización de memoria RAM
Entorno	Estado del ventilador
	Estado del sensor de temperatura
	Estado del suministro de Energía
Red	Interconectividad entre los dispositivos
	Utilización de las interfaces de red
	Tiempo de respuesta

Nota. Fuente: Los autores

Con el inventario de dispositivos críticos obtenido en el paso previo, se realizó posteriormente la configuración de los tres niveles de parámetros en el sistema de monitoreo.

Es importante considerar que la herramienta de monitoreo por lo menos sea capaz de medir las métricas básicas propuestas por el proyecto. En el caso de estudio de la presente investigación se encontraron distintos tipos de dispositivos TI, sin embargo, esta clasificación permite estandarizar el proceso de monitoreo para los distintos dispositivos existentes (routers, switches y servidores). Esta información se tiene presente para utilizarla en la configuración de la herramienta que apoya el proceso de monitoreo.

5.2.3. Análisis y selección de la herramienta de monitoreo para la infraestructura TI del Hospital Regional de Cajamarca.

En el presente proyecto se requirió analizar un conjunto de sistemas de monitoreo que gestionen las incidencias de la infraestructura de TI del Hospital Regional de Cajamarca.

Las características de los diferentes sistemas de monitoreo fueron analizadas del universo creado en el marco teórico del proyecto. Los sistemas de monitoreo descritos fueron seleccionados, en base a las referencias y recomendaciones encontradas en foros y páginas web de gran renombre en la comunidad informática. Consultoras que se encargan periódicamente de emitir informes y estudios acerca del análisis de las tecnologías y las herramientas que la apoyan. Sin embargo, es importante resaltar que cada organización tiene distintas necesidades, las cuales se relacionan directamente al tamaño de su infraestructura de TI, diversidad de los componentes que soportan los procesos de la organización y la capacidad económica de inversión en dichas herramientas. Entre las características que debe de poseer el sistema de monitoreo en el cual se instaló y probó el funcionamiento del proyecto propuesto para el Hospital Regional de Cajamarca, se citan las siguientes:

- Debe de poseer bajo costo y fácil acceso a los instaladores de la herramienta.
- Debe poseer documentación precisa, disponible y suficiente, acerca del proceso de instalación y configuración.

- Ser capaz de monitorear los parámetros comunes y básicos de los componentes críticos del Hospital Regional de Cajamarca.
- Pueda ser ejecutada bajo los sistemas operativos Linux o Windows.
- Compatible con el protocolo SNMP.
- Compatible con el protocolo WMI, nativo de Windows.
- Capacidad de gestionar las incidencias de los dispositivos críticos de la infraestructura de TI.
- Capacidad para manejar las incidencias en servidores, routers y switch
- Permita presentar los datos en tiempo real de la infraestructura TI, a través del uso de una interfaz Web, que gestione alarmas visuales, alarmas audibles y notificaciones por correo electrónico.

Luego de investigar las diferentes herramientas de monitoreo de código abierto descritas en el marco teórico, se seleccionó en principio la herramienta de monitoreo ZABBIX, por sus características y reconocimientos, sin embargo el proceso de instalación y configuración se encontró complicado, debido a la poca documentación disponible y a la cantidad de pasos que se deben realizar para completar una tarea específica; que si bien se logra en el tiempo, este es considerablemente mayor en comparación con otras herramientas. Considerando lo anterior, una de las opciones disponible y similar la herramienta PANDORA FMS, ya que satisface todos los requerimientos incluyendo facilidad de instalación y configuración, una interfaz Web intuitiva, que facilita el desarrollo e implementación del sistema de monitoreo. De manera similar a las otras herramientas analizadas, la documentación y diferentes características de PANDORA FMS se encuentra documentada en el marco teórico.

Recordando que PANDORA FMS es una aplicación de gestión de redes y servidores de código abierto, la cual se administra a través de una interfaz web y permite monitorear disponibilidad, inventario/configuración e incidencias de los dispositivos de TI. Es importante destacar que el propósito de éste paso, no es recomendar ni destacar una herramienta de monitoreo específica, sino realizar una selección optima de acuerdo los requerimientos reconocidos, y que la misma permita verificar el funcionamiento del sistema de monitoreo para el proyecto. A continuación, se describe detalladamente las actividades realizadas para la implementación del proyecto con el sistema de monitoreo PANDORA FMS.

5.2.4. Implementación y configuración del sistema de monitoreo

Para el desarrollo del proyecto, antes de implementar directamente en el hardware establecido, se emplearon herramientas de virtualización sobre las cuales se probaron y configuraron los sistemas de monitoreo establecidos en el marco teórico. En la figura que se muestra a continuación se presenta la topología de la infraestructura TI del Hospital Regional de Cajamarca para determinar el objetivo del proyecto que es la influencia de la implementación de un sistema de monitoreo de infraestructura para gestionar las incidencias de la organización, se considera los servicios de TI y dispositivos TI, mencionados anteriormente. Según describe la figura 16, en la cual se observan los dispositivos que integran la infraestructura TI del Hospital Regional de Cajamarca.

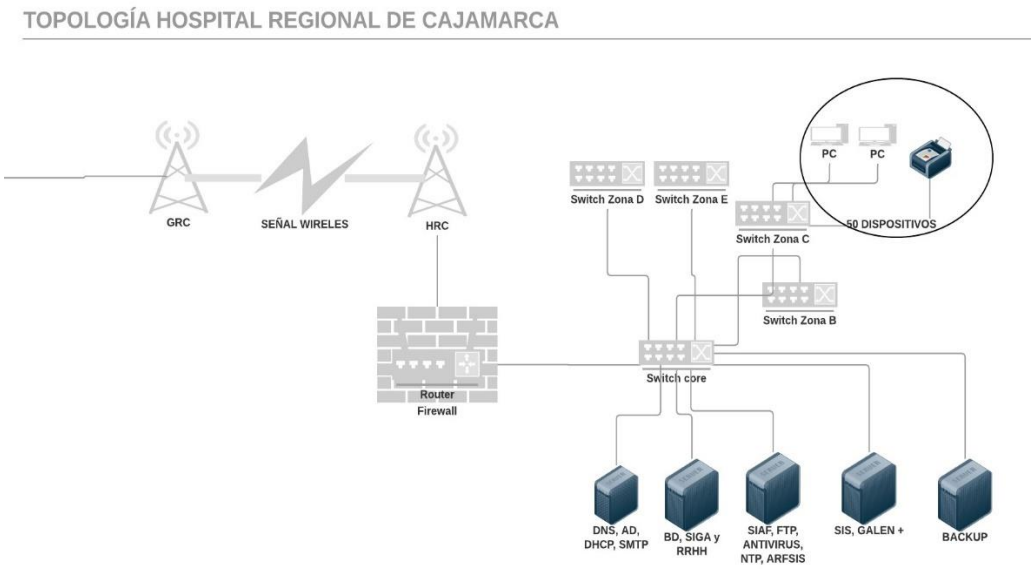


Figura 21. Topología de la red LAN del Hospital Regional de Cajamarca

Fuente: Los autores.

5.2.5. Herramientas de apoyo en el desarrollo del proyecto.

En el presente proyecto se empleó el uso de herramientas virtuales, en primer lugar, ya que, necesitamos obtener todo tipo de conocimiento certero mediante la práctica y equivocación para no dañar el hardware del Hospital. Y, en segundo lugar, debido a que las herramientas virtuales de hoy en día, permiten la ejecución de una imagen de sistema operativo que para el presente proyecto sería S.O. LINUX.

La herramienta de virtualización empleada para instalar los sistemas de monitoreo fue VMware Workstation versión 10.0.0 desarrollado por EMC Corporation y gratuito (VMware, 2007), la cual es multiplataforma compatible con las plataformas Windows, Linux, Macintosh y Solaris. Los sistemas que se muestran en la figura 18 se virtualizaron sobre la mencionada herramienta

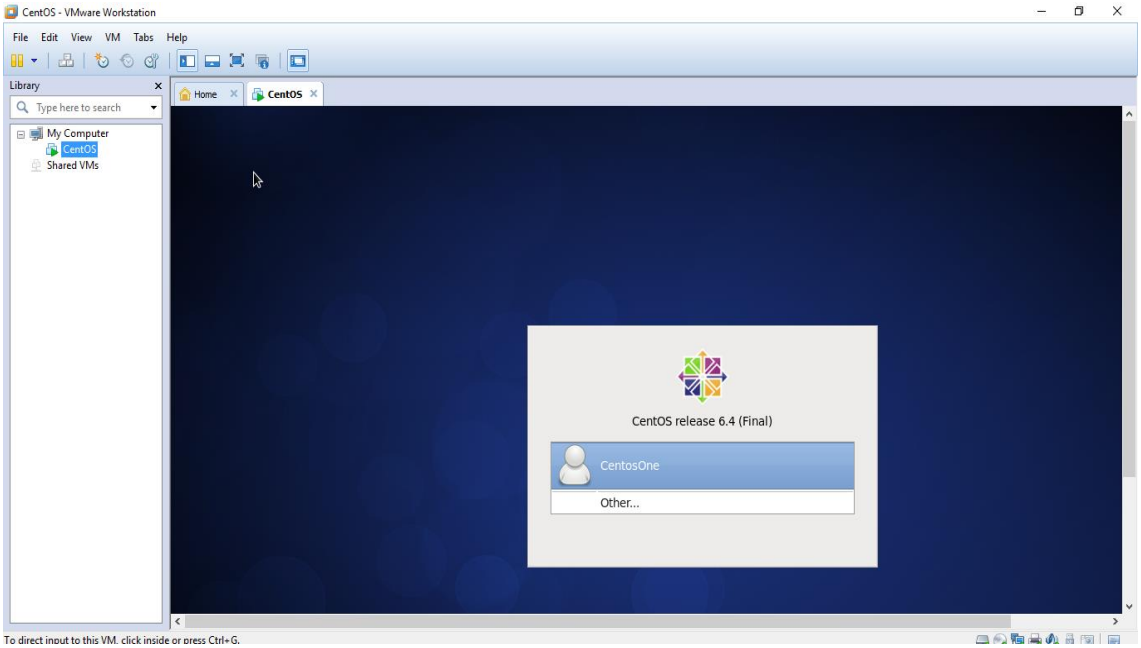


Figura 22. Entorno virtual

Fuente: Los autores.

El hardware establecido para el desarrollo del proyecto proporcionado por el Hospital Regional de Cajamarca posee plataforma de entorno operativo WINDOWS 7, las características del hardware están conformadas por: cuatro (4) gigabytes de memoria RAM, procesador INTEL de 2.00 GHz, características mínimas que se recomiendan para ejecutar el sistema de monitoreo, debido a que consume gran cantidad de los recursos de memoria RAM del equipo. Durante la ejecución del sistema de monitoreo el equipo en algunas ocasiones presento lentitud en el procesamiento de las instrucciones que se le solicitaron, sin embargo, brevemente recuperaba su normal funcionamiento. Cabe destacar que el sistema de Monitoreo PANDORA FMS el cual recolecta todo el tráfico SNMP, PING, WMI, etc. que describe el desempeño de cada uno de los dispositivos y servicios TI de la organización. En la tabla 25 se describe el direccionamiento IP

de cada uno de los servicios y dispositivos que pertenecen a la infraestructura TI del Hospital Regional de Cajamarca.

Tabla 22: Direccionamiento de la topología de red del Hospital Regional de Cajamarca

Segmento	Descripción	Direccionamiento
S1	Segmento para DATOS – VLAN 30	172.16.30.0/23
S2	Segmento para VOZ – VLAN 20	172.16.0.0/23
S3	Segmento de Administración – VLAN 40	172.16.40.0/24
S4	Conexión a wireless LAN (WLAN) – VLAN 50	192.168.1.0/24
SERVIDORES WINDOWS 2000		
S1-A	AD, DNS, DHCP, SMTP	172.16.30.2
S1-B	BASE DE DATOS, SIGA, PERSONAL	172.16.30.3
S1-C	SIAF, FTP, ANTIVIRUS, ARFSIS	172.16.30.4
S1-D	SIS, GALEN+, BD SQL2000	172.16.30.5
S1-E	BACKUP	172.16.30.6
SERVIDORES LINUX DEBIAN		
S1-F	HIS, POSTGRES, APACHE	172.16.30.12
S2-A	CENTRALITA	172.16.0.2
S2-B	ROUTER DHCP	172.16.0.3

Nota. Fuente: Los autores.

5.2.6. Instalación y configuración del servidor de monitoreo.

Una vez configurada el entorno físico o hardware, se procedió a instalar el sistema de monitoreo PANDORA FMS. Se instaló la distribución de Linux CENTOS y además se descargó e instalo PANDORA FMS. Para el proceso de instalación de PANDORA FMS se siguieron los siguientes pasos:

5.2.6.1. Instalación

- Instalamos las librerías EPEL por comandos: Las librerías EPEL, no vienen configuradas dentro de CENTOS, por lo que, es necesario

descargar e instalar de la administración de CENTOS RHEL, estas librerías. Se necesita para que pueda leer el EPEL que ha creado PANDORA FMS, el cual viene configurado con la BD y PHP para su próxima instalación.

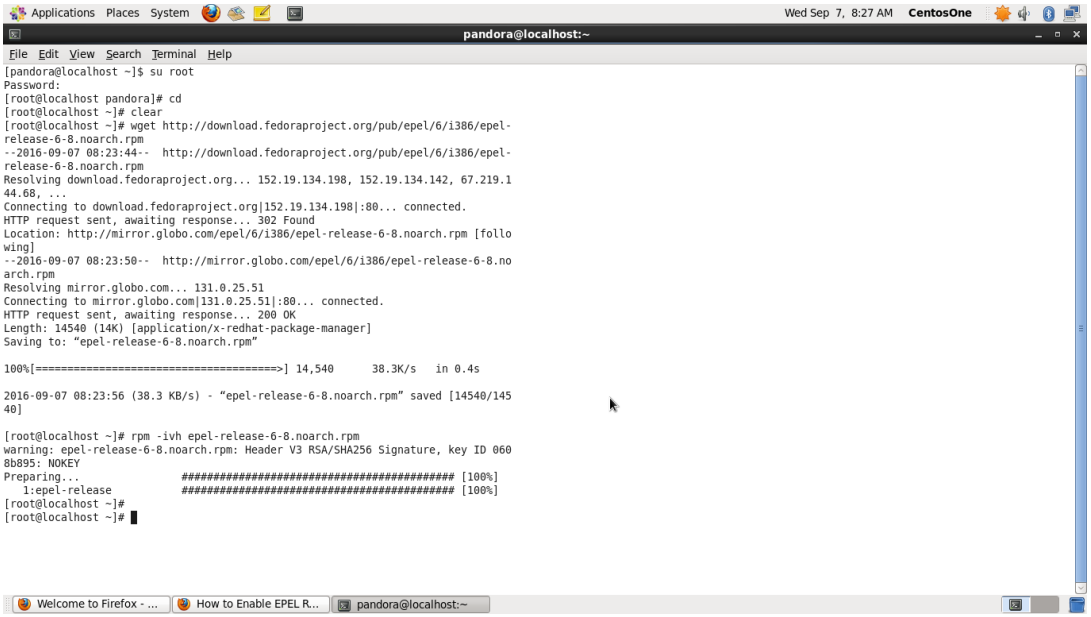


Figura 23. Instalación EPEL

Fuente: los autores.

- Instalamos EPEL-PANDORAFMS: Como antes mencionado, en este paso instalamos el EPEL de Pandora FMS, el cual configurará la parte de BD y programación para tener un acceso más rápido a la interfaz.

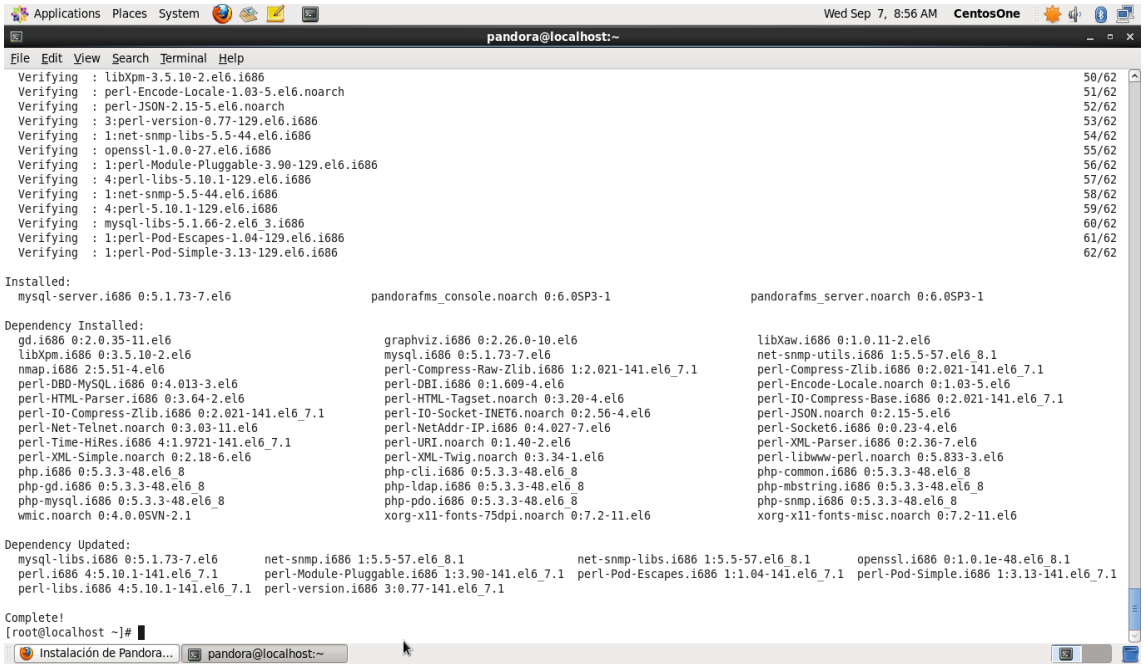


Figura 24. Instalación Pandora

Fuente: los autores.

- Iniciamos los servicios MYSQL y APACHE: iniciamos los servicios con el fin de empezar la instalación. Se inicia el servicio MYSQL para que pueda entrar en acción la BD y guardar datos. También se inicia el servicio HTTPD, que en Linux, éste hace referencia al servidor APACHE, para que pueda cargar la página de configuración.

Figura 25. Inicio de servicios Apache y Mysql

Fuente: los autores.

- Instalación de PANDORAFMS por Interfaz WEB: Los pasos ahora en adelante son los rutinarios.

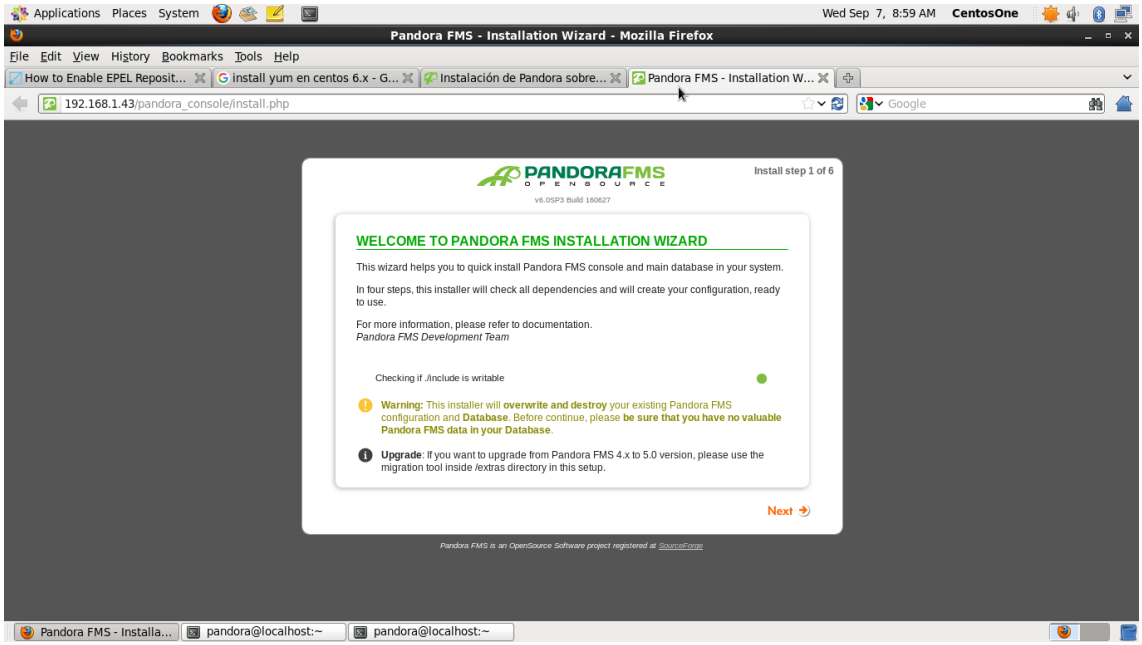


Figura 26. Configuración pandora FMS.

Fuente: los autores

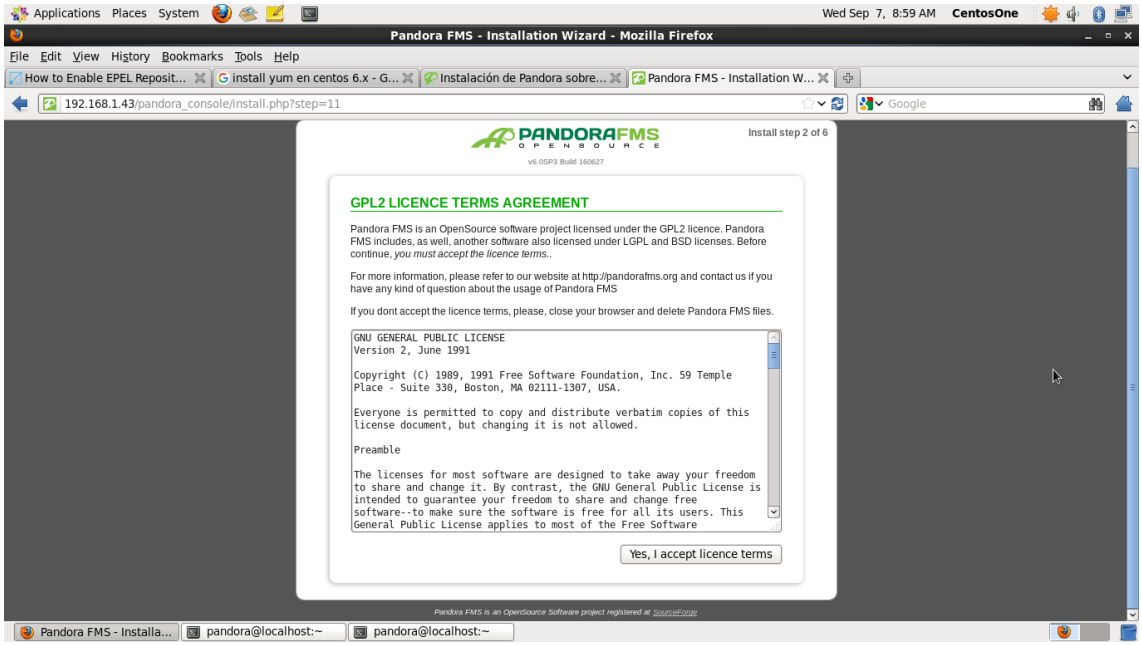


Figura 27. Configuración pandora FMS - 2.

Fuente: los autores

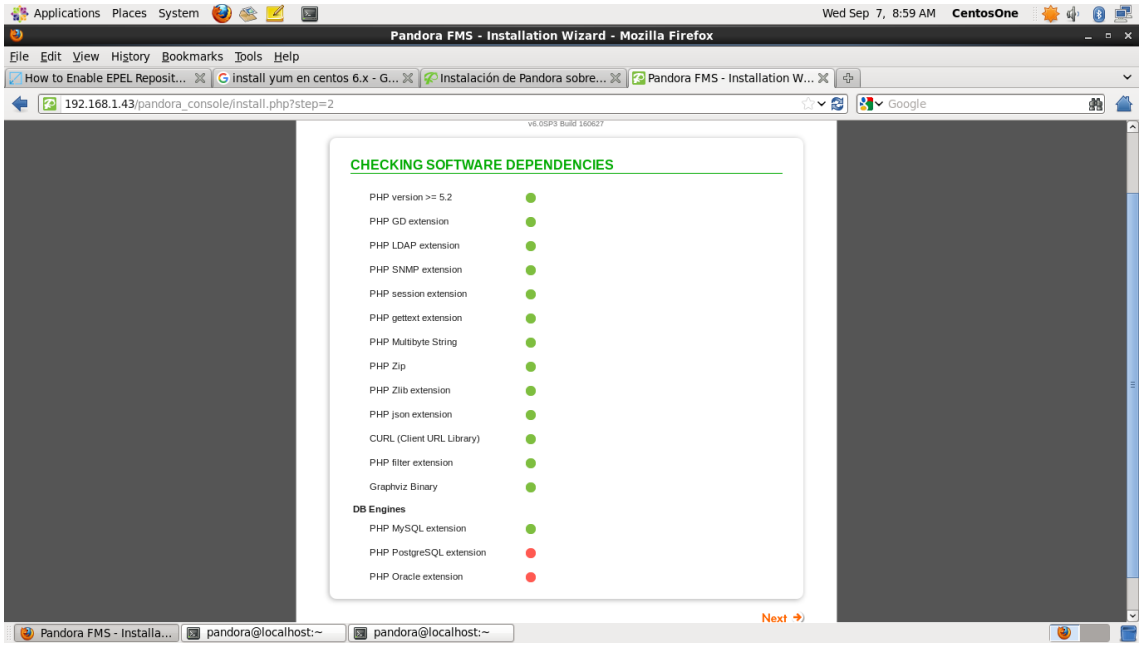


Figura 28. Configuración pandora FMS - 3.

Fuente: los autores

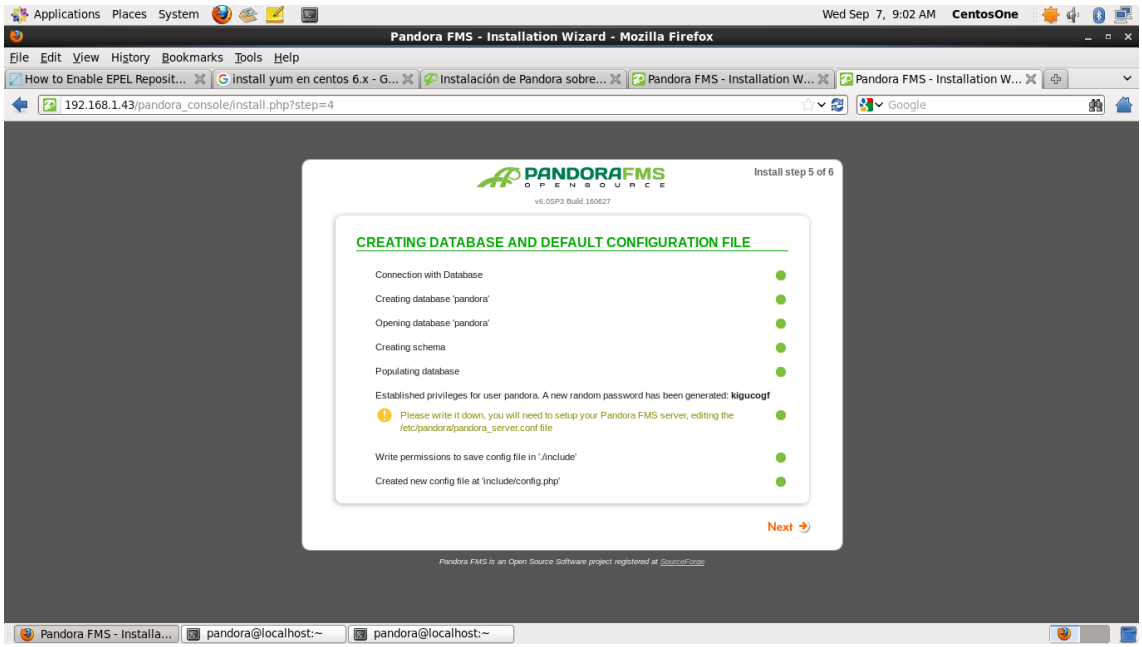


Figura 29. Configuración pandora FMS - 4.

Fuente: los autores

- Verificamos la instalación y borramos el “Install.php”: Se borra el “install.php” con el fin de no equivocarse o entrar nuevamente a la interfaz de instalación esta es por seguridad, sobre todo.

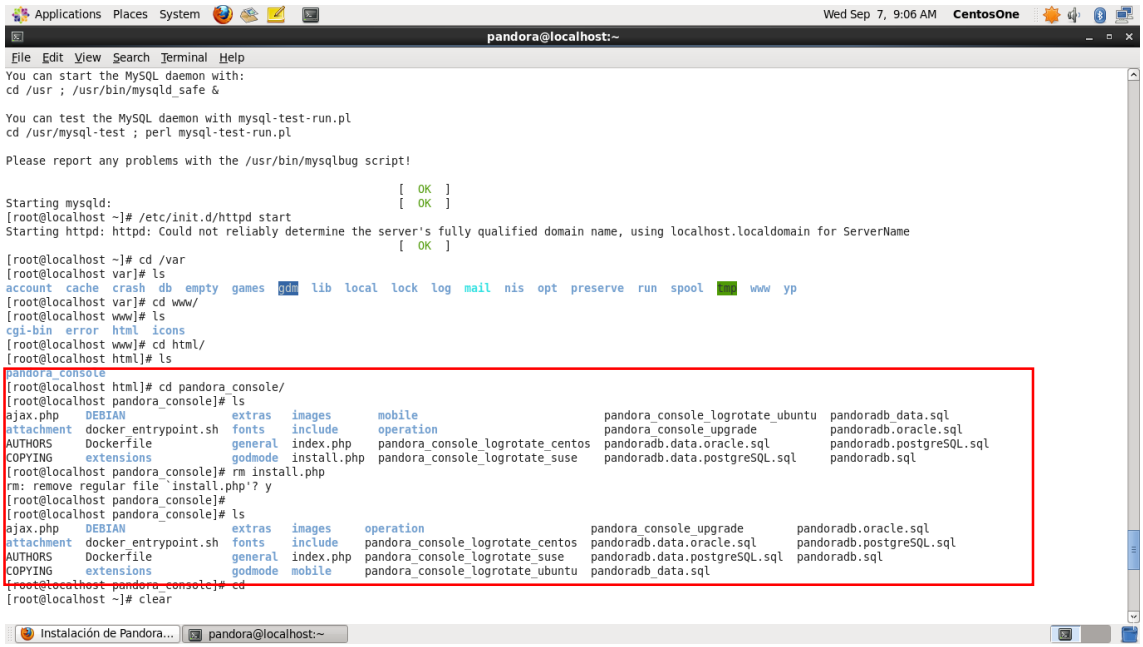


Figura 30. Configuración pandora FMS - 5.

Fuente: los autores

- Interfaz de Pandora FMS

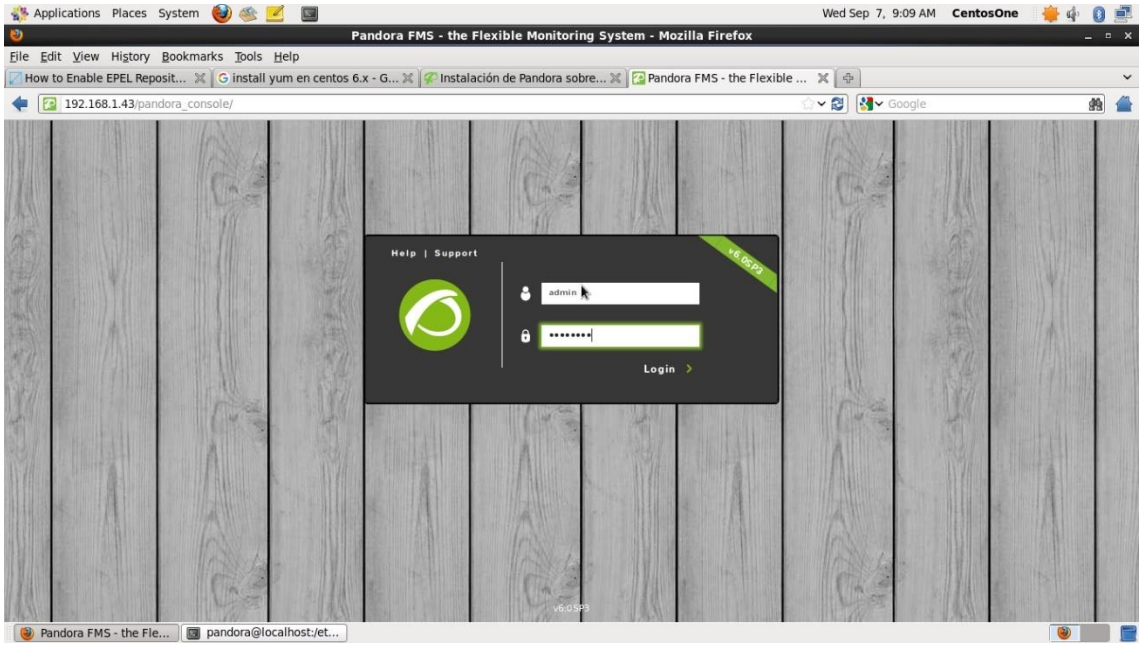


Figura 31. Interfaz de inicio Pandora FMS.

Fuente: los autores

5.2.6.2. Identificación de los dispositivos TI, servicios TI y parámetros a monitorear.

Una vez instalado el servidor de monitoreo, se incorporó a éste los dispositivos críticos y sus parámetros comunes de monitoreo (sistema, entorno y red) definidos en pasos previos, y por relacionarse directamente con los servicios de TI que tienen impacto para el Hospital Regional de Cajamarca. Los dispositivos TI relacionados a los servicios mencionados los cuales serán monitoreados se muestran en la tabla 22.

Tabla 23: Dispositivos y servicios TI a monitorear

N°	Nombre	IP	Descripción
1	Router – Firewall	172.16.30.254	Sonic Wall 3500 Router que funciona como firewall al mismo tiempo encargado de la seguridad del Hospital Regional de Cajamarca

2	Switch Core 2.1 2.2	 I. 172.16.30.1 II. 172.16.40.1	Switch's CISCO conectado con Fibra Óptica con los switch's por zonas, está configurado en 4 VLAN'S, las cuales son para: VOIP, DATA, ADM y WLAN.
3	Switch Zona B 3.1 3.2	 I. 172.16.40.4 II. 172.16.40.5	Switch encargado de conectar todos los dispositivos TI de la zona B con los servicios TI del Hospital. Conecta los dispositivos de los consultorios generales y oficinas administrativas
4	Switch Zona C 4.1 4.2 4.3	 I. 172.16.40.254 II. 172.16.40.11 III. 172.16.40.7	Switch encargado de conectar todos los dispositivos TI de la zona C con los servicios TI del Hospital. Conecta netamente oficinas administrativas
5	Switch Zona D 5.1 5.2	 I. 172.16.40.10 II. 172.16.40.3	Switch encargado de conectar todos los dispositivos TI de la zona D con los servicios TI del Hospital. Conecta oficinas administrativas, pero también oficinas dedicadas al rubro de la organización
6	Switch zona E	I. 172.16.40.2	Switch encargado de conectar todos los dispositivos TI de la zona E con los servicios TI del Hospital. Conecta la mayor parte de oficinas de logística y en los pisos superiores oficinas del rubro de la organización.
7	Servicio de Correo electrónico	172.16.31.253	Servicio brindado de Correo electrónico institucional en ZIMBRA, dominio: mail.hrc.gob.pe
8	Servicio de telefonía	172.16.0.2	Servicio brindado de telefónica sobre VOIP de CISCO. Teléfonos cisco IP Phone 7675
9	Servicio de impresión	172.16.30.2	Servicio brindado especial y obligatoria al área de admisión para la impresión de Citas particulares y relacionadas con el Sistema Integral de Salud. Impresoras en red HP Laserjet Pro 400
10	Servicio de internet	172.16.30.12	Aquí tomamos como referencia al servidor web de la página institucional, ya que, el internet lo provee el GRC mediante AP por modo troncal. www.hrc.gob.pe
11	Servicio DNS	172.16.30.2	Servicio brindado a la infraestructura TI del Hospital el cual transforma el IP de una página web en un nombre.com

12	Servicio DHCP	172.16.30.2	Servicio brindado al hospital, el cual, asigna IP a cada dispositivo.
13	Servicio Active Directory	172.16.30.3	Servicio brindado para que el administrador de la infraestructura TI pueda gestionar equipos cliente, servicios de red y aplicaciones que están distribuidos desde una ubicación central
14	Servicio de Base de Datos	172.16.30.3	Servicio brindado para gestionar de diferentes formas los datos del Hospital, se encuentra en Windows server 2000
15	Servicio Sistema integrado de administración financiera (SIAF)	172.16.30.4	Servicio desarrollado por el Ministerio de Economía y Finanzas netamente para administración pública.
16	Servicio de Antivirus	172.16.30.4	Servicio brindado a los clientes de la infraestructura TI para protección de virus, spyware, etc. Utiliza Kaspersky.
17	Servicio FTP	172.16.30.4	Servicio brindado a la infraestructura TI del Hospital para compartir archivos en red
18	Servicio Network Time Protocol	172.16.30.2	Servicio brindado para sincronizar los relojes de la infraestructura TI a través de la red del Hospital.
19	Servicio GALEN +	172.16.30.5	Servicio brindado para la gestión de citas para los diferentes tipos de consultorios.
20	Servidor de backup	172.16.30.6	Servicio brindado para el respaldo de toda la información.

Nota. Fuente: Los autores

Tabla 23: Parámetros a monitorear

Parámetros	**Descripción**
Sistema	Uso de procesador
	Uso de disco
	Utilización de memoria RAM
Entorno	Estado del ventilador
	Estado del sensor de temperatura
	Estado del suministro de Energía
Red	Disponibilidad (ping)
	Tiempo de respuesta

Nota. Fuente: Los autores

5.2.6.3. Configuración

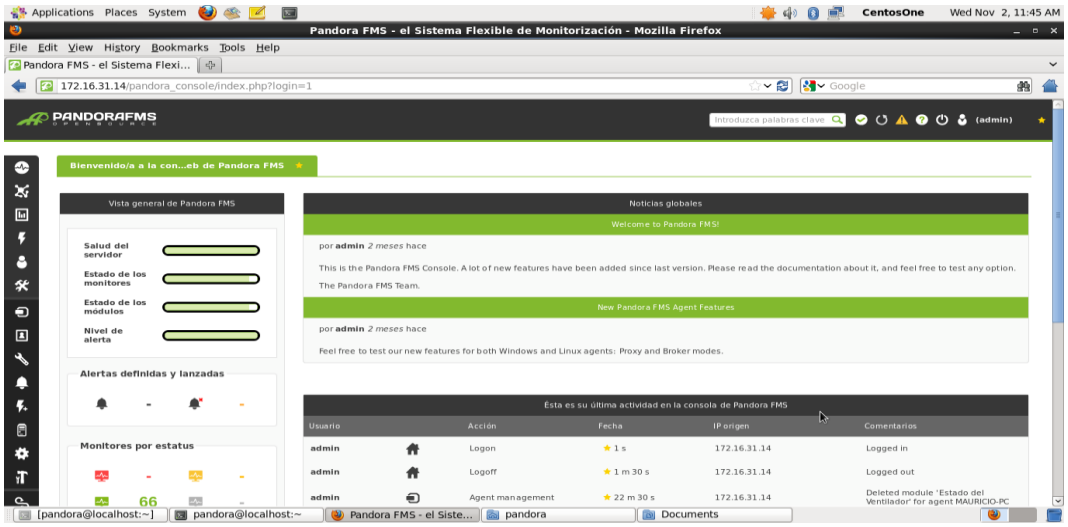


Figura 32. Interfaz de administración

Fuente: Los autores.

Configuración de dispositivos y servicios TI a monitorear.

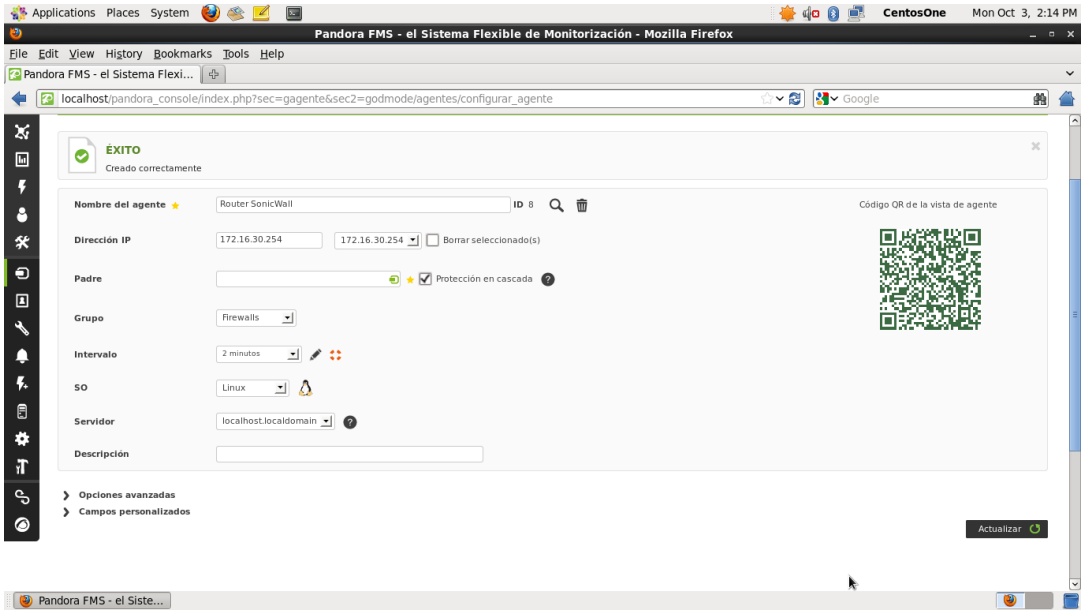


Figura 33. Creación de agentes para dispositivos TI

Fuente: Los autores.

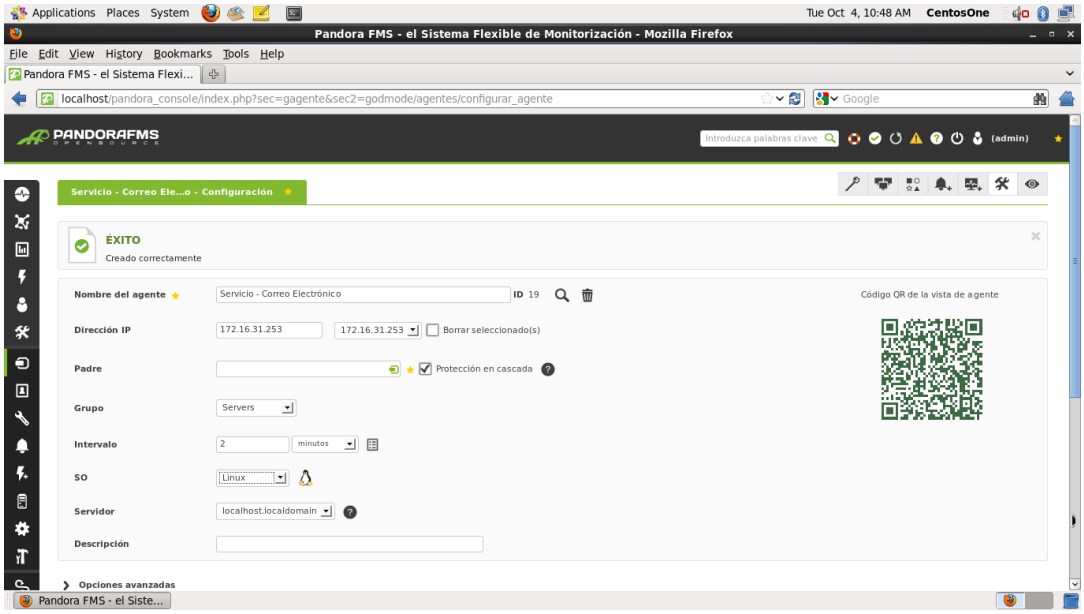


Figura 34. Creación de agentes para servicios TI

Fuente: Los autores.

Campos obligatorios:

Nombre de agente: en este recuadro escribiremos el nombre con el cual identificaremos al agente del dispositivo o servicio TI.

Dirección IP: en este recuadro escribiremos la dirección IP del dispositivo o servicio TI que deseamos monitorear.

Padre: En este recuadro escribiremos el IP o el nombre del agente para proteger por cascada o hacer herencia a un padre.

Grupo: es una lista desplegable donde elegiremos a que grupo pertenece, ejemplo: Aplicaciones, base de datos, servidores, etc.

Intervalo: en esta lista desplegable se puede elegir o en todo caso se puede, personalizar el intervalo de tiempo el cual monitorizará el agente.

SO: En esta lista desplegable elegiremos el sistema operativo de nuestro agente

Servidor: Este recuadro viene por defecto ya que es el instalado anteriormente en donde se registrará todos los incidentes.

Añadimos los demás dispositivos TI y Servicios TI

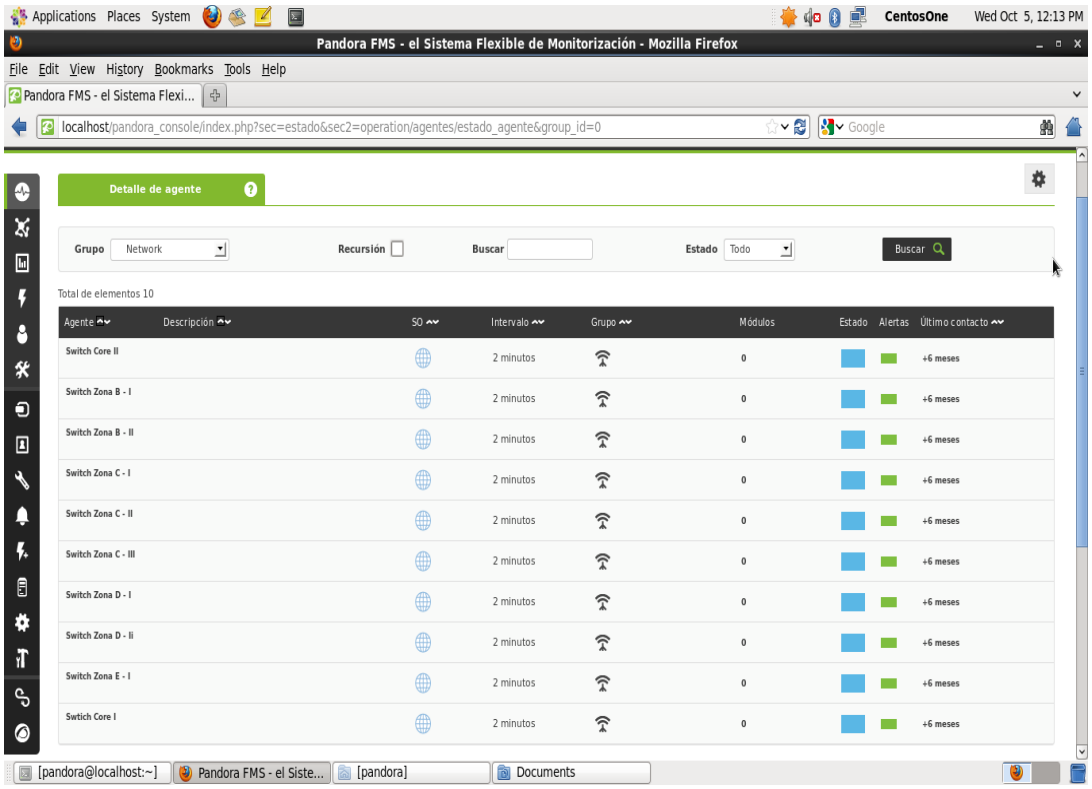


Figura 35. Dispositivos TI configurados

Fuente: Los autores.

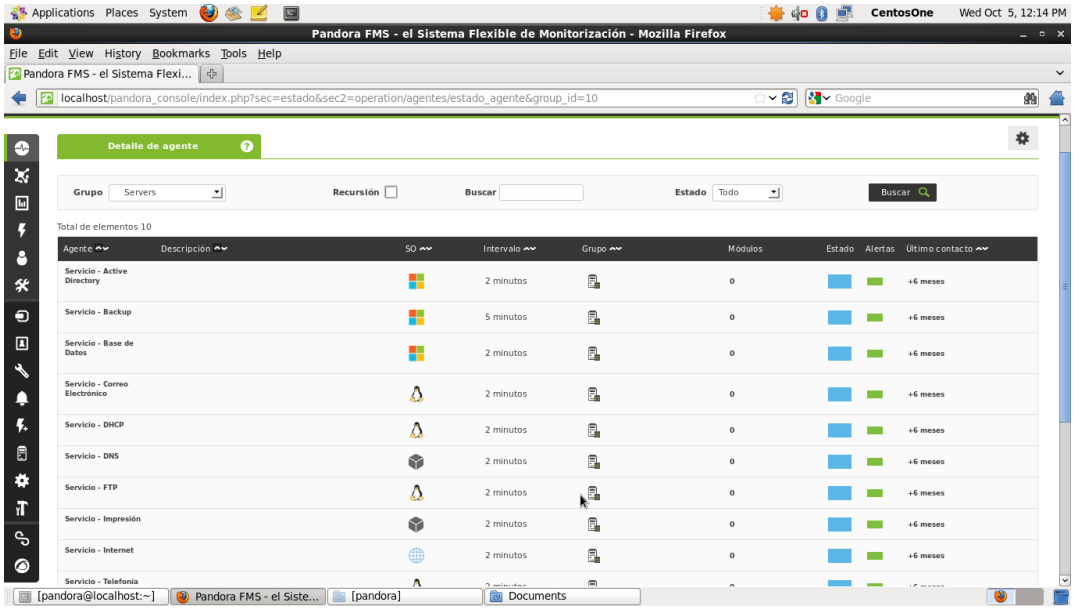


Figura 36. Servicios TI configurados

Fuente: Los autores.

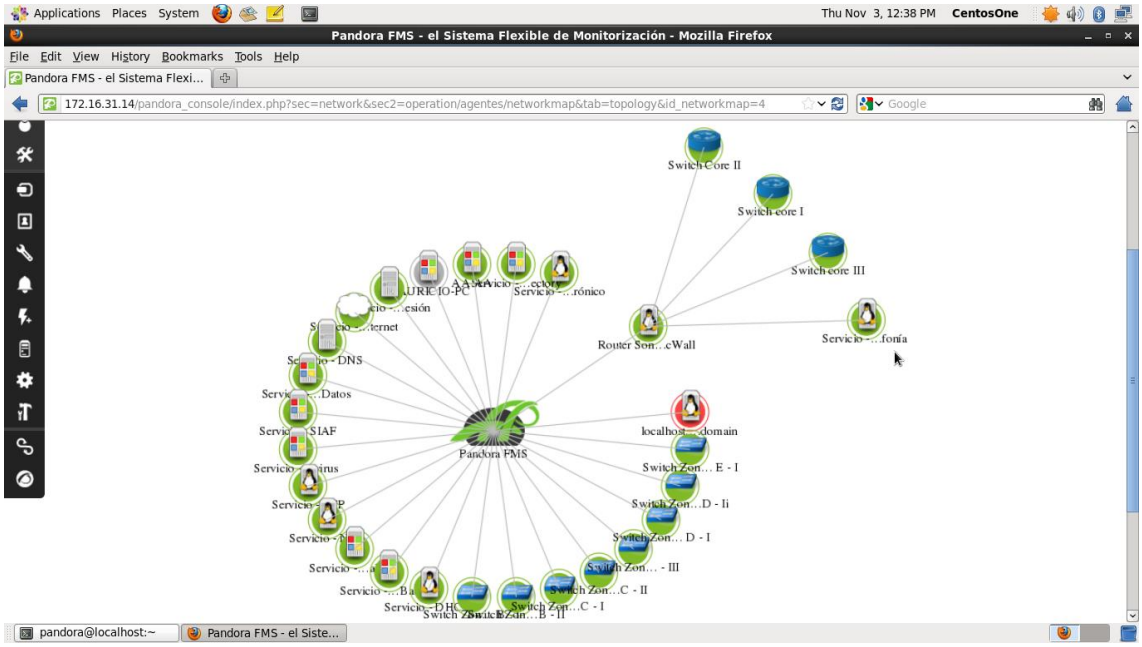


Figura 37. Vista topológica de los dispositivos monitoreados.

Fuente: Los autores.

Configuración de parámetros de monitoreo en los dispositivos.

Módulos para dispositivos de la infraestructura TI

En la parte izquierda ingresamos a **Gestión de Agentes,** podremos observar todos nuestros agentes creados anteriormente, elegiremos un agente, en este caso es el Switch Core III, luego hacemos clic en la pestaña módulos y obtendremos la siguiente pantalla:

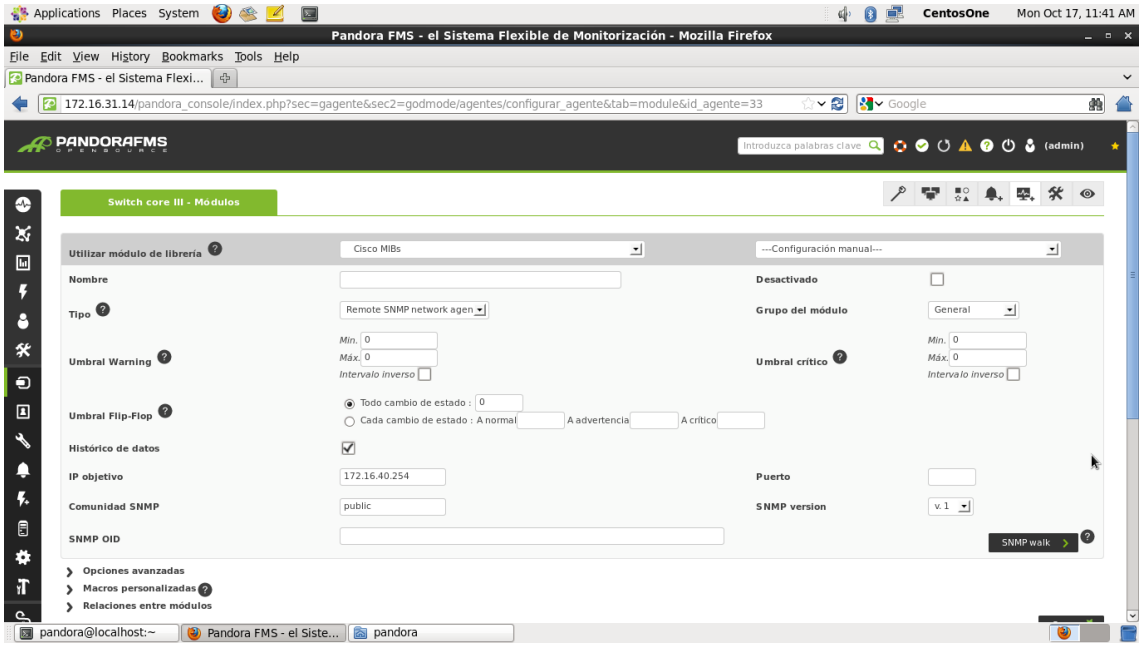


Figura 38. Configuración de agentes.

Fuente: Los autores.

Campos Obligatorios:

Librería de Módulos: Ésta lista desplegable nos permitirá elegir una plantilla predeterminada, pero no es recomendable usarla al 100 %, ya que, al iniciar el monitoreo por SNMP nos pedirá un OID, el cual, es un identificador de objetos y propio del dispositivo a monitorear.

En este caso elegimos Cisco Mibs, ya que, estamos configurando un Switch Cisco Catalyst 3560 de 24 puertos.

Nombre: Escribimos un nombre, el cual, identificamos en la tabla 22 (parámetros a monitorear)

Grupo del Módulo: Elegimos un grupo para éste módulo de monitoreo, ya sea, Sistema o System, Entorno o Enviroment o Red o Network, los cuales están establecidos en la tabla 22 (parámetros a monitorear)

Umbral Warning: Se editan parámetros para el estado de advertencia.

Umbral Crítico: Se editan parámetros para el estado crítico.

Umbral Flip Flop: Este campo indica que hasta que un elemento no esté al menos x veces en el mismo estado después de cambiar desde su estado original, no considere que haya cambiado.

Histórico de Datos: Al marcar esta casilla podremos guardar los incidentes y/o del agente monitoreado, así mismo, podremos generar reportes.

IP Objetivo: En este campo viene por defecto, heredado, del IP destino del dispositivo o servicio configurado en el agente, es a quien se le va agregar el módulo de monitorización.

Puerto: Puerto al cual haremos la consulta SNMP

Comunidad SNMP: Como vimos en el marco teórico del presente proyecto. La comunidad SNMP puede ser Public o Private. De acuerdo a la previa configuración del dispositivo TI por parte del administrador de redes.

SNMP VERSIÓN: Como vimos en el marco teórico del presente proyecto. La versión SNMP puede ser V1, V2, V2c y V3. De acuerdo a la previa configuración del dispositivo TI por parte del administrador de redes.

SNMP OID: En este campo podemos escribir el identificador de objeto de lo que queremos monitorear. Por ejemplo:

Para monitorear el Estado de Temperatura, su OID para Switch CISCO C 3560 es: .1.3.6.1.4.1.9.9.13.1.3.1.3.1005.

SNMP WALK:

Pandora FMS también tiene un examinador SNMP simple que permite hacer un «walk» de un dispositivo remoto a través de un SNMP walk.

Hacer un «walk» («SNMP Walk») sobre un dispositivo hará que todas sus variables MIB estén disponibles, para que pueda elegir una. También puede introducir una MIB usando un OID numérico o un formato comprensible por humanos, si tiene la MIB correcta instalada en su servidor de red de Pandora FMS**.**

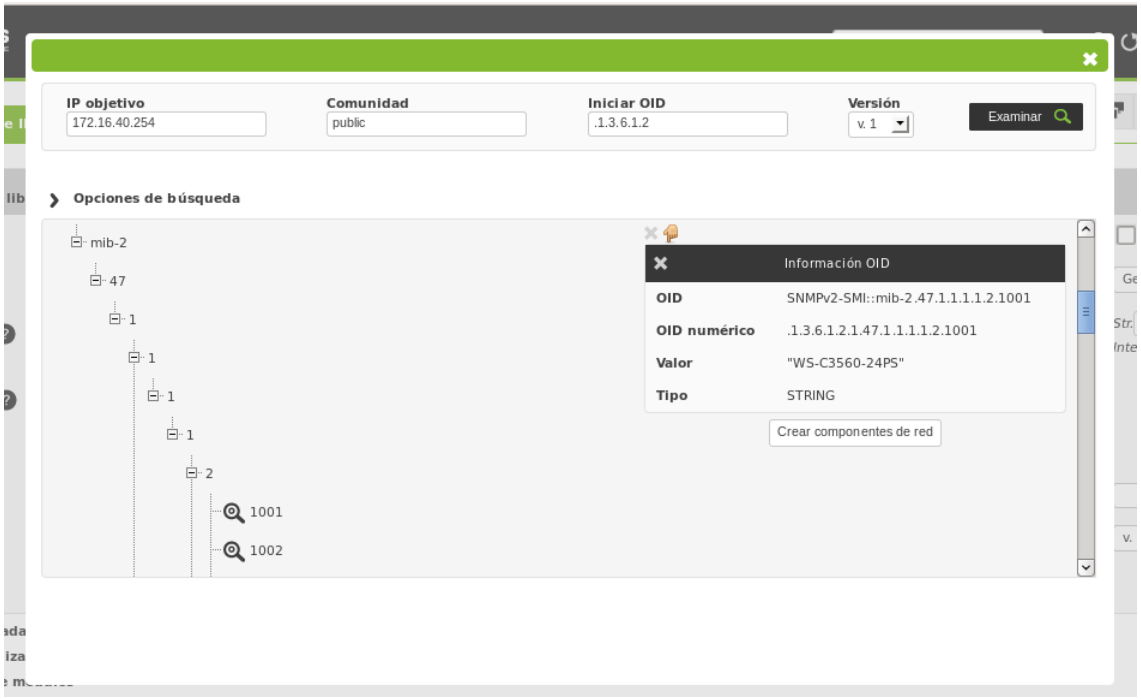


Figura 39. Snmp walk

Fuente: Los autores.

- **Para hacer un Walk necesitamos:**
    - **IP Objetivo:** Viene por defecto, pero también lo podemos corregir.
    - **Comunidad:** Puede ser Public o private previa consulta al administrador de redes.
    - **Iniciar el OID:** Se puede iniciar el OID o simplemente hacer clic en examinar para que haga su trabajo.
    - **Versión:** Puede ser V1, V2 o V3, previa consulta al administrador de redes.
- **Información OID**
    - **OID:** Nombre asignado por jerarquía.
    - **OID Numérico:** Número del OID
    - **Valor:** Nombre del OID

- **Tipo:** Puede ser String, Int o Alphanumeric. Nos sirve para saber cómo monitorear este módulo.

A continuación, presentamos los módulos asignados teniendo como referencia la tabla 27 de los parámetros a monitorear, los cuales, irán configurados en cada uno de los dispositivos TI, mencionados anteriormente en la tabla.

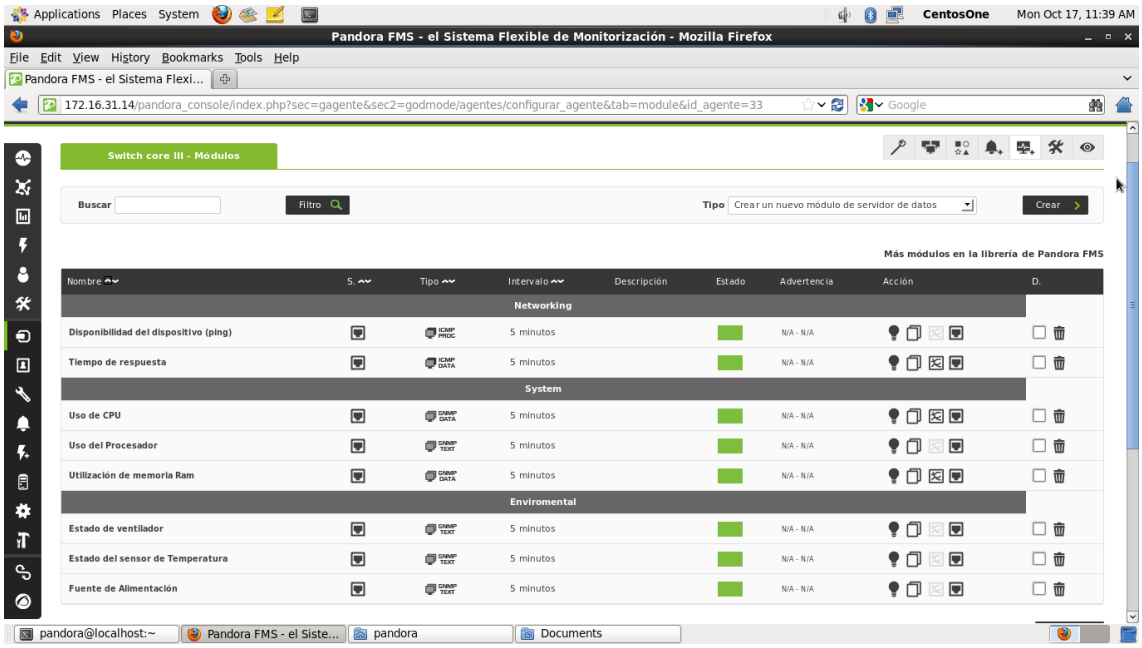


Figura 40. Parámetros críticos a monitorear configurados en Pandora FMS

Fuente: Los autores.

Módulos para Servicios de la infraestructura TI

Para configurar los módulos utilizaremos WMI, ya que, la mayoría de servidores donde se alojan estos servicios, están sobre sistema operativo WINDOWS.

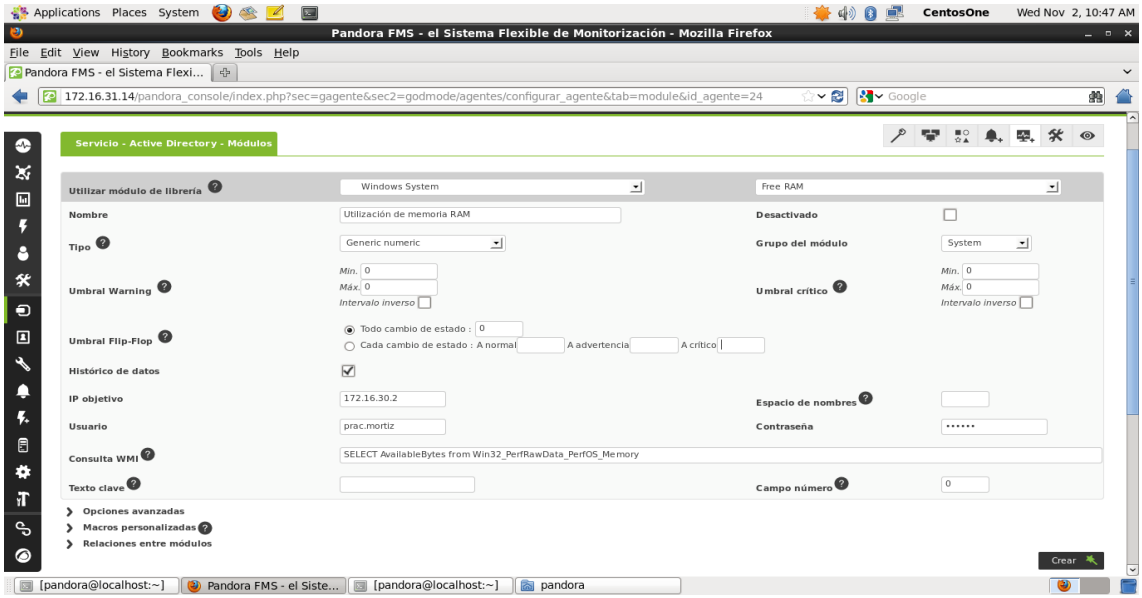


Figura 41. Configuración de WMI

Fuente: Los autores.

Donde:

Utilizar módulo de Librería: En Pandora FMS viene pre-configurado las herramientas a monitorear más utilizadas por los usuarios en este caso Free Ram, monitorea la utilización de la memoria ram.

Nombre: En este campo escribiremos el nombre que queremos para nuestro módulo de monitoreo

Tipo: En este campo elegiremos de la lista desplegable el dato que vamos a obtener al monitorear el módulo.

Grupo: En este campo elegiremos de la lista desplegable el grupo al cual pertenecerá el modulo a monitorear, entre los cuales definimos anteriormente, Sistema (System), Entorno (Enviroment) y Red (Network).

Umbral Warning – Umbral Critical: En este campo escribiremos los parámetros mínimos y máximos lo cuales nos servirán para monitorear el estado de emergencia y el estado crítico del módulo,

Umbral Flip – Flop: se utiliza para "filtrar" los continuos cambios de estado en la creación de eventos/estados, para que pueda indicar a Pandora FMS que hasta que un elemento no esté al menos x veces en el mismo estado después de cambiar desde su estado original, no considere que haya cambiado.

Histórico de Datos: Este casillero debemos de marcarlo para que podamos obtener reportes del módulo más adelante.

IP Objetivo: IP del módulo el cual vamos a monitorear.

Usuario y Password: Necesitamos un usuario a nivel administrador o que pueda tener acceso a consultas WMI, para el presente proyecto, se necesita solo un usuario al cual se le asigne permisos para consultas WMI.

Consulta WMI: Cualquier consulta WQL válida. Según Microsoft, el lenguaje de consultas WMI (WQL) es un subconjunto del estándar ANSI SQL (American National Standards Institute Structured Query Language), con mínimos cambios semánticos para soportar WMI.

Ejemplo: SELECT FreeSpace FROM Win32_LogicalDisk WHERE DeviceID = _VOLUME_ID_

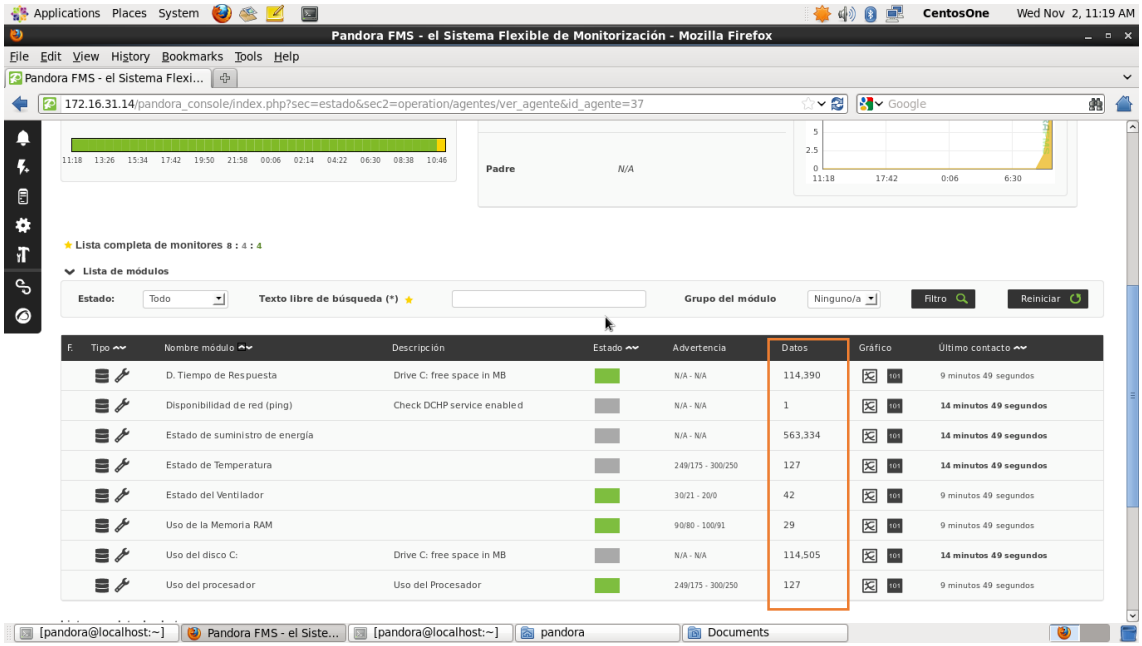


Figura 42. Datos obtenidos por WMI

Fuente: Los autores.

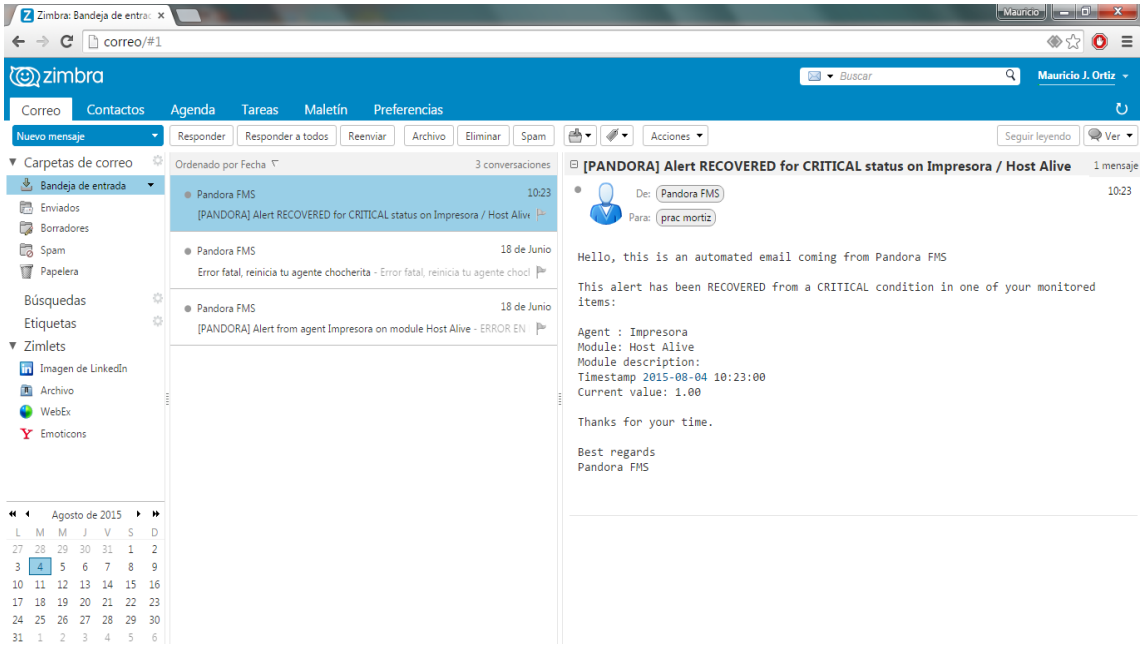


Figura 43. Alertas por correo electrónico institucional

Fuente: Los autores.

5.3. VERIFICACIÓN

Finalizada la fase de implementación del presente proyecto se procede con la fase de verificación del modelo PDCA que comprueba el cumplimiento de los objetivos de monitoreo por parte del sistema de monitoreo. En este caso los objetivos de monitoreo que se definieron en la fase de análisis se reiteran en la tabla N° 23.

Tabla 24: Fase de verificación del modelo PDCA

OBJETIVO	DESCRIPCIÓN	CUMPLIMIENTO EN EL MONITOREO
O1	Lograr la provisión de servicios informáticos, sistemas de información, informática y telemática, en el ámbito institucional.	✓
O2	Lograr que los usuarios internos y externos tengan disponibilidad de asesoría y asistencia técnica en el uso de aplicaciones informáticas y las nuevas tecnologías de la administración.	✓
O3	Lograr la provisión de servicios de información de Telecomunicaciones	✓
O4	Lograr que los usuarios internos y externos tengan la disponibilidad de asistencia técnica, en el uso de aplicación de Telecomunicaciones.	✓
O5	Mantener comunicación permanente con las instituciones afines	✓
O6	Brindar servicios de TI altamente disponibles, con el fin de apoyar los procesos operativos de los usuarios, basados en la comunicación, conectividad con los recursos de la infraestructura de TI y acceso seguro y confidencial a las áreas pertinentes de cada área	✓

Nota. Fuente: Los autores.

De acuerdo a lo implementado y a los requerimientos de monitoreo para el presente proyecto, el sistema de monitoreo seleccionado permitió la implementación completa de todos los parámetros de monitoreo. Para la siguiente fase, no se remiten carencias que deban corregirse.

5.4. OPTIMIZACIÓN

Todos los objetivos pudieron ser implementados, por ende, en la fase de verificación no se encontraron carencias para ser tratadas en esta fase. Tabla N° 22.

Tabla 25: Fase de Optimización modelo PDCA

OBJETIVO	DESCRIPCIÓN	RESULTADO	OBSERVACIÓN
O1	Lograr la provisión de servicios informáticos, sistemas de información, informática y telemática, en el ámbito institucional.	IMPLEMENTADO EN LA MONITORIZACIÓN	NO HAY OBSERVACIONES PARA ESTE OBJETIVO
O2	Lograr que los usuarios internos y externos tengan disponibilidad de asesoría y asistencia técnica en el uso de aplicaciones informáticas y las nuevas tecnologías de la administración.	IMPLEMENTADO EN LA MONITORIZACIÓN	NO HAY OBSERVACIONES PARA ESTE OBJETIVO
O3	Lograr la provisión de servicios de información de Telecomunicaciones	IMPLEMENTADO EN LA MONITORIZACIÓN	NO HAY OBSERVACIONES PARA ESTE OBJETIVO

O4	Lograr que los usuarios internos y externos tengan la disponibilidad de asistencia técnica, en el uso de aplicación de Telecomunicaciones.	IMPLEMENTADO EN LA MONITORIZACIÓN	NO HAY OBSERVACIONES PARA ESTE OBJETIVO
O5	Mantener comunicación permanente con las instituciones afines	IMPLEMENTADO EN LA MONITORIZACIÓN	NO HAY OBSERVACIONES PARA ESTE OBJETIVO
O6	Brindar servicios de TI altamente disponibles, con el fin de apoyar los procesos operativos de los usuarios, basados en la comunicación, conectividad con los recursos de la infraestructura de TI y acceso seguro y confidencial a las áreas pertinentes de cada área	IMPLEMENTADO EN LA MONITORIZACIÓN	NO HAY OBSERVACIONES PARA ESTE OBJETIVO

Nota. Fuente: Los autores.

CAPITULO V

RESULTADOS Y DISCUSIÓN

En este capítulo se presentan los resultados y discusión que se obtuvo luego de la realización de encuestas y cuestionarios a la muestra del presente proyecto. A continuación, se presentan los resultados y seguidamente las discusiones.

6.1. Procesamiento y análisis de datos

6.1.1 Tiempo de respuesta

Media:

Antes de la implementación:

$$\mu = \frac{68 + 10 + 20 + 2}{4} = 25$$

Después de la implementación:

$$\mu = \frac{80 + 19 + 1}{3} = 33.3$$

Varianza:

Antes de la implementación:

$$\sigma^2 = \frac{68^2 + 10^2 + 20^2 + 2^2}{4} - 25^2 = 657$$

Después de la implementación:

$$\sigma^2 = \frac{80^2 + 19^2 + 1^2}{3} - 33.3^2 = 1145.11$$

6.1.2 Exactitud al encontrar el fallo o incidencia

Media:

Antes de la implementación:

$$\mu = \frac{5 + 10 + 70 + 15}{4} = 25$$

Después de la implementación:

$$\mu = \frac{100 + 0 + 0}{3} = 33.3$$

Varianza:

Antes de la implementación:

$$\sigma^2 = \frac{5^2 + 10^2 + 70^2 + 15^2}{4} - 25^2 = 687.5$$

Después de la implementación:

$$\sigma^2 = \frac{100^2 + 0^2 + 0^2}{3} - 33.3^2 = 2224.44$$

6.1.3 Satisfacción del cliente

Media:

Antes de la implementación:

$$\mu = \frac{1 + 20 + 70 + 5 + 4}{5} = 20$$

Después de la implementación:

$$\mu = \frac{20 + 80 + 0 + 0 + 0}{5} = 20$$

Varianza:

Antes de la implementación:

$$\sigma^2 = \frac{1^2 + 20^2 + 70^2 + 5^2 + 4^2}{5} - 20^2 = 668.4$$

Después de la implementación:

$$\sigma^2 = \frac{20^2 + 80^2 + 0^2 + 0^2 + 0^2}{5} - 20^2 = 960$$

6.1.4 Confiabilidad

Media:

Antes de la implementación:

$$\mu = \frac{1 + 20 + 75 + 3 + 1}{5} = 20$$

Después de la implementación:

$$\mu = \frac{0 + 0 + 0 + 90 + 10}{5} = 20$$

Varianza:

Antes de la implementación:

$$\sigma^2 = \frac{1^2 + 20^2 + 75^2 + 3^2 + 1^2}{5} - 20^2 = 807.2$$

Después de la implementación:

$$\sigma^2 = \frac{0^2 + 0^2 + 0^2 + 90^2 + 10^2}{5} - 20^2 = 1240$$

6.1.5 Índice de quejas

Media:

Antes de la implementación:

$$\mu = \frac{4 + 8 + 3 + 7}{4} = 5.5$$

Después de la implementación:

$$\mu = \frac{2 + 0 + 0 + 2}{4} = 1$$

Varianza:

Antes de la implementación:

$$\sigma^2 = \frac{4^2 + 8^2 + 3^2 + 7^2}{4} - 5.5^2 = 4.25$$

Después de la implementación:

$$\sigma^2 = \frac{2^2 + 0^2 + 0^2 + 2^2}{4} - 1^2 = 1$$

6.2. Resultados de Indicadores de medición antes y después de la implementación.

6.2.1. Tiempo de Respuesta

Antes de la implementación

Tabla 26: Resultados Tiempo de Respesta - Antes de la implementación

Pregunta	30 min	1 hora	3 horas	24 hrs
Tiempo de respuesta	68%	10%	20%	2%

Nota. Fuente: Los autores.

Después de la implementación

Tabla 27: Resultados Tiempo de Respuesta - Antes de la implementación

Pregunta	0 a 10 MIN	11 a 40 MIN	41 MIN a 1 HORAS
Tiempo de respuesta	80%	19%	1%

Nota. Fuente: Los autores.

Como se puede observar en las tablas N°26 y N°27, el resultado del antes y después de la implementación del sistema de monitoreo de infraestructura TI con la implementación se ha reducido el tiempo de respuesta en la atención de incidencias en la red LAN del Hospital Regional de Cajamarca, ya que, el análisis de los datos nos indica que el parámetro mínimo de medición, antes de la implementación, era 30 minutos y el parámetro máximo de medición era 24 horas,

obteniendo una gran diferencia con la implementación, en donde, el parámetro mínimo de medición disminuyó de 0 a 10 minutos en una incidencia leve y el parámetro máximo de medición de este indicador disminuyó de 41 min a 1 hora en una incidencia grave según las encuestas realizadas.

En este indicador de medición (Tiempo de respuesta) podemos afirmar que la implementación es satisfactoria para la organización porque acortó el tiempo de respuesta 20 minutos menos en un incidente leve y 23 horas menos en un incidente grave aproximadamente.

6.2.2. Exactitud al encontrar la incidencia

Antes de la implementación:

Tabla 28: Resultados Exactitud al encontrar la incidencia - Antes de la implementación

Pregunta	30 min	1 hora	3 horas	5 horas
Exact. Al enc. La incidencia	5%	10%	70%	15%

Nota. Fuente: Los autores.

Después de la implementación:

Tabla 29: Resultados Exactitud al encontrar la incidencia - Después de la implementación

Pregunta	0 a 10 min	11 a 40 min	40 min A 1 hora
Exact. Al enc. La incidencia	100%	0%	0%

Nota. Fuente: Los autores.

Como se puede observar en las tablas N° 28 y N° 29, el resultado del antes y después de la implementación del sistema de monitoreo de infraestructura TI observamos que se ha reducido el tiempo en la exactitud a encontrar la incidencia en la red LAN del Hospital Regional de Cajamarca, ya que, el análisis de los datos nos indica que el parámetro mínimo de medición, antes de la implementación, era 30 minutos, el parámetro máximo de medición era 5 horas y el parámetro que según las encuestas obtenía el mayor porcentaje con un 70 % era un tiempo aproximado de 3 horas. Según los resultados de las encuestas después de la implementación obtenemos una gran diferencia, ya que, el parámetro mínimo de medición disminuyó de 0 a 10 minutos como máximo en un 100 % sea cual sea la incidencia, admitimos que en promedio es cada 10 minutos como máximo por qué depende del intervalo de monitoreo del servicio o dispositivo de la infraestructura TI asignado en la configuración del sistema de monitoreo.

En este indicador de medición (Exactitud al encontrar la incidencia) podemos afirmar que la implementación es satisfactoria para la organización porque acortó el tiempo de exactitud al encontrar la incidencia de 3 horas como promedio en 2 horas y 50 minutos menos aproximadamente.

6.2.3. Satisfacción de los clientes

Antes de la implementación:

Tabla 30: Resultados Satisfacción del cliente - Antes de la implementación

Pregunta	Excelente	Bueno	Regular	Malo	Pésimo
Satisf. Del cliente	1%	20%	70%	5%	4%

Nota. Fuente: Los autores.

Después de la implementación:

Tabla 31: Resultados Satisfacción del cliente – Después de la implementación

Pregunta	Excelente	Bueno	Regular	Malo	Pésimo
Satisf. Del cliente	20%	80%	0%	0%	0%

Nota. Fuente: Los autores

Como se puede observar en las tablas N° 30 y N° 31, el resultado del antes y después de la implementación del sistema de monitoreo de infraestructura TI se ha aumentado el porcentaje de satisfacción por parte del cliente de "Regular" a "Bueno" y "Excelente" en la atención de incidencias en la red LAN del Hospital Regional de Cajamarca, ya que, el análisis de los datos nos indica que antes de la implementación el 70% de los que atienden las incidencias del Hospital calificaban el mecanismo actual como "Regular", así mismo, estos mismos usuarios calificaron al sistema de monitoreo de infraestructura TI una vez implementado, como "Bueno" con un 80% y se atrevieron a decir que el nuevo mecanismo de monitoreo es "Excelente" con un 20%. Por lo que, hemos eliminado el 10 % que calificaba al mecanismo antiguo como "Pésimo" (5%) y "Malo" (5%) respectivamente, cambiando su opinión por "Bueno" y/o "Excelente" en la última encuesta realizada después de implementar el sistema de monitoreo.

En este indicador de medición (Satisfacción del Cliente) podemos afirmar que la implementación es satisfactoria para la organización por qué aumenta la satisfacción de nuestros clientes-usuarios los cuales trabajan eficazmente en la atención de incidentes en la red LAN del Hospital Regional de Cajamarca

6.2.4. Índice de producción

Resultados Antes de la implementación:

N° de incidencias promedio: 05

N° de incidencias atendidas promedio: 02

Índice de producción = 2.5

Resultados Después de la implementación:

N° de incidencias promedio: 08

N° de incidencias atendidas promedio: 08

Índice de producción = 1

Tabla 32: Resultados Índice de producción.

Indicador	Medidor	Estado	Valor Min	Valor Max	Semáforo
Índice de producción	Número de incidencias / número de incidencias atendidas	Bueno	> 0	< 1.99	
		Regular	>2	<2.99	
		Malo	> 3		

Nota. Fuente: Los autores

Como se puede observar los resultados obtenidos, del antes y después de la implementación del sistema de monitoreo de infraestructura TI se ha logrado mejorado el índice de producción (tabla N°30), de los usuarios encargados de atender las incidencias, ya que, al principio según las encuestas se daban 5 incidencias diarias de las cuales solo eran atendidas 2 aproximadamente y según la fórmula simple para hallar el índice de productividad, obtuvimos un 2.5 que según el recuadro se encontraba en estado “Regular” (color Ámbar según el

semáforo). Una vez instalado el sistema de monitoreo de infraestructura TI, obtuvimos según las encuestas que se daban 8 incidencias diarias (Para recalcar porque se dan más incidencias que antes de implementar el sistema de monitoreo es por que anteriormente solo se sabía de una incidencia si el usuario la encontraba, a diferencia de ahora que salta la alerta e informa automáticamente) y se atienden todas, con un promedio de índice de producción de 1 pero jamás sobre para el 1.99, por lo que, el estado de índice de producción es "Bueno" (color verde según el semáforo).

En este indicador de medición (Índice de producción) podemos afirmar que la implementación es satisfactoria para la organización por qué ha mejorado el índice de producción que en un inicio era "Regular" y ahora es netamente de estado "Bueno" por lo que los usuarios trabajan eficazmente en la atención de incidentes en la red LAN del Hospital Regional de Cajamarca

6.2.5. Confiabilidad

Antes de la implementación:

Tabla 33: Resultados Confiabilidad – Antes de la implementación

Pregunta	Nunca	A veces	Casi siempre	Siempre	Totalmente
Confiabilidad	1%	20%	75%	3%	1%

Nota. Fuente: Los autores

Después de la implementación:

Tabla 34: Resultados Confiabilidad – Después de la implementación

Pregunta	Nunca	A veces	Casi siempre	Siempre	Totalmente
Confiabilidad	0%	0%	0%	90%	10%

Nota. Fuente: Los autores

Como se puede observar en las tablas N° 33 y N° 34, el resultado del antes y después de la implementación del sistema de monitoreo de infraestructura TI se ha aumentado el porcentaje de confiabilidad por parte del cliente-usuario de "Casi Siempre" a "Siempre" y "Totalmente" en la atención de incidencias en la red LAN del Hospital Regional de Cajamarca, ya que, el análisis de los datos nos indica que antes de la implementación el 75% de los que atienden las incidencias del Hospital confiaban el mecanismo actual "Casi Siempre", así mismo, estos mismos usuarios confían en el sistema de monitoreo de infraestructura TI "Siempre" con un 90% y se atrevieron a decir que pueden llegar a confiar "Totalmente" un 10%. Por lo que, hemos eliminado el 21 % que no confiaban en el mecanismo antiguo con un "Nunca" (1%) y "A veces" (20%) respectivamente, cambiando su opinión por "Siempre" y/o "Totalmente" en la última encuesta realizada después de implementar el sistema de monitoreo.

En este indicador de medición (Confiabilidad) podemos afirmar que la implementación es satisfactoria para la organización por qué aumenta el porcentaje de confiabilidad de nuestros clientes-usuarios los cuales pueden trabajar eficazmente en la atención de incidentes en la red LAN del Hospital Regional de Cajamarca

6.2.6. Índice de quejas

Antes de la implementación:

Tabla 35: Resultados Índice de Quejas – Antes de la implementación

Pregunta	1 semana	2 semana	3 semana	4 semana
Índice de quejas	4	8	3	7

Nota. Fuente: Los autores

Después de la implementación:

Tabla 36: Resultados Índice de Quejas – Después de la implementación

Pregunta	1 semana	2 semana	3 semana	4 semana
Índice de quejas	2	0	0	2

Nota. Fuente: Los autores

Como podemos observar en las tablas N° 35 y N° 36, el resultado del antes y después de la implementación del sistema de monitoreo de infraestructura TI se ha disminuido el índice de quejas de nuestros usuarios encargados de atender las incidencias, ya que, al principio según las encuestas generaban un promedio de 5 a 6 quejas por mes del servicio de atención de incidentes brindado por los usuarios del área. Una vez instalado el sistema de monitoreo de infraestructura TI, obtuvimos según las encuestas que se genera un promedio de 1 a 2 quejas máximas del servicio de atención de incidencia).

En este indicador de medición (Índice de quejas) podemos afirmar que la implementación es satisfactoria para la organización por qué ha disminuido el índice de quejas que en un inicio era 5 a 6 quejas y ahora no pasan de 2 quejas por

mes, por lo que, lo que los usuarios trabajan eficazmente en la atención de incidentes en la red LAN del Hospital Regional de Cajamarca

6.2.7. Nivel de aceptación por parte de usuario final

¿Califique usted nuestro nivel de gestión de incidencias?

Realizamos la evaluación respectiva obteniendo como datos lo siguiente:

Tabla 37: Resultados Nivel de aceptación por parte de usuario final– Antes de la implementación

	Votos	Frecuencia relativa(Fi)	Frecuencia Absoluta (Hi)	Porcentaje
Buena	10	10	0.13	13%
Regular	25	35	0.44	44%
Mala	45	80	1	100%
Total	80			

Nota. Fuente: Los autores

- Según la evaluación respectiva solo obtuvimos un 13% de nivel de aceptación a nuestra gestión de incidencias.

Realizamos la segunda evaluación después de la implementación obteniendo como datos lo siguiente:

Tabla 38: Resultados Nivel de aceptación por parte de usuario final – Después de la implementación

	Votos	Frecuencia relativa(Fi)	Frecuencia Absoluta(Hi)	Porcentaje
Buena	69	69	0.86	86%
Regular	9	78	0.11	11%
Mala	2	80	0.03	3%
Total	80			

Nota. Fuente: Los autores

- Obtuvimos como resultado un nivel de aceptación a la gestión de incidencias de un 86% porciento dejando de lado en resultado anterior, con el cual podemos determinar que el sistema de gestión de incidencias de infraestructura TI influye de manera positiva en dicha gestión.

Tabla 39: Resultados Nivel de aceptación por parte de usuario final

	Antes		después	
	Votos	Porcentaje	Votos	Porcentaje
Buena	10	13%	69	86%
Regular	25	31%	9	11%
Mala	45	56%	2	3%
Total	80	100%	80	100%

Nota. Fuente: Los autores

7.1.Discusión

Los resultados de la presente investigación comprueban la hipótesis propuesta en la elaboración del proyecto de tesis, donde se afirma que el sistema de monitoreo de infraestructura TI influye de manera positiva en la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca.

Esta hipótesis se relaciona con los resultados obtenidos por Víctor Arrebola Real (2013) en su proyecto “Sistema de monitorización de servidores Linux” donde afirma que la tecnología de desarrollo de páginas Web ha crecido mucho durante los últimos años, haciendo que la programación de estas sea mucho más fácil obteniendo resultados mucho más interesantes y positivos para el usuario final. Aun así, la linealidad aún es demasiado grande, aunque cada vez está más

implantada la programación orientada a objetos, lo que nos aporta una mayor potencia y flexibilidad. La satisfacción una vez finalizado el mismo es indescriptible, tanto por el resultado, como por la cantidad de conocimientos adquiridos. Por lo tanto, la valoración final es muy positiva, dado que se han cumplido en mayor o menor medida todos los objetivos establecidos inicialmente, además de algunos que han ido surgiendo sobre la marcha durante el desarrollo del sistema.

Asimismo, Evelyn Valdez Zamora (2013) en su proyecto "Gestor automático de eventos en servidores mediante el uso de una matriz de escalamiento, propuesta basada en software open source" obtiene de los resultados que mediante esta herramienta el usuario puede analizar el comportamiento de cada uno de los servidores, desde cualquier lugar, ya que puede acceder desde su celular o recibir alertas por el mismo medio, sin necesidad de estar todo el tiempo observando la pantalla de su monitor. De esta manera nos ayuda a atender en el menor tiempo posible los incidentes y nos evita que las operaciones y los procesos normales de nuestra empresa se detengan, ahorrando grandes cantidades de recursos como económicos, humanos y de tiempo. Estos resultados, detallan la influencia positiva que genera un sistema de monitoreo de infraestructura TI en una organización.

Y por último, Barriga Martínez Edison Lennin (2013) en su proyecto "Análisis e implementación de un sistema de manejo de incidentes con funcionalidad extendida notificación de correo electrónico bajo gnu/Linux aplicado a los servidores y enlaces LAN y WAN de la empresa Edesa S.A." obtiene de los

resultados que la implementación y configuración de un servidor de monitoreo mantiene al administrador de red informado del comportamiento de los enlaces de la red tanto LAN como WAN, además de tener un histórico de los trabajos realizado como memoria para solventar futuros problemas de manera rápida y efectiva, garantizando el servicio de la red. El servidor de monitoreo permite al administrador mantenerse informado del estado de los enlaces y servidores mediante el envío de alertas por correo electrónico a los miembros del departamento de Tecnologías de la Información (TI). Estos resultados detallan y afirman que un sistema de monitoreo influye positivamente en la organización.

Como podemos observar los resultados identificados anteriormente con los resultados obtenidos en el presente proyecto guardan cierta similitud y/o cambia la sintaxis pero terminan siendo los mismo, por lo que, podemos afirmar que un sistema de monitoreo de infraestructura TI influye de manera positiva a la gestión de incidencias de una organización, para efecto del presente proyecto en el Hospital Regional de Cajamarca, acortando los tiempo de respuesta para atender una incidencia, disminuye el tiempo para encontrar la incidencia o fallo en la infraestructura TI, mejorando la calidad de servicio brindado por el área de TI, aumentando la confiabilidad por parte de los usuarios en el mecanismo de monitoreo de la infraestructura TI, disminuyendo el índice de quejas por parte de los clientes al área de TI y mejorando la productividad de los colaboradores encargados del monitoreo y gestión de incidencias.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones que se obtuvieron luego de la realización del presente proyecto. A continuación, se presentan las conclusiones y seguidamente las recomendaciones.

8.1.Conclusiones

Se realizó la comparación entre dos sistemas de monitoreo de infraestructura TI (Zabbix y Pandora FMS) de las cuales se seleccionó Pandora FMS como el sistema de monitoreo por sus características de moldeo al entorno del hospital regional de Cajamarca la cual se elijo por las siguientes razones:

Pandora FMS se podrá adaptar al mismo y no sólo darte la visión que necesitas, sino que podrá crecer a la vez que las necesidades de tu organización.

- Pandora FMS es capaz de integrar todo tipo de elemento o componente en su monitorización.
- Podrás monitorizar hasta 100.000 elementos con un mismo servidor.
- Podrás geo localizar tus componentes.
- Los paneles son altamente personalizables y adaptables al perfilado de cada usuario. Sabemos que un CEO no tiene que ver lo mismo que el administrador de redes.
- Integra todos tus sistemas en una misma herramienta.

Se implementó el sistema de monitoreo para poder mapear toda la red LAN del hospital regional de Cajamarca, se realizó la identificación de todos los parámetros críticos correspondientes los cuales estarán siempre monitoreados para

mantener sus operatividad y disponibilidad de cada uno de estos servicios y/o equipos conectados a la Red LAN del HRC.

Se implementó el sistema de alertas a través de correo electrónico, el cual el sistema enviará un mail de manera automática a los encargados del departamento de sistemas del HRC, si se está presentando una incidencia dentro de la red LAN del HRC el cual deberá de ser atendida de manera oportuna para que no gerente ningún tipo de inconveniente dentro de las actividades de los usuarios finales.

Por último, podemos afirmar que la implementación del sistema de monitoreo de TI incidió positivamente en la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca porque logró satisfacer las necesidades y/o requerimientos de los clientes en el proceso de atención a incidencias, por distintos puntos de medición que se realizó y puede decir que:

Se determinó que la implementación del sistema de monitoreo de infraestructura TI influyó de manera positiva en la gestión de incidencias de la red LAN del Hospital Regional de Cajamarca porque mejoró los tiempos de respuesta, el tiempo en encontrar una incidencia, la confiabilidad en el mecanismo de atención de incidencias y el índice de producción del personal encargado y disminuyó el índice de quejas.

La utilización del sistema de monitoreo utilizando la red del Hospital obtuvo una visión detallada en tiempo real de los dispositivos monitoreados, especificando sus principales parámetros de monitoreo los cuales son: Sistema, Entorno y red.

Adicional a esto la implementación del sistema propuesto acorde con las necesidades del área Informática del Hospital se debió a la elección de un sistema de monitoreo flexible, fácil de instalar y con una interfaz amigable lo cual implicó la implementación del sistema de monitoreo Pandora FMS, el cual, nos ayudó a identificar los parámetros críticos de monitoreo, los dispositivos y servicios a monitorear, y generación de alertas ante una posible incidencia para mantener al encargado de la red informado en tiempo real.

9.1.Recomendaciones

- Para trabajar con un sistema de monitoreo de TI open source, se recomienda tener conocimientos avanzados en comandos y del sistema operativo Linux que se elija, ya que, éste sistema de monitoreo al ser libre y de código abierto necesita de un ambiente que sea semejante para evitar problemas con las licencias.
- En la configuración diaria en Linux se recomienda no trabajar como usuario root, ya que, éste tiene todos los privilegios sobre el sistema y se puede realizar alguna modificación que afecte el sistema.
- Para la administración del sistema de monitoreo de TI se recomienda crear usuarios y contraseñas con alto nivel de seguridad, ya que, si un intruso accede como administrador puede malograr el sistema e inclusive los dispositivos y/o servicios monitoreados por el acceso que se tiene mediante telnet o ssh.

- Se recomienda instalar PhpMyAdmin, para favorecer el entendimiento y la configuración de la base de datos, que en este caso está en Mysql y solo se accede a ella mediante terminal Linux.
- Se recomienda que la contraseña de root de la Base de Datos, sea de alto nivel de seguridad porque éste usuario tiene permisos sobre toda la información que se almacena en el sistema de monitoreo de TI.
- No confiar en foros que no sean netamente de Pandora FMS, ya que, según la presente investigación la mayoría de los sitios consultados, dan información errónea.
- Se recomienda contratar un operador que visualice en tiempo real el sistema de monitoreo de TI e informe de posibles incidentes para aumentar la eficacia del sistema.

BIBLIOGRAFÍA

AJPDSOFT (2010). *Enciclopedia Definición WMI.* Murcia (España): Proyecto Ajpdsoft. Recuperado el 30 de agosto 08 de 2016 de http://www.ajpdsoft.com/modules.php?name=News&file=article&sid=477#wmi

CISCO Systems, Inc. (2009). *Best Practices for Monitoring CISCO Unified*. Contact Center Enterprise with CISCO Unified Operations Manager. Recuperado el 5 de noviembre de 2016, de http://www.CISCO.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/white_paper_c11-543550.html#wp9000677

Dineley, D., Borck, J., Martin Heller, Venezia, P. y Mobley, H. (2013). *Bossie Awards 2014: The best open source networking software*. INFOWORLD. Recuperado el 16 de septiembre del 2016, de http://www.infoworld.com/d/open-source/bossie-awards-2010-the-best-open-source-networking-software-153?Source=rs

Dineley, D., Borck, J., Martin Heller, Venezia, P. y Mobley, H. (2014). *Bossie 2010 winner: Pandora FMS*. INFOWORLD. Recuperado el 16 de septiembre del 2016 de http://www.infoworld.com/d/open-source/bossie-awards-2010-the-best-opensourc e -networking-software-153&current=2&last=1#slideshot

Gonzales Mendez, M. (2011). *Propuesta de un modelo de implantación para un sistema de monitoreo de Infraestructura TI.* (Tesis de grado) Universidad Simon Bolivar.

Holub, E (2009). *ITIL and IT Operations Optimization.* GARTNER GROUP. Recuperado el 2 de septiembre del 2016 desde http://www.gartner.com/it/content/992200/992214/june17_itil_itoperations_ed_holub_final.pdf

IDG, (2010). *About IDG*. IDG. Recupeardo el 25 de septiembre del 2016 de http://www.idg.com/www/HomeNew.nsf/docs/about_IDG#

InfoWorldBossies, (2010). *InfoWorld Bossies (Best of Open Source Software).* INFOWORLD. Recuperado el 22 de septiembre del 2016 de http://www.infoworld.com/infoworld-bossie-awards-755

Internet Control Message Protocol (ICMP). (2013). Erg.abdn.ac.uk. Recuperado el 30 agosto de 2016, desde http://www.erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/icmp.html

Janakiraman, B. y Gopal, R. (2006). *Total Quality Management: Text and Cases.* Prentice-Hall of India: New Delhi. Recuperado el 21 de agosto del 2016 de http://books.google.co.ve/books?id=-Ljyx785QvUC&pg=PA104&dq=Plan+do+check+act+cycle+deming+total+quality&hl=es&ei=fvqbTITNMP68Ab6_KCzAw&sa=X&oi=book_result&ct=bookthumbnail&resnum=1&ved=0CCsQ6wEwAA#v=onepage&q&f=false

Managing Windows with WMI. (2009). Msdn.microsoft.com. Recuperado el 30 de Agosto de 2016, desde https://msdn.microsoft.com/en-us/library/bb742445.aspx?f=255&MSPPError=-2147217396

LLC, Z. (2010). *Zabbix: The Enterprise-Class Open Source Network Monitoring Solution.* Zabbix.com. Recuperado el 4 Septiembre de 2016, de http://www.zabbix.com/

On premise monitoring software | Pandora FMS. (2008). Pandora FMS. Recuperado el 4 de septiembre de 2016, de https://pandorafms.com/

Pandora FMS, (2014). *El porqué de la monitorización hoy*. Recuperado el 25 de agosto desde 2016, de https://pandorafms.com/downloads/presentacion_pandora_2014-ES.pdf

Ravikanth Chaganti. (2009). *eBook: WMI Query Language via PowerShell*. Recuperado el 09 de Octubre de 2016 de http://www.ravichaganti.com/blog/?p=1979

Selley Rojas, H. (2008). *Monitoreo del Comportamiento de Servidores.* Tesis de grado. Centro de Investigación en computación, Instituto Politécnico Nacional - México D.F.

staff, I. (2014). *Bossie Awards 2014: The best open source application development tools.* InfoWorld. Recuperado el 2 septiembre de 2016, de http://www.infoworld.com/article/2687772/application-development/164642-Bossie-Awards-2014-The-best-open-source-application-developmenttools.html#slide3

Vara Horna, A. (2012). *Siete pasos para una tesis exitosa.* Recuperado el 10 de abril de 2017, desde http://www.administracion.usmp.edu.pe/wp-contnt/uploads/sites/9/2014/02/Manual_7pasos_aristidesvara1.pdf

Weill, P y Vitale, M, (2001*). Information Technology Infrastructure for E-Business. Massachusetts Institute of Technology*. Cambridge, Recuperado el 02 de septiembre del 2016, desde http://dspace.mit.edu/bitstream/handle /1721.1/48160/informationtechn00weil.pdf?sequence=1

Weill, P y Vitale, M, (2004). *Information Technology Infrastructure for E-Business.* Dspace.mit.edu. Recuperado el 19 de Agosto de 2016, desde http://dspace.mit.edu/bitstream/handle/1721.1/48160/informationtechn00weil.pdf?seq

Zabbix, (2014). *Zabbix Conference 2014*. Recuperado el 25 agosto de 2016, desde https://zabbix.com/2017/03/zabbix_supervision_conference_server/

LISTA DE ABREVIATURAS

BD: Base de datos**.**

CPU: Unidad central de procesos**.**

DNS: Sistema de nombres de dominio**.**

FMS: Sistema de monitoreo flexible.

FTP: Protocolo de Red para la Transferencia de Archivos

GPL: Licencia Pública General

HRC: Hospital Regional de Cajamarca

HTML: Lenguaje de marca de Salida de Hiper texto

HTTP: Protocolo de Transferencia de Hipertexto

ICMP: Protocolo de Mensajes de Control de Internet

ING: Ingeniero

IP: Protocolo de internet.

ISP: Proveedor de servicio de internet.

ITIL: Librería de Infraestructura de Tecnologías de Información

LAN: Red de área local.

NTP: Protocolo de tiempo de red.

MYSQL: Sistema de gestión de base de datos relacional, multihilo y multiusuario.

PHP: Preprocesador de Hipertexto.

SSH: Protocolo de Transferencia de Archivos Seguro.

SNMP: Protocolo Simple de Administración de Red.

SMTP: Protocolo para la Transferencia Simple de Correo Electrónico.

TCP: Protocolo de Transferencia de Archivos.

TI: Tecnologías de información.

URL: Localizador de Fuente Uniforme.

UPAGU: Universidad Privada Antonio Guillermo Urrelo.

WMI: Instrumentación Administrativa de Windows.

XML: Lenguaje de Marcas Extensible.

GLOSARIO

Apache: Este proyecto es un esfuerzo por desarrollar y mantener un servidor HTTP para los sistemas operativos modernos. El objetivo de este proyecto es proveer un servidor seguro, eficiente y extensible que provea servicios HTTP de acuerdo a los estándares actuales.

Base de datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su uso posterior.

Bash: Es un intérprete de comandos del proyecto GNU. Es un acrónimo de Bourne Again Shell, donde Bourne fue el primer intérprete de comandos importante en UNIX.

Bit: Acrónimo de Binary Digit, un bit es la unidad mínima en la numeración binaria y solo puede tomar el valor 1 ó 0.

Byte: Conjunto de ocho bits. Es el prefijo que se usa como base en combinación de otros prefijos de cantidad. Utilizado en computación y electrónica**.**

Cisco Systems: Empresa multinacional ubicada en San José California, Estados Unidos, dedicada principalmente a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicación.

Código abierto (Open Source): También llamado como Software Libre, es el término mediante al cuál se define a todas las aplicaciones computacionales que se desarrollan y distribuyen libremente. Todo el software desarrollado de esta forma brinda libertad de uso, instalación, modificación y redistribución.

CPU. (Central Processing Unit) Unidad Central de Procesamiento, se refiere al micro-procesador de una computadora el cuál se encarga de realizar todas las operaciones lógicas y aritméticas.

DHCP. (Dynamic Host Configuration Protocol): Protocolo de Configuración Dinámica de Host, es el protocolo que se encarga de asignar la configuración de red automáticamente a los clientes que se conecten a la red donde este se encuentre.

DNS. (Domain Name Server): Servidor de Nombres de Dominio. Este servidor se encarga de resolver los nombres de host solicitadas por los clientes y entregarle la dirección IP que corresponda para poder establecer una comunicación.

GPL. (General Public License): La Licencia Pública General de GNU, llamada comúnmente GNU GPL, la usan la mayoría de los programas de GNU y más de la mitad de las aplicaciones de software libre. Esta licencia otorga derechos de uso, instalación, modificación y redistribución, siempre y cuando se mantenga la licencia del software en cuestión.

Hardware: Se refiere a todos los componentes físicos (que se pueden tocar), en el caso de una computadora personal serían los discos, unidades de disco, monitor, teclado, la placa base, el microprocesador, etcétera

HTML. (HyperText Markup Lenguaje): El Lenguaje de Etiquetas de Híper Texto es el lenguaje de marcado predominante para la construcción de páginas Web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se

escribe en forma de "etiquetas", rodeadas por corchetes angulares (). HTML también puede describir, hasta un cierto punto, la apariencia de un documento, y puede incluir un script (por ejemplo, JavaScript), el cual puede afectar el comportamiento de navegadores Web y otros procesadores de HTML.

HTTP. (Hyper TexT Protocol): El Protocolo de Transferencia de Híper Texto es usado en cada transacción de la Web. Fue desarrollado por el consorcio W3C y la IETF. Define la sintaxis y la semántica que utilizan los elementos software de la arquitectura Web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

Infraestructura: Es el conjunto de dispositivos o servicios que están considerados como necesarios para que los procesos de una organización puedan funcionar o bien para que una actividad se desarrolle efectivamente.

Internet: Red mundial de computadoras con un conjunto de protocolos, siendo TCP/IP el más destacado. Aparece por primera vez en 1969, cuando ARPAnet establece su primera conexión entre tres universidades en California y una en Utah. Cuando se dice red de redes se hace referencia a que es una red formada por la interconexión de otras redes menores.

IP (Internet Protocol): Protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Linux: Es el nombre de un kernel desarrollado como software libre basado en Unix. Cuando es integrado con un conjunto de aplicaciones GNU se forma un sistema operativo llamado “distribución Linux/GNU”.

Monitoreo: consiste en la observación del curso de uno o más parámetros para detectar eventuales anomalías

LAN: Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

RAM (Random Access Memory): Compuesta por chips y se utiliza como memoria de trabajo para programas y datos. Es un tipo de memoria temporal que pierde sus datos cuando se queda sin energía, por lo cual es una memoria volátil.

Red: Hace referencia al conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios.

Sistema: Consiste en un software que sirve para controlar e interactuar con el sistema operativo, proporcionando control sobre el hardware y dando soporte a otros programas.

Software: Es el conjunto de los componentes intangibles de una computadora, es decir, el conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica

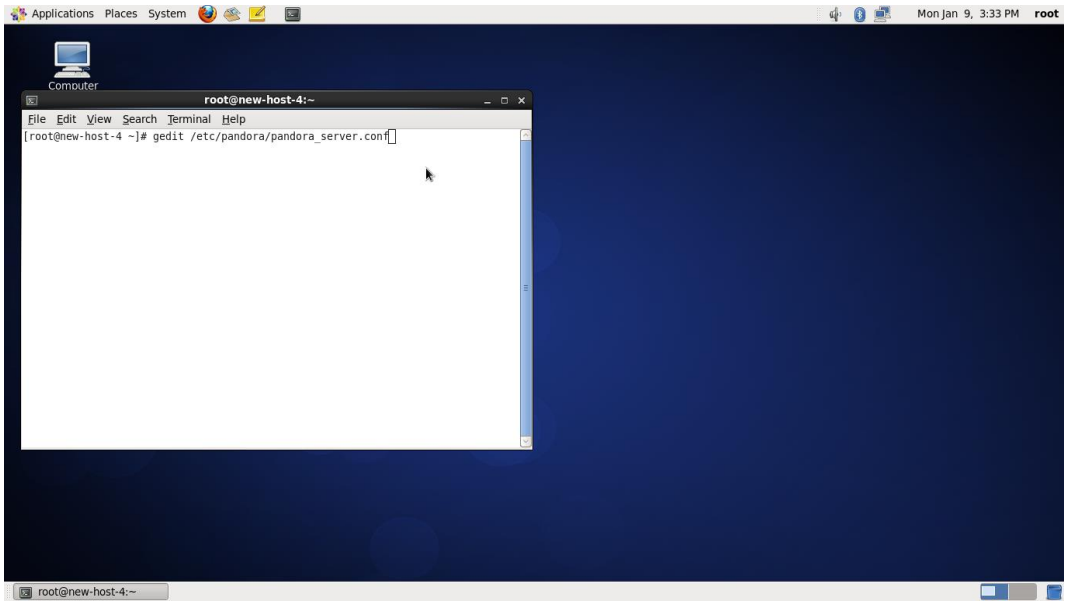
SSL: Protocolo criptográfico que proporciona comunicaciones seguras en Internet. Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

TCP (Transmission Control Protocol): Es uno de los protocolos fundamentales en Internet, fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP y SSH.

WWW (World Wide Web): Nombrado como "Web" solamente es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet. Con un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces

ANEXOS

ARCHIVO DE CONFIGURACIÓN DEL SERVIDOR DE PANDORA FMS.




```
##########################################################################
# Pandora FMS Server Parameters

# Pandora FMS, the Flexible Monitoring System.

# Version 6.0SP3

# Licensed under GPL license v2,

# (c) 2003-2014 Artica Soluciones Tecnologicas

# http://www.pandorafms.com

# Please change it for your setup needs

##########################################################################

# Servername: Name of this server

# if not given, it takes hostname. It's preferable to setup one
```

```
# because machine name could change by some reason.
# servername greystone
# incomingdir:  Defines directory where incoming data packets are stored
# You could set directory relative to base path or absolute, starting with /
incomingdir /var/spool/pandora/data_in
# log_file: Main logfile for pandora_server
# You could set file relative to base path or absolute, starting with /
log_file /var/log/pandora/pandora_server.log
# Log file for Pandora FMS SNMP console. Its generated by NetSNMP Trap daemon
snmp_logfile /var/log/pandora/pandora_snmptrap.log
# Error logfile: aux logfile for pandora_server errors (in Daemon mode)
# You could set file relative to base path or absolute, starting with /
errorlog_file /var/log/pandora/pandora_server.error
# daemon: Runs in daemon mode (background) if 1, if 0 runs in foreground
# this could be also configured on commandline with -D option
# daemon 1
# dbengine: mysql, postgresql or oracle (mysql by default)
dbengine mysql
# Database credentials. A VERY important configuration.
# This must be the same credentials used by your Pandora FMS Console
```

but could be different if your console is not running in the same

host than the server. Check your console setup in /include/config.php

dbname: Database name (pandora by default)

dbname pandora

dbuser: Database user name (pandora by default)

dbuser pandora

dbpass: Database password

dbpass pandora

dbhost: Database hostname or IP address

dbhost 127.0.0.1

dbport: Database port number

Default value depends on the dbengine (mysql: 3306, postgresql: 5432, oracle: 1521)

dbport 3306

By default, parent agent will not be updated

#update_parent 0

verbosity: level of detail on errors/messages (0 default, 1 verbose, 2 debug.... 10 noisy)

-v in command line (verbose) or -d (debug). Set this to 10 when try to locate problems and

set to 1 or 3 on production enviroments.

verbosity 3

Master Server priority. The running server with the highest master value will

be the master. Ties are broken at random. If set to 0, this server will

never become master.

master 1

Activate Pandora SNMP console (depending on snmptrapd)

snmpconsole 1

snmpconsole_threads: number of SNMP console threads for processing SNMP traps.

snmpconsole_threads 1

Attempt to translate variable bindings when processing SNMP traps. 1 enabled, 0 disabled. 0 by default. (ENTERPRISE ONLY).

translate_variable_bindings 0

Attempt to translate enterprise strings when processing SNMP traps. 1 enabled, 0 disabled. 1 by default. (ENTERPRISE ONLY).

translate_enterprise_strings 0

snmptrapd will ignore authenticationFailure traps if set to 1.

snmp_ignore_authfailure 1

snmptrapd will read the PDU source address instead of the agent-addr field is set to 1.

snmp_pdu_address 0

Path to the snmp_trapd binary. If set to manual, the server will not attemp to start snmp_trapd.

#snmp_trapd manual

Activate (1) Pandora Network Server

networkserver 1

```
# Activate (1) Pandora Data Server

dataserver 1

# Activate (1) Pandora FMS Recon server

reconserver 1

# pluginserver : 1 or 0. Set to 1 to activate plugin server with this setup

pluginserver 1

# Pandora FMS Plugin exec tool filepath (by default at /usr/bin)

plugin_exec /usr/bin/timeout

# predictionserver : 1 or 0. Set to 1 to activate prediction server with this setup

# DISABLED BY DEFAULT

predictionserver 0

# wmiserver : 1 or 0. Set to 1 to activate WMI server with this setup

# DISABLED BY DEFAULT

wmiserver 1

# Network timeout (in seconds) for timeout in network connections for Network agents

network_timeout 4

# Server keepalive (in seconds)

server_keepalive 45

# Server Threshold: defines number of seconds of main loop (in sec)

server_threshold 5
```

Network threads: Do not set too high (~40). Each threads make a network module check.

network_threads 4

icmp_checks x : defines number of pings for each icmp_proc module type. at least one of

that ping should be 1 to report 1. Setting this to 1 will make all icmp montioring faster but

with more probability of failure.

icmp_checks 3

Number of ICMP packets to send per request.

icmp_packets 1

tcp specific options :

tcp_checks: number of tcp retries if first attempt fails.

tcp_timeout: specific timeout for tcp connections

tcp_checks 1

tcp_timeout 10

snmp specific options :

snmp_checks: number of snmp request retries if first attempt fails.

snmp_timeout: specific timeout for snmp request.

snmp_checks 1

snmp_timeout 4

snmp_proc_deadresponse 1 (default): Return DOWN if cannot contact

or receive NULL from a SNMP PROC module.

snmp_proc_deadresponse 1

plugin_threads: Specify number of plugin server threads for processing plugin calls

plugin_threads 1

plugin_timeout: Specify number of seconds calling plugin exec waiting for response

after this time, call is aborted and result is "unknown".

plugin_timeout 12

wmi_timeout : specific timeout for wmi request.

wmi_timeout 7

wmi_threads: Specify number of WMI server threads for processing WMI remote calls

wmi_threads 1

recon_threads. Each thread will scan a different scantask.

recon_threads 1

dataserver_threads: Number of threads for data server (XML processing threads)

dataserver_threads 1

mta_address: External Mailer (MTA) IP Address to be used by Pandora FMS internal email capabilities

mta_address 172.16.30.254

mta_port, this is the mail server port (default 25)

#mta_port 25

mta_user MTA User (if needed for auth, FQD or simple user, depending on your server)

#mta_user myuser@mydomain.com

mta_pass MTA Pass (if needed for auth)

#mta_pass mypassword

mta_auth MTA Auth system (if needed, it supports LOGIN, PLAIN, CRAM-MD5, DIGEST-MD)

#mta_auth LOGIN

mta_from Email address that sends the mail, by default is pandora@localhost

#probably you need to change it to avoid problems with your antispam

#mta_from Pandora FMS <pandora@mydomain.com>

Set 1 if want eMail deliver alert in separate mail (default).

Set 0 if want eMail deliver shared mail by all destination.

mail_in_separate 1

xprobe2: Optional package to detect OS types using advanced TCP/IP

fingerprinting tecniques, much more accurates than stadard nmap.

If not provided, nmap is used insted xprobe2

xprobe2 /usr/bin/xprobe2

nmap: If provided, is used to detect OS type with recon server using

advanded OS fingerprint technique. Xprobe2 gives more accurate results

Nmap is also used to do TCP port scanning in detected host.

nmap /usr/bin/nmap

Default path is /usr/sbin/fping for installation default in distro Centos , if you are installing in other distribution,

you install fping in /usr/bin/fping and change the path in this line.

Path to the fping binary. Used by the Enterprise ICMP Server.

fping /usr/sbin/fping

fping /usr/bin/fping

A value that specifies how aggressive nmap should be from 1 to 5. 1 means slower but more reliable, 5 means faster but less reliable. 2 by default.

nmap_timing_template 2

Like nmap_timing_template, but applies to Satellite Server and Recon Server network scans. 3 by default.

recon_timing_template 3

snmpget: Needed to do SNMP checks. By default is on /usr/bin/snmpget

snmpget /usr/bin/snmpget

Location of the braa binary needed by the Enterprise SNMP Server

/usr/bin/braa by default (PANDORA FMS ENTERPRISE ONLY).

braa /usr/bin/braa

Number of retries before braa hands a module over to the Network Server (PANDORA FMS ENTERPRISE ONLY).

braa_retries 3

Default group id for new agents created with Pandora FMS Data Server

If this token is enabled and Agent is setup with a fixed group, server settings will override agent settings

If this token is disabled and group is not provided in the agent, or provided group doesn't exist, agent data

will be dropped. We use the Group ID #10 (Unknown) for a "valid" default value, please change as your own decision.

autocreate_group 10

Set to 1 if want to autocreate agents with Pandora FMS Data Server,

set to 0 to disable (for security purposes, for example).

autocreate 1

max_log_size: Specify max size of Pandora FMS server log file (1MB by default). If

log file grows above this limit, is renamed to "pandora_server.log.0".

max_log_size 1048576

max_log_generation: Specify max generation count (between 1 and 9) of Pandora FMS server log files.

max_log_generation 1

max_queue_files (5000 by default)

When server have more than max_queue_files in incoming directory, skips the read

the directory to avoid filesystem overhead.

max_queue_files 5000

Use the XML file last modification time as timestamp.

use_xml_timestamp 1

```
# Pandora FMS will autorestart itself each XXX seconds, use this if you experience problems with

# shutting down threads, or other stability problems.

# auto_restart 86400

# Pandora FMS will restart after restart_delay seconds on critical errors.

restart 1

restart_delay 60

# More information about GIS Setup in /usr/share/pandora_server/util/gis.README

# Flag to activate GIS (positional information for agents and maps)

# by default it is desactivated

#activate_gis 0

# Radius of error in meters to consider two gis locations as the same location.

#location_error 50

# Recon reverse geolocation mode [disabled, sql, file]

#   disabled    The recon task doesn't try to geolocate the ip discovered.

#   sql         The recon task trys to query the SQL database to geolocate the

#               ip discovered

#   file        The recon task trys to find the geolocation information of the

#               ip discovered in the file indicated in the

#               recon_reverse_geolocation_file parameter

# recon_reverse_geolocation_mode disabled
```

```
# Recon reverse geolocation file. This is the database with the reverse

# geolocation information using MaxMind GPL GeoLiteCity.dat format).

#recon_reverse_geolocation_file /usr/local/share/GeoIP/GeoIPCity.dat

# Radius (in meters) of the circle in where the agents will be place randomly

# when finded by a recon task. Center of the circle is guessed

# by geolocating the IP.

#recon_location_scatter_radius 1000

# Pandora Server self-monitoring (embedded agent) (by default enabled)

self_monitoring 1

# Self monitoring interval (in seconds).

self_monitoring_interval 300

# Update parent from the agent xml

#update_parent 1

# This enable realtime reverse geocoding using Google Maps public api.

# This requires internet access, and could have performance penalties processing GIS

# information due the connetion needed to resolve all GIS input.

# NOTE: If you dont pay the service to google, they will ban your IP in a few days.

# google_maps_description 1

# This enable realtime reverse geocoding using Openstreet Maps public api.

# This requires internet access, and could have performance penalties processing GIS
```

information due the connetion needed to resolve all GIS input.

You can alter the code to use a local (your own) openstreet maps server.

openstreetmaps_description 1

Enable (1) or disable (0) Pandora FMS Event Web Server (PANDORA FMS ENTERPRISE ONLY).

webserver 1

Number of threads for the Web Server (PANDORA FMS ENTERPRISE ONLY).

web_threads 1

Uncomment to perform web checks with CURL instead of LWP.

#web_engine curl

Enable (1) or disable (0) Pandora FMS Inventory Server (PANDORA FMS ENTERPRISE ONLY).

inventoryserver 1

Number of threads for the Web Server (PANDORA FMS ENTERPRISE ONLY).

inventory_threads 1

Enable (1) or disable (0) Pandora FMS Export Server (PANDORA FMS ENTERPRISE ONLY).

exportserver 0

Number of threads for the Export Server (PANDORA FMS ENTERPRISE ONLY).

export_threads 1

Enable (1) or disable (0) Pandora FMS Event Server (PANDORA FMS ENTERPRISE ONLY).

eventserver 0

Event Server event window in seconds (3600 by default) (PANDORA FMS ENTERPRISE ONLY).

event_window 3600

Enable (1) or disable (0) Pandora FMS Enterprise ICMP Server (PANDORA FMS ENTERPRISE ONLY).

You need nmap 5.20 or higher in order to use this !

icmpserver 1

Number of threads for the Enterprise ICMP Server (PANDORA FMS ENTERPRISE ONLY).

icmp_threads 4

Enable (1) or disable (0) Pandora FMS Enterprise SNMP Server (PANDORA FMS ENTERPRISE ONLY).

Check braa tool is running and operative.

snmpserver 1

Number of threads for the Enterprise SNMP Server (PANDORA FMS ENTERPRISE ONLY).

snmp_threads 4

Block size for block producer/consumer servers, that is, the number of modules

per block (15 by default) (PANDORA FMS ENTERPRISE ONLY).

block_size 20

If set to 1, process XML data files in a stack instead of a queue. 0 by default.

WARNING: Incremental modules will not work properly if dataserver_lifo is set to 1!!!

dataserver_lifo 0

If set to 1, the policy manager is enabled and the server is listening the policy queue.

0 by default (PANDORA FMS ENTERPRISE ONLY)

policy_manager 1

If set to 1, the event replicate process is enabled. 0 by default. (PANDORA FMS ENTERPRISE ONLY)

WARNING: This process doesn't do anything if is not properly configured from the console setup

event_replication 0

If set to 1, new events validate older event for the same module. This will

affect the performance of the server. This was the "normal behaviour" on previous (4.x) versions.

disable only if you really know what you are doing !!.

event_auto_validation 1

If defined, events generated by Pandora FMS will be written to the specified text file.

#event_file /var/log/pandora/pandora_events.txt

Set the maximum number of traps that will be processed from a single source in a

configured time interval.

snmp_storm_protection 25

Time interval for snmp_storm protection (in seconds).

snmp_storm_timeout 10

Default texts for some events. The macros _module_ and _data_ are supported.

#text_going_down_normal Module '_module_' is going to NORMAL (_data_)

#text_going_up_critical Module '_module_' is going to CRITICAL (_data_)

#text_going_up_warning Module '_module_' is going to WARNING (_data_)

#text_going_down_warning Module '_module_' is going to WARNING (_data_)

#text_going_unknown Module '_module_' is going to UNKNOWN

Events older that the specified time (in seconds) will be auto-validated. Set to 0 to disable this feature.

event_expiry_time 0

Only events more recent than the specified time window (in seconds) will be auto-validated. This value must

be greater than event_expiry_time.

#event_expiry_window 86400

If set to 1, SNMP modules run by the Network Server will be claimed back by

the SNMP Enterprise Server when pandora_db is run.

claim_back_snmp_modules 1

If set to 1 asynchronous modules that do not receive data for twice their

interval will become normal. Set to 0 to disable.

async_recovery 1

Console API credentials.

Required for some features like the module graphs macros.

console_api_url: Api URL (http://localhost/pandora_console/include/api.php by default)

console_api_url http://localhost/pandora_console/include/api.php

console_api_pass: Api pass

console_api_pass 1234

console_user: Console user name (admin by default)

console_user admin

console_pass: Console password (pandora by default)

console_pass pandora

Passphrase used to generate the key for password encryption (PANDORA FMS ENTERPRISE ONLY).

#encryption_passphrase passphrase

Time interval (as a multiple of the module interval) before a module becomes unknown. Twice the module's interval by default.

#unknown_interval 2

Maximum executing time of an alert (in seconds)

global_alert_timeout 15

If set to 1 allows PandoraFMS Server to be configured via the web console (PANDORA FMS ENTERPRISE ONLY).

remote_config 0

Remote address to send the configuration file (PANDORA FMS ENTERPRISE ONLY).

remote_config_address localhost

Remote port to send the configuration file (PANDORA FMS ENTERPRISE ONLY).

#remote_config_port 41121

Extra options for the Tentacle client to send the configuration file (PANDORA FMS ENTERPRISE ONLY).

#remote_config_opts

Module status change events will not be generated and module alerts will not

be executed for the specified number of seconds since the server starts up.

warmup_event_interval 0

Modules will not become unknown (so no unknown events will be generated) and

keepalive modules will not be updated for the specified number of seconds

since the server starts up.

warmup_unknown_interval 300