UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE PANDORA FMS OPEN SOURCE COMO PLATAFORMA DE MONITOREO PARA LA EMPRESA MICROTEL.COM EIRL”

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Christian Vidal Lopez Montoya

Asesor:

Ing. Eduardo Martin Reyes Rodríguez
https://orcid.org/0000-0003-2050-9616

Lima - Perú

2023

INFORME DE SIMILITUD

TSP Christian Vidal López Montoya

INFORME DE ORIGINALIDAD

13%	12%	1%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	1%
2	Submitted to Unviersidad de Granada Trabajo del estudiante	1%
3	www.whatsupgold.com Fuente de Internet	1%
4	vdocuments.es Fuente de Internet	1%
5	wiki.pandorafms.com Fuente de Internet	<1%
6	1library.co Fuente de Internet	<1%
7	es.scribd.com Fuente de Internet	<1%
8	Submitted to Universidad Privada del Norte Trabajo del estudiante	<1%
9	repositorio.unican.es Fuente de Internet	<1%

DEDICATORIA

A mis padres, por el apoyo incondicional durante este periodo de estudio y porque han sido mi fuente de inspiración.

A mi hijo Christian, por ser el principal motor de superación diaria y por darme la fuerza inagotable de seguir luchando.

AGRADECIMIENTO

A la Universidad Privada del Norte y a los excelentes docentes que han impartido conocimiento, experiencia y sabiduría durante el desarrollo de esta carrera tan apasionante.

Al asesor, el Ing. Eduardo Martin Reyes Rodríguez, por su experiencia y conocimiento para el desarrollo de este proyecto.

Finalmente, a la empresa Microtel.Com EIRL, que ha permitido lograr mis experiencias y desarrollo profesional a lo largo de estos años.

Tabla de contenidos

INFORME DE SIMILITUD **2**
DEDICATORIA **3**
AGRADECIMIENTO **4**
ÍNDICE DE TABLAS **7**
ÍNDICE DE FIGURAS **8**
RESUMEN EJECUTIVO **11**
CAPÍTULO I. INTRODUCCIÓN **12**
1.1. Descripción de la Empresa 12
1.2. Datos de la Empresa 14
1.2.1. Logotipo 14
1.2.2. Microtel.Com E.I.R.L 14
1.2.3. Misión 14
1.2.4. Visión 14
1.2.5. Organigrama 15
1.2.6. Información ficha RUC 15
1.3. Productos y Servicios 16
CAPÍTULO II. MARCO TEÓRICO **18**
2.1 Fundamentos de Monitorización 18
2.1.1. Conceptos de Monitoreo 18
2.1.2. Tipos de Monitoreo 19
2.1.2.1. Monitoreo de Redes 20
2.1.2.2. Monitoreo de Servidores 25
2.2. Monitorización en las Empresas 26
2.2.1. Evolución del Monitoreo en las Empresas 26
2.2.2. Beneficios del Monitoreo en las Empresas 27
2.3. Plataformas de Monitoreo 29
2.3.1. Clasificación de Plataformas de Monitorización 30
2.3.2. Comparativa de Plataformas de Monitoreo Privativas y Open Source 32
2.3.3. Ventajas del Uso de Plataformas de Monitoreo Open Source 34
2.4. Plataforma de Monitoreo Pandora FMS Open Source 35
2.4.1. Introducción a Pandora FMS 35
2.4.1.1. Historia 35
2.4.2. Principales Características 36
2.4.3. Funcionalidades de la Plataforma 36
2.4.4. Arquitectura de Pandora FMS Open Source 41
2.4.4.1. Servidores de Pandora FMS 42

2.5. Fundamentos de Implementación de Pandora FMS Open Source 43
2.5.1. Requisitos Mínimos de Hardware 43
2.5.2. Requisitos Mínimos de Software 43
2.5.3. Diseño de Arquitectura de Monitoreo con Pandora FMS Open Source 44
2.5.3.1. Redes Accesibles 45
2.5.3.2. Redes con Dificultad de Acceso 45
2.5.4. Métricas y Umbrales en Pandora FMS Open Source 46
2.5.4.1. Métricas 46
2.5.4.2. Umbrales 47
2.5.5. Definición de Agentes Software para el Monitoreo 48
2.5.6. Alertas y Eventos en Pandora FMS 49
2.5.6.1. Alertas 49
2.5.6.2. Eventos 50
2.5.7. Consolas Visuales y Dashboards 51
2.5.7.1. Consolas Visuales 51
2.5.7.2. Dashboards 53
2.6. Términos Básicos 54
2.7. Limitaciones para el Desarrollo del Proyecto 59

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA 61
3.1. Ingreso a la Empresa 61
3.2. Funciones 61
3.3. Impacto en la Empresa 62
3.4. Identificación del Problema 62
3.5. Objetivo General 64
3.6. Objetivos Específicos 64
3.7. Experiencia. 64
3.7.1. Participantes del Proyecto. 64
3.7.2. Estrategias. 65
3.7.3. Metodología 66
3.7.4. Diagrama de Arquitectura de Red Empresarial. 69
3.7.5. Instalación de Pandora FMS 78
3.7.6. Configuración de Pandora FMS 83

CAPÍTULO IV. RESULTADOS 105

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 113
5.1. Conclusiones 113
5.2. Recomendaciones 114

REFERENCIAS 115

ÍNDICE DE TABLAS

Tabla 1 Comparativa plataformas de monitoreo privativas y open source 33
Tabla 2 Requisitos mínimos de hardware..... 43
Tabla 3 Requisitos mínimos de puertos..... 44
Tabla 4 Requisitos de sistema operativo para agentes software..... 48
Tabla 5 Participantes del proyecto..... 64
Tabla 6 Componentes de la arquitectura 69
Tabla 7 Supervisión de recursos TI antes de Pandora FMS 105
Tabla 8 Supervisión de recursos TI después de Pandora FMS..... 107
Tabla 9 Reporte de incidencias de recursos TI antes de Pandora FMS..... 108
Tabla 10 Reporte de incidencias de recursos TI después de Pandora FMS 109

ÍNDICE DE FIGURAS

Figura 1 Logotipo Microtel.Com EIRL 14
Figura 2 Fachada Microtel.Com E.I.R.L. 14
Figura 3 Organigrama Microtel.Com E.I.R.L. 15
Figura 4 Socios estratégicos Microtel.Com EIRL 17
Figura 5 Ejecución de comando ping 21
Figura 6 Ejecución de comando traceroute 21
Figura 7 Diagrama básico de comunicación SNMP 22
Figura 8 Diagrama de árbol de MIB 23
Figura 9 Plataforma de monitoreo Nagios 30
Figura 10 Plataforma de monitoreo Zabbix 30
Figura 11 Plataforma de monitoreo Pandora FMS 31
Figura 12 Plataforma de monitoreo PRTG 31
Figura 13 Plataforma de monitoreo SolarWinds 32
Figura 14 Plataforma de monitoreo ManageEngine 32
Figura 15 Arquitectura de Pandora FMS 41
Figura 16 Arquitectura de monitoreo remota 45
Figura 17 Arquitectura de monitoreo con agentes software 45
Figura 18 Arquitectura de monitoreo modo broker 46
Figura 19 Arquitectura de monitoreo modo proxy 46
Figura 20 Definición de umbrales en Pandora FMS 48
Figura 21 Estructura de las alertas 50
Figura 22 Consola visual hosting status 52
Figura 23 Consola visual soporte 52
Figura 24 Consola visual nano datacenter 52
Figura 25 Consola visual datacenter 53
Figura 26 Dashboard hosting panel 54
Figura 27 Dashboard general status 54
Figura 28 Acta de inicio del proyecto 67
Figura 29 Diagrama gantt del proyecto 68
Figura 30 Router ISP Castlenet Technology CBV384Z4 71
Figura 31 Firewall Untangle NG 71
Figura 32 Switch core CISCO SF300 72
Figura 33 Switch D-Link DGS-1100-24P 72
Figura 34 Switch D-Link DGS-1100-8P 73
Figura 35 Central telefonía VOIP Zycoo 73
Figura 36 Servidor NVR HIKVISION 74
Figura 37 Servidor hypervisor Proxmox VE 74
Figura 38 Punto de acceso TP-LINK TL-WR940N 75
Figura 39 Punto de acceso TP-LINK TL-WA901ND 75
Figura 40 Cámara exterior HIKVISION 76
Figura 41 Cámara interior 1 HIKVISION 76
Figura 42 Cámara interior 2 HIKVISION 77
Figura 43 Diagrama de topología de la red empresarial 77
Figura 44 Asistente de creación VM–general 78

Figura 45 Asistente de creación VM–disco 79
Figura 46 Asistente de creación VM–CPU 79
Figura 47 Asistente de creación VM–RAM 79
Figura 48 Asistente de creación VM–network 80
Figura 49 Resumen VM Pandora FMS 725 NG 80
Figura 50 Resumen VM Pandora FMS 772 LTS 80
Figura 51 Wizard de instalación ISO Appliance CentOS 7 81
Figura 52 Instalando ISO Appliance CentOS 7 81
Figura 53 Wizard de instalación Rocky Linux 8 82
Figura 54 Instalando Rocky Linux 8 82
Figura 55 Pantalla de sesión en terminal Pandora FMS 725 NG 83
Figura 56 Script de instalación Pandora FMS 772 LTS 83
Figura 57 Pantalla de inicio consola web Pandora FMS 84
Figura 58 Wizard de inicio consola web Pandora FMS 84
Figura 59 Configuraciones generales Pandora FMS 85
Figura 60 Configuración de base de datos Pandora FMS 85
Figura 61 Configuración de alerta por email 85
Figura 62 Vista de creación de usuarios 86
Figura 63 Listado de usuarios en consola 86
Figura 64 Definición de grupos de agentes 87
Figura 65 Vista de creación de agentes 87
Figura 66 Listado de agentes en consola 88
Figura 67 Métricas de los agentes de red 88
Figura 68 Configuración de métrica Host Alive 89
Figura 69 Configuración de métrica Host Latency 89
Figura 70 Definición de alerta ICMP 89
Figura 71 Instalación script en Proxmox VE 90
Figura 72 Instalación script en ERP Odoo 90
Figura 73 Archivo de configuración agente software 90
Figura 74 Agentes software en consola Pandora FMS 91
Figura 75 Métricas del agente software Proxmox VE 91
Figura 76 Métricas del agente software ERP Odoo 91
Figura 77 Configuración métrica Cpu Load agente software 92
Figura 78 Configuración métrica Memory Used agente software 92
Figura 79 Configuración métrica Disk Used agente software 92
Figura 80 Definición de alerta Critical Cpu Load 93
Figura 81 Definición de alerta Warning Memory Used 93
Figura 82 Definición de alerta Critical Memory Used 93
Figura 83 Definición de alerta Warning Disk Used 93
Figura 84 Definición de alerta Critical Disk Used 94
Figura 85 Listado de alertas para agentes software 94
Figura 86 Consola visual monitoreo general 95
Figura 87 Consola visual topología de red 95
Figura 88 Consola visual servidores 1 95
Figura 89 Consola visual servidores 2 96
Figura 90 Consola visual ecosistema infraestructura TI 96
Figura 91 Host Alive y latencia router ISP Claro 97
Figura 92 Host Alive y latencia firewall Untangle NG 97
Figura 93 Host Alive y latencia switch core Cisco SF300 98

Figura 94 Host Alive y latencia switch D-Link 1100-24P 98
Figura 95 Host Alive y latencia switch D-Link 1100-8P 99
Figura 96 Host Alive y latencia central VOIP Zycoo 99
Figura 97 Host Alive y latencia AP01-TP-Link TL-WR940N 100
Figura 98 Host Alive y latencia AP02-TP-Link TL-WA901ND 100
Figura 99 Host Alive y latencia cámara exterior HIKVISION 101
Figura 100 Host Alive y latencia cámara interior 1 HIKVISION 101
Figura 101 Host Alive y latencia cámara interior 2 HIKVISION 102
Figura 102 Host Alive y latencia servidor de backups OMV 102
Figura 103 Host Alive y latencia servidor hypervisor Proxmox VE 103
Figura 104 Host Alive y latencia servidor NVR HIKVISION 103
Figura 105 Promox VE CPU, Memory, Disk 104
Figura 106 Cobertura de recursos TI supervisados antes de Pandora FMS 106
Figura 107 Cobertura de recursos TI supervisados después de Pandora FMS 107
Figura 108 Tiempo de inactividad en los recursos TI antes de Pandora FMS 109
Figura 109 Tiempo de inactividad en los recursos TI después de Pandora FMS 110
Figura 110 Comparativa en horas de inactividad en los recursos TI 111
Figura 111 Promedio de tiempo de respuesta a incidentes de recursos TI 112

RESUMEN EJECUTIVO

El presente trabajo de suficiencia profesional aborda la implementación de Pandora FMS Open Source, como plataforma de monitoreo para la infraestructura TI de la empresa Microtel.Com EIRL, debido a que la empresa cuenta con diversos recursos tecnológicos y ha venido experimentando inactividad, tiempos de respuesta excesivos y eventos críticos en los mismos.

Se utilizó la metodología PMI (Project Management Institute) para lograr el objetivo principal, abarcando la fase de inicio, planificación, ejecución, seguimiento, control y cierre. Se identificaron los componentes de la arquitectura para el desarrollo del diagrama de topología de la red empresarial, luego se implementó Pandora FMS en una máquina virtual en el hypervisor Proxmox VE, asimismo se configuró la plataforma de monitoreo para el correcto funcionamiento en la empresa.

Los resultados analizados muestran satisfactoriamente la cobertura de supervisión total de los recursos TI con un incremento del 90%, así como la reducción del tiempo de inactividad a 5.4 horas, y la mejora en los tiempos de respuesta a incidentes ocurridos en la empresa con un promedio de 0.56 horas.

CAPÍTULO I. INTRODUCCIÓN

1.1. Descripción de la Empresa

Microtel.Com E.I.R.L., es una Empresa Individual de Responsabilidad Limitada fundada en el año 2005 por José Lazo Moreno, con RUC 20511040729. Inició realizando actividades de consultoría y capacitaciones dedicadas a temas de cableado estructurado, networking, fibra óptica, telefonía IP, CCTV y sistemas eléctricos. Durante varios años la empresa ha consolidado conocimientos especializados en tecnología y ha venido trabajando con personal totalmente calificado, entre profesionales y técnicos.

Esta experiencia ha permitido a la empresa en el año 2014, especializarse en centros de datos, desde su concepción y diseño, hasta la implementación y mantenimiento; logrando ofrecer a sus clientes nuevos servicios y productos en el futuro. Desde el inicio de actividades y a lo largo de los años, Microtel.Com EIRL ha operado en locales alquilados, motivo por el cual, el traslado ha conllevado a desarrollar un método eficaz y sencillo de mover el equipamiento IT (Infraestructura Tecnológica) que la empresa posee, siendo principalmente un gabinete, router, switches, servidores, ups y aire acondicionado, dando como resultado a la creación del producto “Skylink Networks”, un microdatacenter lanzado el año 2017 y que ha tomado relevancia en el mercado debido a la portabilidad y ahorro que éste representa. La marca “Skylink Networks” viene posicionándose en el mercado peruano, como un producto novedoso.

Microtel.Com EIRL para poder operar de manera eficaz y óptima utiliza diversos recursos, tanto hardware como software, como es el caso de dispositivos de comunicaciones entre los que destacan el router que permite la conectividad a internet, un firewall de próxima generación que permite asegurar el perímetro de la red de la empresa, tres switches que proporcionan la comunicación entre los usuarios y los recursos tecnológicos de la empresa.

También posee una central de telefonía IP, un servidor de NVR que integra diversas cámaras de seguridad. Asimismo, cuenta con un servidor hypervisor, destinado a provisionar máquinas virtuales que actúan como servidores, entre ellos el servidor de respaldos y copias de seguridad, el servidor ERP que permite gestionar el CRM y cotizaciones hacia los clientes.

Adicionalmente la empresa utiliza diversos servicios en la nube, como es el caso de una plataforma file server para el trabajo colaborativo y el servicio de web hosting, permitiendo a la empresa tener una página web y correos corporativos. Debido a la diversidad de soluciones tecnológicas que la empresa utiliza, se decide implementar una solución de supervisión y monitorización para estos recursos, motivo por el cual, quien suscribe y con experiencia en monitoreo presenta una prueba de concepto de la plataforma de monitoreo Pandora FMS Open Source, una solución eficaz y completa, destacada principalmente por su arquitectura, ya que al no conllevar costos de licenciamiento tanto en sistema operativo como en software, logró posicionarse de manera exitosa en la empresa, permitiendo supervisar los recursos IT en tiempo real y alertar de presentarse algún evento.

Esto conllevó a Microtel.Com EIRL, a integrar la plataforma de monitorización Pandora FMS Open Source a su portafolio de productos y servicios, motivo por el cual, en el año 2018, la empresa se convierte en representante oficial en el Perú. Gracias a las características y ventajas de la plataforma de monitoreo y a la experiencia obtenida con Pandora FMS Open Source, Microtel.Com EIRL ha desarrollado proyectos de monitorización a clientes importantes en nuestro sector.

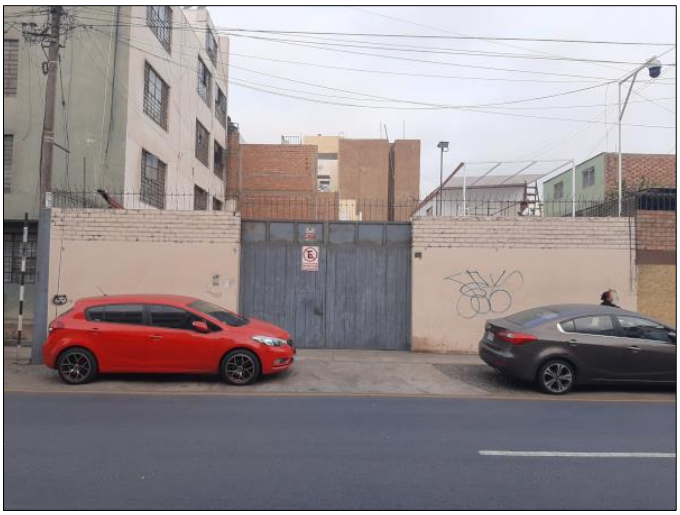
1.2. Datos de la Empresa

1.2.1. Logotipo

Figura 1
Logotipo Microtel.Com EIRL

1.2.2. Microtel.Com E.I.R.L.

Figura 2
Fachada Microtel.Com E.I.R.L.



Fuente: Elaboración propia

1.2.3. Misión

Somos una organización que brinda soluciones de infraestructura tecnológica, buscando los más altos estándares de calidad y excelencia en todo lo que hacemos.

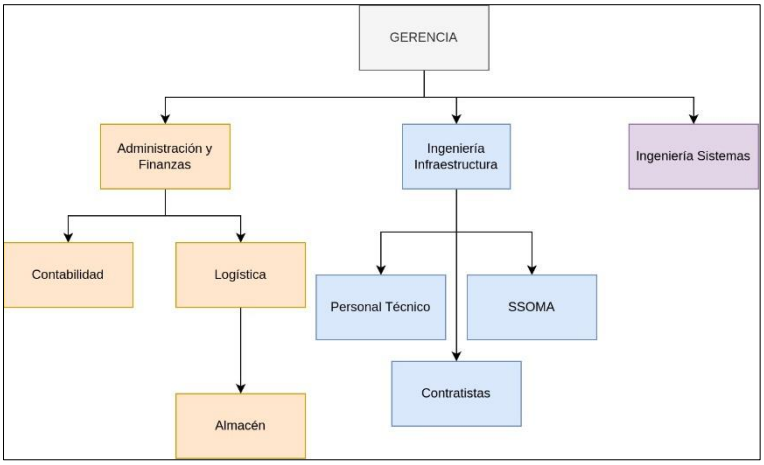
1.2.4. Visión

Ser líderes en soluciones de infraestructura tecnológica y ser reconocidos por la calidad y la alta especialización de nuestros servicios.

1.2.5. Organigrama

Figura 3

Organigrama Microtel.Com E.I.R.L.



Fuente: Elaboración Propia

1.2.6. Información ficha RUC

a) Información General del Contribuyente

- Razón Social: MICROTEL.COM E.I.R.L.
- Tipo de Contribuyente: 07-EMPRESA INDIVIDUAL DE RESP. LTDA
- Fecha de Inscripción: 21/06/2005
- Fecha de Inicio de Actividades: 21/06/2005

b) Datos del Contribuyente

- Actividad Económica Principal: 6202 - CONSULTORÍA DE INFORMÁTICA Y GESTIÓN DE INSTALACIONES INFORMÁTICAS
- Actividad Económica Secundaria: 6209 - OTRAS ACTIVIDADES DE TECNOLOGÍA DE LA INFORMACIÓN Y DE SERVICIOS INFORMÁTICOS
- Teléfono Fijo 1: 5640329
- Teléfono Fijo 2: 5646828
- Teléfono Móvil 1: 986656140
- Correo Electrónico: administracion@microtelperu.com

c) Domicilio Fiscal

- Departamento: LIMA
- Provincia: LIMA
- Distrito: LIMA
- Tipo y Nombre Zona: URB. LOS CIPRESES
- Tipo y Nombre Vía: CAL. TENIENTE ARISTIDES DEL CARPIO MUÑOZ
- Nro.: 1269

d) Representante Legal

- Apellidos y Nombres: GONZALES REQUE ISABEL MILAGROS
- Cargo: GERENTE
- DNI: 06669507

1.3. Productos y Servicios

Microtel.Com EIRL, ofrece los siguientes productos y servicios:

a) Productos

- Microdatacenter, en los modelos Silver-M, Industrial, Platinum, Nano y Mini Datacenter.
- Bancos de energía con y sin redundancia.
- Transformadores monofásicos y trifásicos.
- Sistemas de enfriamiento portátil para centros de datos.

b) Servicios

- Monitorización de Infraestructura TI.
- Ingeniería, suministro e instalación de sistemas de cableado estructurado.
- IOT aplicado a la industria 4.0.
- Servicios de fibra óptica.
- Servicios de diseño, implementación e ingeniería para centros de datos.

- Servicios TI.

Hoy en día Microtel.Com EIRL trabaja en estrecha colaboración con socios estratégicos cuidadosamente seleccionados para crear sinergias que generen un impacto mayor a la hora de desarrollar y entregar sus servicios, dentro de los que destacan Tripp Lite by EATON, Vertiv, Furukawa, Siemon, Commscope, Leviton, Panduit, Pandora FMS, entre otros.

Figura 4
Socios estratégicos Microtel.Com EIRL

Fuente: Microtel.Com EIRL.

Asimismo, los principales clientes ocupan un lugar especial en la estrategia debido a su contribución sustancial y su compromiso continuo con los productos y servicios, resaltando principalmente a Komatsu Mitsui Maquinarias del Perú, Cirion Technologies, Ransa, Tramarsa, Natclar, Sunarp Moquegua, entre otros.

CAPÍTULO II. MARCO TEÓRICO

Se describe los componentes y conceptos requeridos para abordar la implementación de la plataforma de monitoreo Pandora FMS Open Source:

2.1 Fundamentos de Monitorización

2.1.1. Conceptos de Monitoreo

La monitorización consiste en supervisar lo que ocurre en nuestra red y recibir notificaciones sobre eventos que podrían ser relevantes para nosotros, dado que es imposible estar vigilando constantemente todo lo que sucede, durante las 24 horas del día, los 365 días del año (Arrebola Real, 2010); por otro lado, podemos indicar que el monitoreo es el proceso de evaluar la utilización de los recursos proporcionados por una máquina permitiendo prever situaciones de sobrecarga y las subsiguientes actualizaciones requeridas; además, notificar a los administradores en cuanto un servicio no esté operativo o funcione de manera incorrecta posibilita una resolución más ágil de los problemas que puedan surgir (Hertzog & Mas, 2017).

Otro autor explicó que la monitorización, consiste en la comprobación de un valor numérico que refleja el estado de un componente a lo largo del tiempo, con el propósito de estar en condiciones de identificar cualquier anomalía en ese componente (Michis, 2022); por otra parte, podemos indicar que tiene como finalidad optimizar el rendimiento y prolongar la disponibilidad de los servicios de tecnología de la información, gracias a la supervisión constante que facilita la detección de las razones detrás de las fallas y permite ofrecer soluciones más rápidamente (Intriago et al., 2022).

Por lo expuesto, podemos considerar a la monitorización a un procedimiento fundamental en el dominio de las tecnologías, abarcando la observación, cuantificación y recopilación de información concerniente a sistemas, redes, servidores, aplicaciones y otros

elementos tecnológicos. El propósito primordial radica en la supervisión concurrente de su rendimiento, disponibilidad, seguridad y otros atributos pertinentes. Mediante esta práctica, se logra adquirir una perspectiva en tiempo real de la operatividad de dichos sistemas y su conducta en situaciones habituales y excepcionales.

2.1.2. Tipos de Monitoreo

Existen diversos tipos de monitoreo, cada uno especifico y eficaz en su área, para este trabajo de suficiencia se abarcará específicamente la monitorización en redes y en servidores. Por ello es importante conocer conceptos básicos sobre redes y servidores, descritos a continuación:

a) Red

Es el conjunto de equipos o dispositivos interconectados, pudiendo comunicarse entre sí. La finalidad de una red es la transferencia datos, información y recursos entre los equipos conectados. Existen diversos tipos de redes con respecto a su función, alcance y propósito, como lo son las redes LAN, WAN, MAN, WIFI, Campus (Clavijo Moran, 2021).

b) Servidor

Los servidores son componentes esenciales de toda infraestructura tecnológica moderna, gracias a estos, es posible facilitar la comunicación, el intercambio de información y la disponibilidad de servicios, tanto en las propias redes y en Internet.

La función principal de los servidores es atender solicitudes de los clientes y proporcionarles aquellos recursos que necesitan como: páginas web, documentos, archivos, aplicaciones, entre otros. Sin los servidores, muchas de las funciones que damos por sentado en línea, como acceder a sitios web o enviar correos electrónicos, serían imposibles.

Existen diferentes tipos de servidores, destinados a cumplir una función específica, comúnmente estos pueden ser: (IONOS, 2023)

- **Servidor Web:** Se encargan de almacenar y entregar páginas web a los navegadores de los usuarios.
- **Servidor de Correo Electrónico:** Realizan la gestión de la recepción, almacenamiento y envío de correos electrónicos.
- **Servidor de Archivos:** Estos servidores cumplen la función de almacenar y gestionar archivos compartidos, permitiendo a los usuarios acceder a estos recursos en una red local o a través de Internet.
- **Servidor de Base de Datos:** Almacenan, gestionan y permiten el acceso a bases de datos, lo que es esencial para muchas aplicaciones y sitios web que requieren almacenamiento de datos estructurados.
- **Servidor de Aplicaciones:** Tienen el objetivo de proporcionar y ejecutar aplicaciones y servicios que los usuarios finales utilizarán (Marañón Martín, 2013).

2.1.2.1. Monitoreo de Redes

La monitorización de red se puede definir como un procedimiento de observación de los elementos que componen la red, y para llevar a cabo este procedimiento, es esencial recopilar métricas de estos dispositivos. La recopilación de datos puede efectuarse de manera activa o pasiva (Leira Osuna, 2019); además, se define a la monitorización de redes como una parte esencial de la gestión de redes que se enfoca en asegurar que los elementos estén disponibles y funcionen de manera eficiente. Esto se logra al analizar y procesar las métricas recopiladas de los elementos y administrar su configuración (Trigo Caparros, 2021).

Considerando lo anterior, podemos definir que la monitorización de redes implica el seguimiento de diversos parámetros y métricas que permiten evaluar el rendimiento y la disponibilidad de la red, así como la detección temprana de posibles amenazas o interrupciones. Para realizar el seguimiento de estas métricas es necesario realizar mecanismos de monitorización de red, como son el sondeo o polling, que son procedimientos

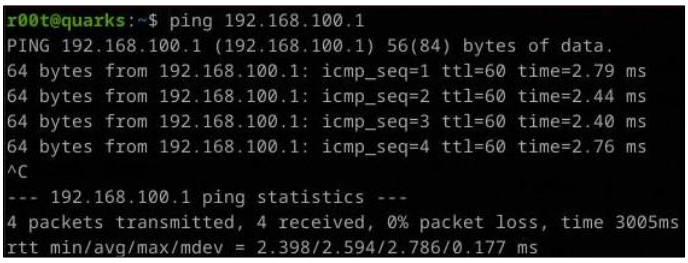
de acceso regular a los datos de gestión almacenados en los nodos administrados. Este enfoque presenta la ventaja de que los objetos que se administran solo necesitan estar listos para responder, lo que simplifica el proceso (Cantos San Emeterio, 2021).

El uso de estos mecanismos requiere operar con los protocolos ampliamente conocidos en el mundo de la monitorización, como son el protocolo ICMP y SNMP, descritos a continuación:

a) Monitorización por ICMP

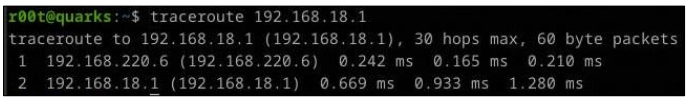
Es un protocolo de la capa de red, ampliamente utilizado para enviar mensajes y obtener información de conectividad y latencia, es decir, el estado de los dispositivos en una red, creado por la RFC 792 en el año 1981. Por otra parte, el protocolo ICMP se emplea para transmitir mensajes que contienen información de control de errores. Este protocolo se utiliza comúnmente en conjunción con las utilidades de comando como ping y traceroute (Lamana Núñez, 2022).

Figura 5
Ejecución de comando ping



Fuente: Elaboración Propia

Figura 6
Ejecución de comando traceroute



Fuente: Elaboración Propia

Gracias a la monitorización con este protocolo podemos comprobar lo siguiente:

- Comprobar disponibilidad.
- Obtener la latencia.

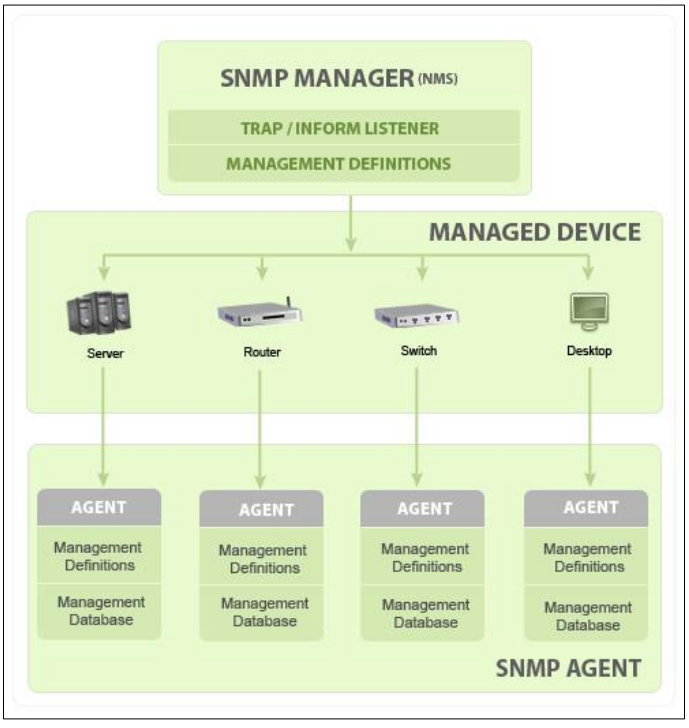
- Detectar problemas en la red.
- Identificar dispositivos inactivos.

b) Monitorización por SNMP

Aunque la monitorización por ICMP suele ser útil, no es completamente representativa para obtener el estado de nuestra red. Por ello, es necesario utilizar el protocolo SNMP que fue creado en el año 1990 en la RFC 1157. Este protocolo es un estándar para supervisar y administrar dispositivos de red, servidores, enrutadores, conmutadores y otros componentes de infraestructura tecnológica.

El protocolo SNMP involucra varios elementos, como puede observarse en el siguiente diagrama de comunicación SNMP (Rodríguez Trujillo et al., 2022):

Figura 7
Diagrama básico de comunicación SNMP



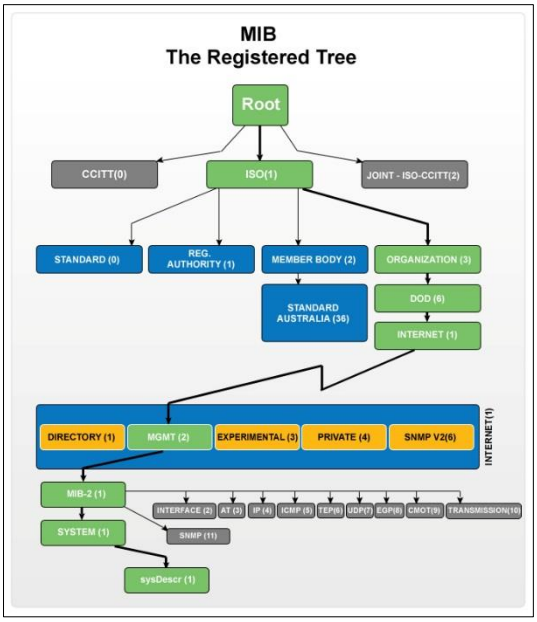
Fuente: Tomado de (Manageengine, s.f.)

- **Agentes SNMP:** Este agente recopila y almacena información sobre el dispositivo, como estadísticas de rendimiento y datos de configuración.

- **Gestor SNMP:** Se encargar de utilizar comandos SNMP para acceder y solicitar información de los agentes SNMP.
- **MIB:** Es una base de datos jerárquica que almacena información sobre los objetos gestionados en un dispositivo. Cada objeto tiene una identificación única llamada OID (Identificador de Objeto).

Además, existen de tres tipos de MIBs: públicas, experimentales y privadas. Las MIBs públicas se encuentran definidas mediante estándares y ofrecen información general del sistema. Las MIBs experimentales están en proceso de desarrollo por parte de los grupos de trabajo de Internet. Por último, las MIBs privadas son definidas por los fabricantes individuales y brindan información más específica y detallada sobre sus dispositivos, ampliando las capacidades de las MIBs estándar (Gobantes Martínez, 2023).

Figura 8
Diagrama de árbol de MIB



Fuente: Tomado de (Manageengine, s.f.)

El protocolo SNMP admite operaciones básicas, destacando:

- **Get request:** Mediante esta operación podemos obtener información específica del dispositivo.

- **Set request:** Con esta solicitud puede cambiarse la configuración en los dispositivos remotos.
- **Traps:** Son eventos y notificaciones enviados al gestor SNMP.

El protocolo SNMP tiene tres versiones actualmente: SNMP V1, SNMP V2C y SNMP V3 (Gobantes Martínez, 2023):

- **SNMP V1:** Es la versión antigua de este protocolo, hoy en día los fabricantes han dejado de implementarlo en sus dispositivos, puesto que esta versión presenta diversas restricciones significativas, ya que no es apropiada para administrar redes de gran envergadura y no permite una configuración sencilla de la transferencia de grandes volúmenes de datos.
- **SNMP V2C:** Fue definida en las RFC 1441-1452 en el año 1993, y aunque ha sido reemplazada por la versión 3, todavía es ampliamente utilizado puesto que ha cubierto ciertas limitaciones en comparación con su predecesor, la versión 1. Por otra parte, alguna de las mejoras más notables es la inclusión de la PDU GetBulkRequest, que permite al gestor recuperar eficazmente grandes cantidades de datos con una sola solicitud.
- **SNMP V3:** Actualmente es la última versión de SNMP definidas en las RFC 2273-2275 en el año 1997, abordando las preocupaciones seguridad y privacidad que presentaban sus predecesores. Proporciona métodos de autenticación y cifrados más fuertes.

Sin embargo, a pesar de ser la versión actual de este protocolo, los fabricantes de dispositivos todavía siguen incorporando versiones antiguas del protocolo SNMP, ya sea debido a su resistencia al cambio o al hecho de que los dispositivos y elementos en cuestión, cuyo diseño precede a la adopción de SNMPv3, todavía no han alcanzado el final de su ciclo de vida (Marcos García, 2021).

En definitiva, el protocolo SNMP permite realizar una monitorización exhaustiva en entornos de redes empresariales, proporcionando control y visión detallada de la infraestructura tecnológica, aportando características valiosas como:

- Supervisión Proactiva.
- Recopilación de datos.
- Alertas y notificaciones.

2.1.2.2. Monitoreo de Servidores

La monitorización de servidores es un proceso crítico, que tiene como implicancia la supervisión continua y sistemática, para poder garantizar el óptimo rendimiento, disponibilidad, eficiencia y desempeño. A lo largo de los años esta práctica se ha vuelto esencial en la era digital, ya que los servidores desempeñan un papel fundamental en la entrega de servicios en línea, el almacenamiento de datos y el funcionamiento de aplicaciones críticas. Al igual que la monitorización por ICMP, necesitamos mecanismos para poder recopilar y analizar una variedad de datos y métricas relacionadas con el funcionamiento de los servidores. El protocolo SNMP aporta un conjunto básico para realizar esta tarea, ya que al ser un estándar y estar presente de manera nativa en la mayoría de sistemas operativos, representa una manera sencilla de realizar las consultas. Asimismo, para los sistemas operativos Windows, existe el protocolo WMI patentado por Microsoft que ayuda a consultar los sistemas remotos.

También debemos indicar que la monitorización de servidores puede realizarse de manera local, es decir, instalando un software llamado agente, que tiene como finalidad la ejecución de scripts o realizar consultas directas en el servidor para luego entregárselos a la herramienta de monitoreo.

Realizar la monitorización de servidores permite obtener principalmente lo siguiente (Montero Cadena, 2022):

- Uso de CPU, almacenamiento y memoria RAM.
- Respuesta de red y latencia.
- Temperatura y salud de hardware.
- Estado de servicios y aplicaciones.

2.2. Monitorización en las Empresas

2.2.1. Evolución del Monitoreo en las Empresas

En la década de los 80 y 90 la monitorización de sistemas se realizaba de manera manual y rudimentaria. Los administradores de sistemas utilizaban herramientas de línea de comandos para monitorear los servidores. Existía gran limitación a la hora de obtener métricas y la detección de problemas dependía de la observación humana, en estas décadas surge el protocolo SNMP, con su versión 1, para luego en los 90s crear las versiones 2 y 2c (Livaction, 2022).

A mediados de los años 2000 el aumento de servicios digitales, la creciente evolución y complejidad tecnológica, permitió el desarrollo de herramientas de monitorización avanzadas y automatizadas. Estos permitían la recopilación automática de datos y la generación de alertas en caso de algún evento de tipo crítico. Sin embargo, se requería una configuración manual intensa y se carecía de capacidades de visualización avanzadas, es decir, dashboards. Fue en el año 1999 que aparece la primera versión de Nagios, y ser convierte en el primer software de monitorización, estableciendo los estándares de monitorización (Zidek, 2022).

Para el año 2010, la nube comenzaba a tomar un protagonismo significativo, las empresas la empezaban a adoptar y emergían aplicaciones web más sofisticadas. Es por ello que las soluciones de monitorización no podían quedarse atrás, y estos también empezaban a migrarse hacia la nube. Aparecen modelos de servicios como el SaaS, permitiendo a las empresas supervisar sus activos tecnológicos independientemente de la ubicación

geográfica. Esto también allanó el camino para la monitorización de recursos en la nube, como instancias de máquinas virtuales y servicios en la nube (Livaction, 2022).

En la actualidad, la monitorización en las empresas ha avanzado significativamente hacia la detección predictiva y la automatización avanzada. Se han implementado técnicas de aprendizaje automático, observabilidad y análisis de datos para predecir problemas potenciales antes de que ocurran. Las soluciones de monitoreo ahora son capaces de ajustar de manera automática los umbrales y realizar acciones correctivas (Harithsa, 2023).

En definitiva, la monitorización en las empresas ha evolucionado desde métodos manuales hasta soluciones automatizadas, integrales e inclusive orientadas a la nube. Esta evolución ha permitido a las empresas mantener un control más efectivo sobre sus infraestructuras tecnológicas y poder garantizar óptimo rendimiento de sus sistemas críticos.

2.2.2. Beneficios del Monitoreo en las Empresas

La monitorización en las empresas tiene crucial importancia en un entorno cada vez más digital y dependiente de la tecnología. A continuación, explicaremos algunos beneficios de la monitorización en las empresas (International IT, 2021):

a) Supervisión de la red

Supervisar todos los elementos de una red, incluyendo los dispositivos y el flujo de datos, es crucial para asegurar un rendimiento óptimo y mantener la salud de la red. A pesar de que esta labor puede resultar desafiante, las herramientas de mapeo automatizado incorporadas en las soluciones de monitoreo de redes brindan una valiosa solución, proporcionando una visión integral incluso en entornos de red altamente complejos.

b) Gestión de Riesgos y Cumplimiento

Las empresas que deben cumplir con normativas como LGPD, GDPR, PCI DSS, HIPAA, FISMA, SOX y otras, requieren soluciones de monitoreo adecuadas como parte de

su sistema de control interno para garantizar el cumplimiento. Esto complementa los controles de seguridad externos que ya están en funcionamiento.

c) Prevención del Tiempo de Inactividad

El tiempo de inactividad representa un obstáculo significativo para la productividad y puede resultar en costos considerables, por ello el monitoreo desempeña un papel crucial en la prevención de interrupciones imprevistas. Esto permite detectar y abordar el problema de manera proactiva. Además, el monitoreo no solo contribuye a prevenir el tiempo de inactividad, sino que también posibilita que los equipos de TI optimicen el rendimiento para lograr operaciones más eficientes.

d) Identificar y Resolver Problemas Ágilmente

El monitoreo facilita la pronta identificación y aislamiento de problemas, ya sea una fluctuación en el tráfico, errores de configuración u otras cuestiones más críticas. Los mapas de red resultan efectivos para localizar rápidamente el origen del problema. Esto se traduce en una disminución del tiempo promedio de reparación (MTTR), permitiendo que el equipo de TI dedique tiempo a otras problemáticas.

e) Detectar Riesgos de Seguridad

La monitorización, a pesar de su enfoque principal en el rendimiento, también se convierte en una herramienta valiosa para la detección de amenazas de seguridad en la empresa. Al mantener una vigilancia constante sobre la actividad inusual o sospechosa, puede identificar incluso las amenazas más pequeñas antes de que se conviertan en un problema significativo.

f) Supervisar el Ancho de Banda

Cuando el ancho de banda de la empresa experimenta congestiones, se traduce en insatisfacción de los empleados y clientes, gracias a la monitorización del uso del ancho de banda, proporciona la capacidad de identificar el inicio de ralentizaciones en la red, además,

si la utilización del ancho de banda se acerca a niveles críticos, recibirá alertas que le permitirán tomar medidas como ajustar los protocolos de calidad de servicio (QoS) u otras acciones para mejorar el rendimiento.

g) Planificar la Capacidad

Las necesidades en constante cambio de los usuarios pueden complicar la predicción de cómo y dónde se consumirán los recursos de la empresa en el futuro. Al llevar a cabo una supervisión y seguimiento activo del rendimiento y uso, la plataforma de monitoreo facilita la identificación de las necesidades futuras de capacidad y la actualización de la red en consecuencia. Además, los datos históricos pueden desempeñar un papel clave en la justificación de inversiones futuras.

h) Retorno de la Inversión

La monitorización también ofrece un retorno de inversión (ROI) cuantificable, es decir, si se puede evitar una hora de inactividad al año, justificará fácilmente la inversión en supervisión. Además, al considerar la reducción de llamadas de soporte, el tiempo empleado en resolver problemas y el mantenimiento de niveles adecuados de rendimiento, rápidamente se percibirá un retorno tangible de la inversión.

2.3. Plataformas de Monitoreo

Las plataformas de monitoreo son conjuntos de software y recursos que permiten a las empresas supervisar y gestionar sus sistemas, aplicaciones y servicios de manera eficiente y centralizada. Estas plataformas recopilan datos y métricas en tiempo real de diversas fuentes y presentan información visual para poder tomar decisiones informadas y responder a problemas de manera proactiva (TechTarget, 2023).

Estas plataformas garantizan la disponibilidad, el rendimiento y la seguridad de los sistemas informáticos en las empresas. La elección de la plataforma adecuada depende de las necesidades específicas de las empresas y de su entorno tecnológico.

2.3.1. Clasificación de Plataformas de Monitorización

Clasificar las plataformas de monitoreo varía según sus características, enfoques y capacidades. Describiremos algunas de las principales categorías:

a) Plataformas Basadas en Open Source

Son plataformas que ofrecen una amplia variedad de características de monitoreo y al ser Open Source, son altamente personalizables y adecuadas para organizaciones que buscan opciones de bajo costo. Algunos ejemplos son: Nagios, Zabbix, Pandora FMS, entre otros (DevopsCube, 2023).

Figura 9
Plataforma de monitoreo Nagios

Fuente: Tomado de (Nagios.org, s.f.)

Figura 10
Plataforma de monitoreo Zabbix

Fuente: Tomado de (Zabbix.com, s.f.)

Figura 11

Plataforma de monitoreo Pandora FMS

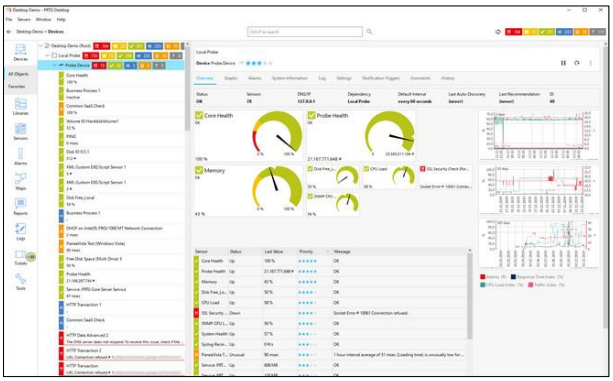
Fuente: Tomado de (Pandorafms.com, s.f.)

b) Plataformas Comerciales o Privativas

Son soluciones comerciales diseñadas para supervisar y gestionar sistemas, aplicaciones y redes en entornos empresariales y a diferencia de las plataformas Open Source, son desarrolladas y mantenidas por empresas que ofrecen sus productos como productos comerciales. A menudo se distinguen por su enfoque en la facilidad de uso y la integración con otros sistemas empresariales. Ejemplos: PRTG, SolarWinds, ManageEngine, entre otros (Acronis International GmbH, 2020).

Figura 12

Plataforma de monitoreo PRTG



Fuente: Tomado de (Paessler.com, s.f.)

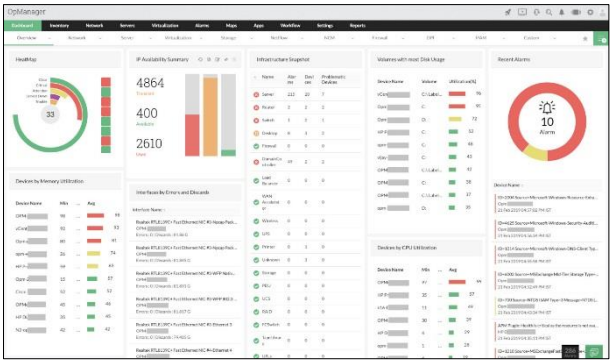
Figura 13

Plataforma de monitoreo SolarWinds

Fuente: Tomado de (Solarwinds.com, s.f.)

Figura 14

Plataforma de monitoreo ManageEngine



Fuente: Tomado de (Manageengine.com, s.f.)

2.3.2. Comparativa de Plataformas de Monitoreo Privativas y Open Source

Las plataformas de monitoreo privativas suelen ofrecer una experiencia más completa y con mayor soporte, mientras que las soluciones de código abierto brindan flexibilidad y opciones económicas. En la siguiente tabla se muestra una comparativa entre estos tipos de plataformas de monitorización (Vega Picon, 2018):

Tabla 1

Comparativa plataformas de monitoreo privativas y open source

	Privativas	Open Source
Características	Ofrecen interfaces intuitivas y amigables. Amplia gama de funciones y análisis avanzados. Proporcionan soporte técnico y actualizaciones. Integración con sistemas empresariales y herramientas.	Altamente personalizables y ajustables a necesidades específicas. Comunidad activa que proporciona soporte y desarrollo continuo. Integración con otras herramientas y sistemas de código abierto.
Ventajas	Mayor soporte, documentación y facilidad de implementación. Funcionalidades avanzadas para entornos empresariales complejos. Interfaz de usuario amigable y atractiva.	No tienen costos de licencia, más económicas en implementación. Adaptación flexible a entornos y requisitos específicos. Base de usuarios activa que comparte conocimientos y desarrolla características.
Consideraciones	Licencias y costos asociados. Dependencia a largo plazo del proveedor. Limitaciones en personalización y adaptación.	Requieren más tiempo y esfuerzo para configurar y dominar. Soporte de la comunidad.

	Algunas funciones avanzadas pueden no estar disponibles.

Fuente: Elaboración propia

2.3.3. Ventajas del Uso de Plataformas de Monitoreo Open Source

Son muchas las ventajas del uso de plataformas de monitoreo Open Source, a continuación, describiremos las más resaltantes (Portero López, 2021):

a) Costo: Las plataformas de monitoreo Open Source son gratuitas, resultando ahorro significativo en comparación con las soluciones comerciales. No hay costos de licencia ni tarifas de suscripción, convirtiéndolo en una opción atractiva para empresas con presupuestos limitados.

b) Flexibilidad: Suelen ser flexibles en términos de integración con otras herramientas y sistemas. Permitiendo a las organizaciones construir soluciones de monitoreo que se ajusten a su entorno tecnológico existente.

c) Personalización: Optar por una plataforma de monitoreo Open Source representa la posibilidad de personalizar y ajustar a las necesidades específicas de la empresa, esto permite un monitoreo más preciso y adecuado a su infraestructura tecnológica.

d) Transparencia y Control: Al tener acceso al código fuente, las empresas tienen visibilidad total sobre cómo funciona la plataforma y pueden identificar y resolver problemas sin la dependencia de terceros. Esto brinda un mayor nivel de control.

e) Constante Innovación: La naturaleza Open Source fomenta la innovación constante. Las nuevas características, mejoras y actualizaciones suelen ser desarrolladas por la comunidad y se comparten en beneficio de todos los usuarios.

f) Comunidad Activa: Las plataformas de monitorización Open Source a menudo tienen comunidades activas de usuarios y desarrolladores en todo el mundo, colaborando con

el propósito de mejorar y mantener la plataforma. Esto proporciona acceso a soporte y conocimientos a través de foros, blogs y documentación en línea.

g) **Escalabilidad:** Estas plataformas suelen ser escalables y pueden adaptarse a medidas cada vez mayores según el requerimiento de la infraestructura de la empresa. Esto permite un monitoreo constante y eficiente en cualquier escala.

2.4. Plataforma de Monitoreo Pandora FMS Open Source

2.4.1. Introducción a Pandora FMS

Pandora FMS es una plataforma de monitoreo Open Source que se utiliza para supervisar y gestionar la infraestructura tecnológica en una variedad de entornos, como empresas, organizaciones gubernamentales y proveedores de servicios. Esta solución permite a los administradores de sistemas y equipos de operaciones de TI obtener información en tiempo real sobre el rendimiento y la disponibilidad de los recursos tecnológicos, permitiendo tomar decisiones e identificar problemas para ser mitigados (Vega Picon, 2018).

2.4.1.1. Historia

Pandora FMS nació a finales del año 2002, desarrollado principalmente por el actual CEO y fundador Sancho Lerena, en España. La plataforma se concibe por necesidad propia del autor de contar con graficas potentes y poder agregar datos de diferentes fuentes (Pandora FMS).

Inicialmente el proyecto fue nombre como "Pandoramon", y en el año 2005 se funda oficialmente la empresa Ártica Soluciones Tecnológicas, con ello decidieron renombrarlo a "Pandora"; sin embargo, a finales del año 2006 se agrega la coletilla FMS, quedando "Pandora FMS".

Durante todos estos años, Pandora FMS se ha consolidado como una de las plataformas de monitoreo con una historia exitosa, puesto que han sido muchas versiones, parches y

actualizaciones que han transformado lo que en sus orígenes era un proyecto para resolver problemas técnicos. Gracias a la colaboración de decenas de programadores, técnicos de sistemas, usuarios y clientes, hoy día Pandora FMS es una herramienta profesional de monitorización y gestión de grandes entornos.

2.4.2. Principales Características

Pandora FMS está publicado con licencia GPL 2.0 y la primera línea de código la escribió el CEO de la empresa en 2004 de manera oficial. En esa época, el software libre estaba en plena efervescencia y MySQL todavía era una compañía independiente.

Pandora FMS cuenta con muchas características, destacando principalmente las siguientes (Montero Cadena, 2022):

a) **Monitoreo Multiservicio:** Supervisa servidores, redes, aplicaciones, bases de datos y más recursos tecnológicos.

b) **Notificaciones y Alertas:** Configura reglas de alerta con notificaciones por correo, sonidos y Telegram.

c) **Visualización Gráfica:** Ofrece gráficos en tiempo real y varios tipos de representación de datos.

d) **Mapas de Red:** Crea mapas visuales de la infraestructura de red y sus dependencias.

e) **Automatización:** Detecta dispositivos automáticamente y aplica plantillas de monitoreo.

f) **Escalabilidad:** Adaptable a entornos pequeños y grandes, con gestión distribuida.

2.4.3. Funcionalidades de la Plataforma

A continuación, se detallan las funcionalidades más importantes de Pandora FMS Open Source (Pandora FMS, 2021):

a) Monitorización de Redes

- Monitorización de Tráfico: Soporte para sFlow, NetFlow y JFlow para la monitorización del tráfico de red.
- Compatibilidad IPv4 e IPv6: Admite ambas versiones de IP para una amplia cobertura.
- Rendimiento del Equipo: Controla el uso de CPU, memoria y disco.
- Monitorización Programada: Programa chequeos en fechas y horas específicas.
- Puertos Físicos y Lógicos: Muestra puertos de routers y switches, abiertos y en uso.
- Sondas Intermedias: Distribuye sondas para la monitorización distribuida.
- Acceso Remoto Linux/Unix: Consulta equipos remotamente a través de SSH.
- Pérdida de Paquetes: Supervisa la pérdida de paquetes en interfaces de red.
- Monitorización de Interfaces: Controla ancho de banda, disponibilidad, errores, y más.
- Diagramas de Red Automáticos: Representa la red en diagramas actualizados automáticamente.
- Compatibilidad SNMP e ICMP: Admite SNMP e ICMP en múltiples versiones.
- Acceso Remoto Windows: Consulta equipos Windows de forma remota usando WMI.
- Recolección de Logs: Captura logs simultáneamente con la monitorización, sin límites de tamaño.
- Mapas Geográficos: Mapas en tiempo real muestran la ubicación de dispositivos con seguimiento de GPS.

b) Sistema de Permisos y Perfiles

- Multitenant: Permite dar servicio a múltiples clientes o grupos sin visibilidad entre ellos.
- Perfiles y Accesos Segregados: Usuarios en un grupo pueden tener funciones distintas.
- Auditoría Interna: Registra acciones de usuarios, incluyendo intentos de acceso fallidos.
- Recuperación de Contraseñas: Usuarios pueden recuperar contraseñas olvidadas.

- Autenticación Flexible: Ofrece autenticación propia y es compatible con Active Directory, LDAP y SAML.
- Política de Contraseñas: Puede imponer políticas de seguridad, como cambios y contraseñas fuertes.
- Doble Autenticación: Utiliza métodos como Google Auth para una autenticación adicional.

c) Monitorización Servidores y Equipos

- Tarjeta de Red: Controla disponibilidad y carga por tarjeta de red.
- Acciones Correctivas Locales: Ejecuta acciones en agentes según condiciones predefinidas.
- Información de Operación: Supervisa ventiladores y temperatura interna.
- Monitorización de Pantallas: Captura salidas de comandos para revisión.
- Almacenamiento: Controla disponibilidad, espacio y puntos de montaje.
- Detección Automática: Detecta nuevos sistemas de almacenamiento y puntos de montaje.
- Privilegios Limitados: Ejecuta agentes con usuarios sin privilegios.
- Uso de Proxies: Utiliza proxies para enviar información si los agentes no pueden acceder al servidor central.
- Watchdog de Servicios: Reinicia servicios y procesos en caso de fallo.
- Entornos Virtuales: Monitoriza una amplia gama de entornos virtuales.
- Agentes Locales y Remotos: Monitoriza equipos con agentes locales y remotos.
- Operación de Hardware: Controla CPU, RAM, memoria virtual, procesos, y más.
- Soporte Multiplataforma: Compatible con diversas arquitecturas y sistemas operativos.
- Recogida de Datos Local: Almacena información localmente en caso de desconexión para enviarla posteriormente.

d) Monitorización de Entorno

- UPS: Compatible con los principales fabricantes.
- Aire Acondicionado: Registra el historial de uso y sensores, generando reportes y alertas.
- Control de Acceso: Registra el historial de acceso al centro de cómputo, generando informes y alarmas.
- Sensores IoT: Se integra con sistemas IoT a través de SNMP o Rest API para monitoreo de recursos.

e) Informes Integrados

- Informes SLA: Genera informes diarios, semanales, mensuales y globales (por períodos) para evaluar el cumplimiento de SLAs.
- Informes de Disponibilidad: Muestra el rendimiento con pruebas, incluyendo porcentaje de éxito y fallo.
- Informes Personalizados: Permite definir y aplicar filtros a datos para informes personalizados tipo "Top-N."
- Paradas Planificadas: Excluye ventanas de mantenimiento de los informes.
- Vistas Gráficas: Crea paneles gráficos personalizados con datos de monitorización.
- Datos en Tiempo Real: Presenta información en tiempo real, no datos precalculados.
- Acceso Web en Tiempo Real: Administra Pandora FMS en tiempo real desde una aplicación web para navegadores modernos.
- Presentación Centralizada: Ofrece una interfaz única para datos en diferentes formatos, incluyendo gráficos, pantallas, dashboards y listados.

f) Sistema de Alertas

- Generación y Envío de Alarmas: Genera alertas y envía notificaciones inmediatas por mensaje de texto, correo electrónico y Telegram, además de alertas en pantalla.

- Auto Validación de Eventos: Los eventos se autovalidan cuando se resuelve la causa original.
- Acciones Correctivas Manuales: Permite a los operadores tomar medidas manuales sobre eventos, como diagnósticos o apertura de incidencias.
- Formato de Envío Programable: Los usuarios pueden definir el formato de envío de alertas para integración con diferentes plataformas a través de API Rest.
- Consola de Avisos Sonoros: Ofrece avisos audibles basados en filtros de origen y criticidad, permitiendo notificaciones sonoras.

g) Monitorización de Bases de Datos

- Bases de Datos Relacionales Comerciales Soportadas: Ofrece soporte para Oracle, Sybase, Informix, DB2, Microsoft SQL Server, MySQL y PostgreSQL.
- Bases de Datos NoSQL Comerciales Soportadas: Incluye soporte para motores como MongoDB, RavenDB, HBase y Cassandra.
- Monitorización de Almacenamiento: Supervisa el almacenamiento físico, disk groups y tablespaces (datafiles).
- Disponibilidad: Informa sobre la disponibilidad mediante la apertura y cierre de conexiones y servicios a nivel de sistema operativo.
- Transacciones: Proporciona información sobre bloqueos de la base de datos, sesiones, y cursores abiertos.
- Registros de Eventos y Advertencias: Registra errores, advertencias, estado de usuarios, sesiones, procesos de replicación, actualización de datos y verificación de backups.
- Consumo de CPU: Identifica el consumo de la base de datos en el servidor que la aloja.
- Uso de Caché: Muestra el consumo de la caché por la base de datos.
- Conexiones en Tiempo Real: Monitorea el movimiento en tiempo real de las conexiones y su estado.

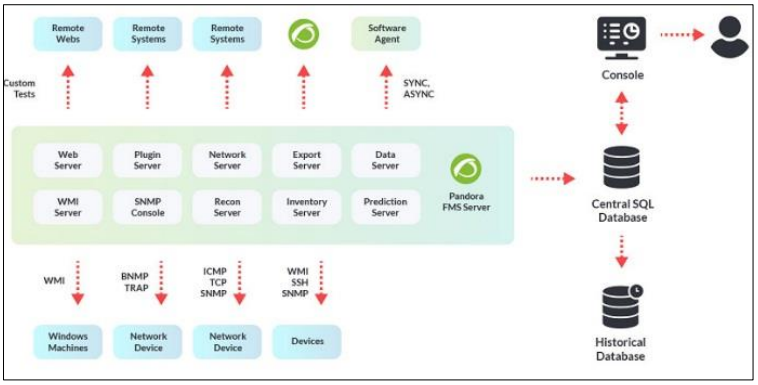
- Fallas en Jobs: Informa de fallos en la ejecución de trabajos programados.
- Fragmentación: Identifica el nivel de fragmentación en almacenes de datos.
- Errores en Backup: Genera alarmas por fallos en backups, tanto manuales como programados.

2.4.4. Arquitectura de Pandora FMS Open Source

El componente vital y donde se almacena casi toda la información es la base de datos MySQL. Todos los componentes de Pandora FMS se pueden replicar y funcionar en un entorno de HA puro (Activo/Pasivo) o en un entorno de grupo o clúster (Activo/Activo con balanceo de carga) (Pandora FMS).

Los Servidores de Pandora FMS, con la información generada por ellos mismos o por los Agentes, introducen los datos y la información en la base de datos. La Consola web es la parte encargada de mostrar los datos y de interactuar con el usuario final. Los Agentes Software son aplicaciones que corren en los sistemas monitorizados y recolectan la información para enviarla a los servidores Pandora FMS.

Figura 15
Arquitectura de Pandora FMS



Fuente: Tomado de (Pandorafms.com, s.f.)

2.4.4.1. Servidores de Pandora FMS

Los Servidores están integrados en una única aplicación, llamada de forma genérica Pandora Server, que es una aplicación multihilo que ejecuta de forma concurrente diferentes instancias o servidores especializados de Pandora FMS (Pandora FMS).

A continuación, iremos describiendo los servidores de Pandora FMS:

a) Data Server: Solamente procesa la información enviada por los Agentes Software, los cuales construyen un paquete de información en formato XML y lo entregan en un directorio específico que el servidor de datos procesa primero y luego almacena su resultado en la base de datos.

b) Network Server: Ejecuta tareas de monitorización remota a través de la red: chequeos ICMP, peticiones TCP y peticiones SNMP.

c) SNMP Trap Server: Este servidor utiliza el daemon estándar del sistema de recolección de traps, el snmptrapd: Recibe traps SNMP y la Consola SNMP de Pandora FMS los procesa y almacena en la base de datos. También se ocupa de lanzar las alertas asociadas a traps SNMP que hayan sido definidas.

d) WMI Server: Este es el servidor dedicado para monitorizar de forma remota sistemas Windows mediante el protocolo WMI.

e) Discovery Server: Empleado para explorar regularmente la red y detectar nuevos sistemas en funcionamiento y aplicar una plantilla de monitorización y comenzar a monitorizar inmediatamente.

f) Plugin Server: Ejecuta chequeos complejos de forma remota mediante scripts personalizados, gestionándose de forma centralizada. Esto permite a un usuario avanzado definir sus propias pruebas complejas e integrarlas en la aplicación para que se puedan usar de forma cómoda y centralizada desde Pandora FMS.

g) **Web Server:** Realiza comprobaciones web completas, como el proceso de identificación de un usuario, paso de parámetros por formulario, comprobación de contenidos, navegación por menús, etc. Se utiliza para chequeos de disponibilidad verdadero/falso y para obtener tiempos de latencia de experiencia completa de navegación.

2.5. Fundamentos de Implementación de Pandora FMS Open Source

2.5.1. Requisitos Mínimos de Hardware

Actualmente, Pandora FMS puede instalarse en servidores físicos, virtuales, inclusive en Raspberry Pi. Es importante conocer el entorno y aproximar la cantidad de métricas a monitorizar. En la siguiente tabla se muestra de manera detalla los requisitos mínimos de hardware para la instalación de Pandora FMS Open Source (Pandora FMS).

Tabla 2
Requisitos mínimos de hardware

Hardware	Pequeño: Hasta 5.000 módulos	Mediano: Hasta 15.000 módulos	Grande: Hasta 30.000 módulos	Extra Grande: Hasta 80.000 módulos
CPU	2 núcleos a 2 GHz	4 núcleos a 2,5 GHz	6 núcleos a 3 GHz	10 núcleos a 3 GHz
RAM	4 GB	8 GB	16 GB	32 GB
Velocidad de almacenamiento	7200 rpm	15K rpm o SSD	SSD	SSD
Espacio mínimo	40GB mínimo, 60GB recomendado	60GB mínimo, 150GB recomendado	120GB mínimo, 250GB recomendado	250GB mínimo, 400GB recomendado

Fuente: Tomado de (Pandorafms.com, s.f.)

2.5.2. Requisitos Mínimos de Software

Oficialmente Pandora FMS necesita GNU/Linux para el servidor y la consola, por ello el termino EL8 es utilizado para indicar el conjunto de sistemas operativos soportados oficialmente, el cual está conformado por Rocky Linux 8, AlmaLinux 8 y RedHat 8 (Pandora FMS).

Adicionalmente, en el servidor se debe de ejecutar el servicio de Pandora FMS Server con permisos de root. Es necesario a su vez que se tengan permisos de escritura en el directorio del servidor: /var/spool/pandora/

Para la consola, se puede utilizar desde cualquier navegador web. Apache debe tener permisos de lectura y ejecución sobre los ficheros de la Consola. También el fichero config.php debe tener los permisos 600 (lectura y escritura para administrator/root). Se requiere usar PHP en su versión 8.

Con respecto a la base de datos, se puede usar MySQL Standard para entornos pequeños y Percona Server for MySQL para entornos grandes.

Adicionalmente se requiere facilitar la comunicación desde el servidor Pandora FMS a toda su red, siendo obligatorio la necesidad de los siguientes puertos:

Tabla 3
Requisitos mínimos de puertos

Puerto	Protocolo	Servicio/Proceso	Descripción	Dirección
80	TCP	Servidor Pandora FMS	Monitorización web para servidor WUX	Servidor Pandora FMS → Servidor a monitorizar
161	UDP	Consola y Servidor Pandora FMS	Monitorización mediante SNMP Polling	Servidor Pandora FMS → Servidor a monitorizar
443	TCP	Servidor Pandora FMS	Monitorización web para servidor WUX	Servidor Pandora FMS → Servidor a monitorizar
ICMP	ICMP	Consola y Servidor Pandora FMS	Monitorización de red con ICMP	Servidor Pandora FMS → Servidor a monitorizar

Fuente: Tomado de (Pandorafms.com, s.f.)

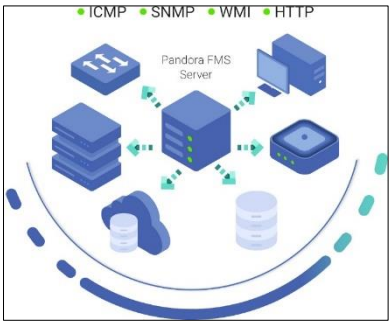
2.5.3. Diseño de Arquitectura de Monitoreo con Pandora FMS Open Source

Pandora FMS Open Source, cuenta con diferentes diseños de arquitectura para la monitorización, desde entornos accesibles, hasta redes con dificultad de acceso, a continuación, iremos detallando cada una de ellas (Pandora FMS):

2.5.3.1. Redes Accesibles

a) **Monitorización Remota Centralizada:** donde, desde el servidor de Pandora FMS, se puede acceder a todas las máquinas y/o dispositivos para sondear remotamente.

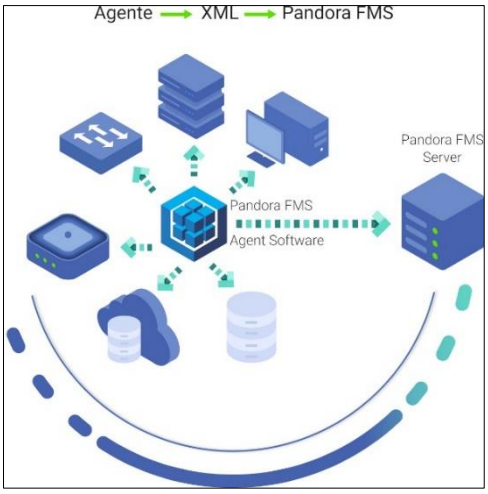
Figura 16
Arquitectura de monitoreo remota



Fuente: Elaboración Propia

b) **Monitorización Basada en Agentes:** donde, desde los Agentes Software instalados en las máquinas monitorizadas, pueden llegar sin problemas al servidor de Pandora FMS.

Figura 17
Arquitectura de monitoreo con agentes software



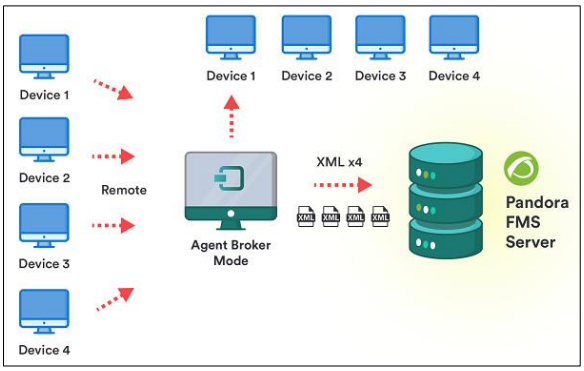
Fuente: Elaboración Propia

2.5.3.2. Redes con Dificultad de Acceso

a) **Modo Broker:** Red remota no alcanzable por los chequeos remotos de Pandora FMS.

Figura 18

Arquitectura de monitoreo modo broker

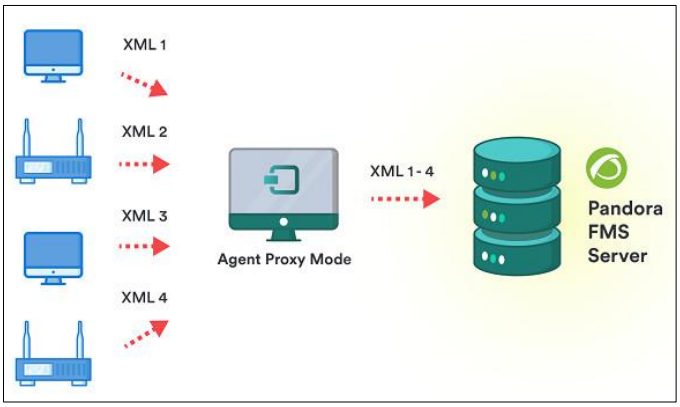


Fuente: Tomado de (Pandorafms.com, s.f.)

b) Modo Proxy: Agentes Software que no tienen acceso al servidor de Pandora FMS, utiliza la característica de proxy.

Figura 19

Arquitectura de monitoreo modo proxy



Fuente: Tomado de (Pandorafms.com, s.f.)

2.5.4. Métricas y Umbrales en Pandora FMS Open Source

2.5.4.1. Métricas

Las métricas también llamados módulos en Pandora FMS, son unidades de información almacenadas dentro de un agente con los cuales se extrae la información del dispositivo o servidor al que apunta el agente. Cada módulo puede almacenar solo un tipo de métrica, dentro de un agente cada módulo tiene un nombre único. Los módulos tienen alguno de los varios tipos de datos, como son el booleano, numérico o alfanumérico, entre otros (Pandora FMS).

Los módulos tienen diferentes estados asociados:

- No iniciado: En espera de recepción de datos.
- Normal: Recibiendo datos con valores comprendidos fuera de los umbrales de advertencia o crítico.
- Advertencia: Datos comprendidos en ese umbral.
- Crítico: Datos comprendidos en ese umbral.
- Desconocido: El módulo ha estado funcionando y ha dejado de recibir información durante un tiempo determinado.

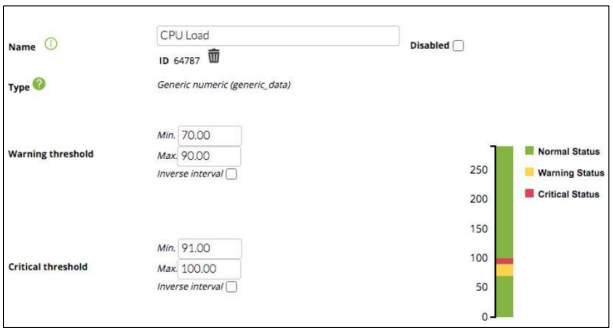
En la consola de Pandora FMS los estados suelen representarse por colores como son: celeste (No iniciado), verde (Normal), amarillo (Advertencia), rojo (Crítico), gris (Desconocido).

2.5.4.2. Umbrales

Pandora FMS permite establecer umbrales para definir el estado que un chequeo tendrá basándose en los datos que haya recogido, los tres estados posibles son: Normal, Warning y Critical (Pandora FMS).

- Estado Advertencia: Si el valor numérico del módulo se encuentra en los límites inferior y superior. Si no se especifica límite superior todo valor mayor al límite inferior ocasionará el cambio de estado.
- Estado Crítico: Se comporta de igual forma que el warning status.
- Intervalo Inverso: Presente tanto para el umbral warning como critical, si se encuentra activado, el módulo cambiará de estado cuando sus valores estén fuera del intervalo especificado. También funciona para módulos alfanuméricos.
- Porcentaje: Si está activado, el valor del umbral se interpreta como un porcentaje. En caso de que los umbrales warning y critical se solapen en algún rango, siempre prevalecerá el umbral critical.

Figura 20
Definición de umbrales en Pandora FMS



Fuente: Tomado de (Pandorafms.com, s.f.)

2.5.5. Definición de Agentes Software para el Monitoreo

Los agentes software están disponibles en diferentes formatos para instalarse en una gran variedad de sistemas operativos, como se muestra en la tabla (Pandora FMS):

Tabla 4
Requisitos de sistema operativo para agentes software

Componente	Sistema Operativo
Pandora Agent 4.0 o superior	RedHat Enterprise (RHEL) 6.x y 8. Fedora 34. CentOS 6.x, 7 y 8. AlmaLinux. SLES 11 SP1 o posterior. OpenSUSE 11.x o posterior. Debian 5.x o posterior. Ubuntu Server o Desktop versión 11 o posterior. Linux Mint. Elementary OS. Manjaro. HPUX B.11.11 o posterior, con Perl 5.8. AIX 4.3.3 o posterior, con Perl 5.8. AIX 7.1 y 7.2. BSD Systems (NetBSD, OpenBSD, FreeBSD), con Perl 5.8. MacOS X 10.6 o posterior. Solaris 8 o posterior, con Perl 5.8. Windows NT4 (ver notas especiales de esta version). Windows XP. Windows 2000. Windows 2003. Windows 2008. Windows 7. Windows 8. Windows 10.

	Windows 11. Windows 2012. Windows server 2016. Windows server 2019.
Pandora Android Agent 2.0 o superior	Android 6 o superior
Pandora Embedded Agent 4.0 o superior	Dispositivos embebidos, requiere compilación

Fuente: Elaboración propia

Los agentes software se encuentran en ejecución en los sistemas operativos de los cuales recogen información, realizando un chequeo para cada módulo. Las directivas propias del agente software sirven para recoger ciertos datos directamente del sistema operativo como, por ejemplo, el uso de CPU, memoria, eventos, entre otros. El agente ejecuta comandos propios del sistema operativo siguiendo instrucciones de scripts predefinidos.

Toda la información de los chequeos realizados se plasma en un único fichero de datos en formato XML, que es enviado a través del protocolo Tentacle al servidor de Pandora FMS en un intervalo predeterminado de 300 segundos. También es posible transmitir los paquetes usando SSH o FTP.

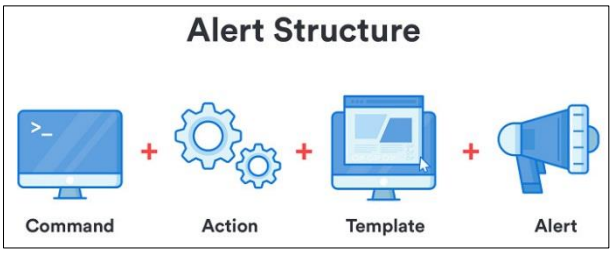
2.5.6. Alertas y Eventos en Pandora FMS

2.5.6.1. Alertas

En Pandora FMS, las alertas funcionan mediante la definición de unas condiciones de disparado, unas acciones elegidas para esa alerta, y finalmente la ejecución de unos comandos en el servidor de Pandora FMS, que se encargarán de llevar a cabo las acciones configuradas (Pandora FMS).

Figura 21

Estructura de las alertas



Fuente: Tomado de (Pandorafms.com, s.f.)

- **Comandos:** Especifican qué se hará; será la ejecución que realizará el servidor de Pandora FMS al disparar la alerta.
- **Acciones:** Especifican cómo se hará; son las personalizaciones de los argumentos del comando.
- **Plantillas:** Especifican cuándo se hará; definen las condiciones para disparar la acción o acciones.

2.5.6.2. Eventos

Los eventos son el registro y una parte fundamental de un sistema de monitorización. El sistema de eventos de Pandora FMS permite ver un registro en tiempo real de todos los acontecimientos que ocurren en los sistemas monitorizados. Por defecto, en la vista de eventos se verá una instantánea de lo que está sucediendo en ese momento (Pandora FMS).

Los eventos se clasifican según su severidad y son representados con los siguientes colores:

- Mantenimiento (azul).
- Informativo (gris).
- Normal (verde).
- Menor (rosa).
- Advertencia (amarillo).
- Mayor (marrón).

- Crítico (rojo).

Adicionalmente se pueden realizar diversas acciones sobre eventos:

- Cambiar su estado (validado o en progreso).
- Cambiar el propietario.
- Eliminar.
- Mostrar información adicional.
- Añadir un comentario.
- Realizar respuestas personalizables.

2.5.7. Consolas Visuales y Dashboards

2.5.7.1. Consolas Visuales

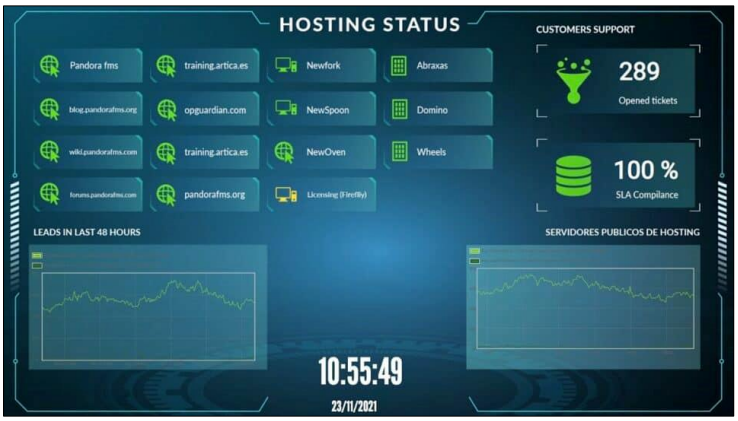
Pandora FMS permite construir mapas visuales donde cada usuario define su propia forma de representar visualmente la monitorización. El editor de consolas visuales permite al usuario, arrastrando elementos con el ratón, diseñar de forma visual el aspecto final, eligiendo el fondo y los iconos que representan el estado de cada aspecto relevante que quiere mostrar (Pandora FMS).

Con Pandora FMS vienen una serie de iconos, pero el usuario puede fácilmente personalizar los suyos. Diferentes consolas visuales pueden interactuar entre sí, visualizando de forma jerárquica el estado de mapas que están "por debajo" en un mapa superior, pudiendo conceptualizar, de esta forma, la monitorización, y visualizando a alto nivel toda una serie de elementos.

A continuación, se muestran algunos diseños de consolas visuales:

Figura 22

Consola visual hosting status



Fuente: Tomado de (Pandorafms.com, s.f.)

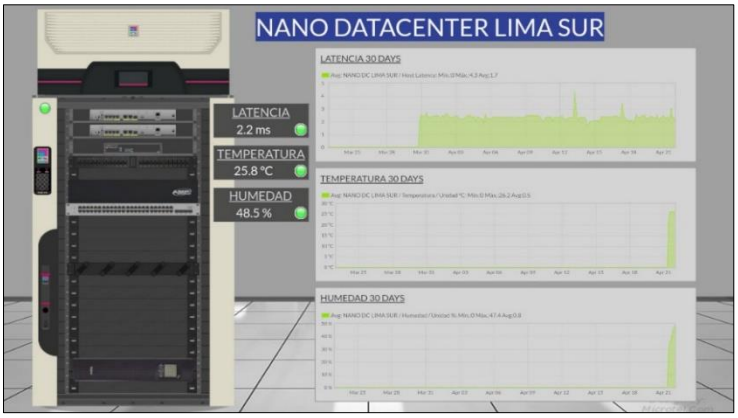
Figura 23

Consola visual soporte

Fuente: Tomado de (Pandorafms.com, s.f.)

Figura 24

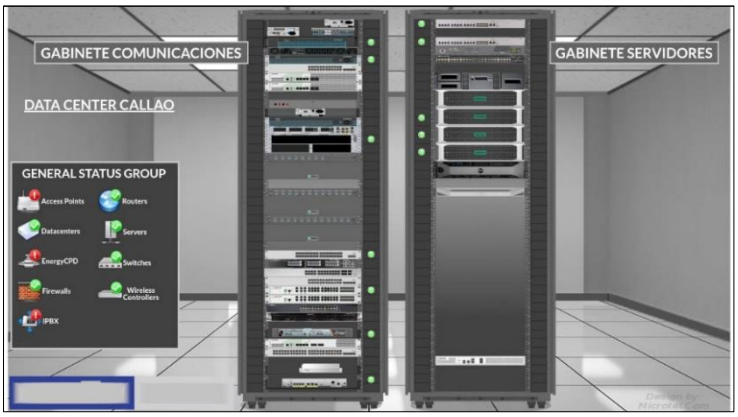
Consola visual nano datacenter



Fuente: Tomado de (Microtelperu.com, s.f.)

Figura 25

Consola visual datacenter



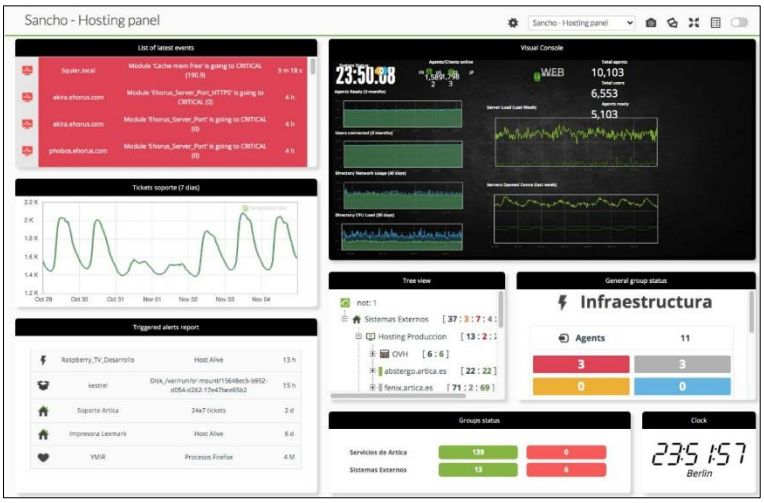
Fuente: Tomado de (Microtelperu.com, s.f.)

2.5.7.2. Dashboards

Los cuadros de mandos (Dashboard) es una funcionalidad de Pandora FMS que permite que cada usuario construya su propia página de monitorización. Se puede añadir más de una página, y en ella se pueden añadir mapas de monitorización, gráficas y resúmenes de estado, entre otros elementos llamados widgets (Pandora FMS).

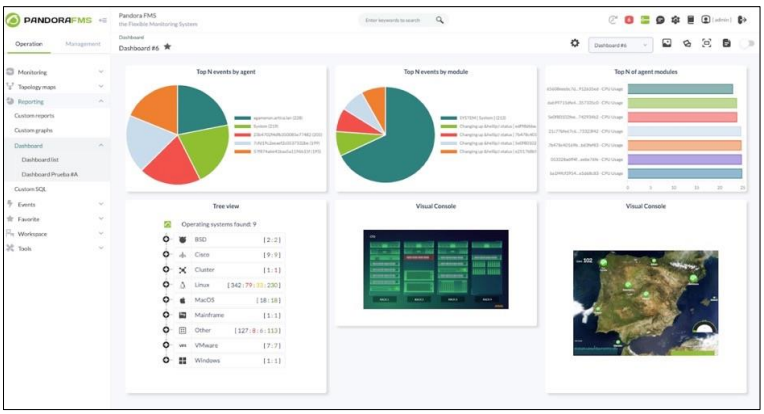
Los dashboards funcionan mediante un modo de presentación, lo cual consiste en seleccionar aquellas páginas de monitorización, que serán mostradas de manera automática mediante un intervalo de tiempo. Por lo general los dashboards están destinadas a mostrarse en las pantallas de monitoreo de la empresa. A continuación, se muestran algunos dashboards:

Figura 26
Dashboard hosting panel



Fuente: Tomado de (Pandorafms.com, s.f.)

Figura 27
Dashboard general status



Fuente: Tomado de (Pandorafms.com, s.f.)

2.6. Términos Básicos

- **Apache:** Es un servidor web de código abierto ampliamente utilizado. Actúa como intermediario entre los usuarios y sitios web, entregando contenido como páginas web y archivos (Hostinger, 2023).
- **Backup:** También llamado copia de seguridad, es el proceso de crear réplicas de datos y archivos importantes para prevenir la pérdida de información en caso de fallos, errores o eliminación accidental (IONOS, 2023).

- **Daemon:** Es un programa informático que se ejecuta en segundo plano en sistemas operativos tipo GNU/Linux y Unix. Estos procesos, también son llamados "servicios" en entornos Windows, realizan tareas sin interacción directa del usuario. Los daemons gestionan servicios esenciales del sistema, como servidores web, servicios de red y tareas programadas (Hertzog & Mas, 2017).
- **HA:** High Availability, se refiere a un diseño de sistema o red que busca minimizar la interrupción del servicio, asegurando que los servicios cruciales estén disponibles en todo momento. Esto se logra mediante la duplicación de componentes críticos, como servidores, redes o bases de datos, y la implementación de mecanismos de conmutación por error (Red Hat, Inc., 2022).
- **HTTP:** Hypertext Transfer Protocol, es el fundamento de la comunicación en la web. Define cómo los clientes, como navegadores web, solicitan recursos (como páginas web) a través de URLs a servidores (GoDaddy, 2021).
- **HTTPS:** Hypertext Transfer Protocol Secure, es una extensión del HTTP que añade seguridad mediante cifrado. Utilizado en la navegación web, HTTPS protege la privacidad y autenticidad de los datos transmitidos entre el navegador y el servidor (GoDaddy, 2021).
- **Hypervisor:** Es un software que permite la virtualización al crear y administrar múltiples máquinas virtuales (VM) en un único sistema físico (Red Hat, Inc., 2023).
- **IMAP:** Internet Message Access Protocol, es un protocolo de correo electrónico que permite a los usuarios acceder y gestionar sus correos electrónicos almacenados en un servidor remoto. A diferencia de POP3, IMAP mantiene los correos en el servidor en lugar de descargarlos localmente (Cloudflare, Inc.).
- **Latencia:** Es el tiempo que lleva que los datos viajen de un punto a otro en una red o sistema. Representa la demora entre el envío y la recepción de información. Se mide en

milisegundos (ms) y puede afectar la velocidad y la respuesta en las comunicaciones en línea (Amazon Web Services, Inc.).

- **Licencia GPL:** GNU General Public License, es un tipo de licencia de software libre creada por la Free Software Foundation. Garantiza libertades fundamentales a los usuarios, como ejecutar, estudiar, modificar y compartir el software (Free Software Foundation, Inc., 2022).
- **Multitenant:** Se refiere a una arquitectura de software o sistema en el cual una única instancia o infraestructura sirve a múltiples inquilinos o "tenants". Cada inquilino comparte los mismos recursos subyacentes, como servidores o bases de datos, pero opera de manera aislada y segura, con datos y configuraciones separados (Cloudflare, Inc.).
- **OID:** Object Identifier, es una cadena numérica única que identifica de manera única un objeto en una estructura de gestión de red, como SNMP (Simple Network Management Protocol). Cada OID representa un elemento específico, como un dispositivo o una métrica, en un árbol jerárquico (IBM Corporation, 2022).
- **Open Source:** Se refiere a software cuyo código fuente es accesible públicamente, permitiendo a los usuarios ver, modificar y distribuir libremente el software. Esto fomenta la colaboración, la transparencia y la innovación comunitaria (Red Hat, Inc., 2023).
- **Percona Server:** Es una base de datos de código abierto basada en MySQL que ofrece mejoras de rendimiento, confiabilidad y escalabilidad. Desarrollada por Percona, se centra en optimizar el rendimiento de MySQL con funciones avanzadas como el motor de almacenamiento InnoDB y mejoras en la administración de transacciones (Infranetworking Internacional, 2018).

- **PHP:** Es un lenguaje de programación de código abierto ampliamente utilizado para el desarrollo web. Diseñado para crear páginas web dinámicas, interactúa con servidores web para generar contenido en tiempo real (The PHP Group).
- **Ping:** Es una herramienta de diagnóstico de red utilizada para verificar la conectividad y la latencia entre dispositivos en una red IP, midiendo el tiempo que tarda un paquete en viajar desde el emisor hasta el receptor y viceversa (Paessler AG).
- **Polling:** Es un método mediante el cual un sistema de gestión de red envía solicitudes periódicas a dispositivos de red, llamados agentes SNMP, para obtener información sobre su estado y rendimiento (Pandora FMS, 2023).
- **POP3:** Post Office Protocol version 3, es un protocolo de correo electrónico que permite a los usuarios descargar mensajes de correo electrónico desde un servidor a su dispositivo local. Funciona en un modelo "descargar y eliminar", donde los mensajes se transfieren del servidor al cliente y luego se eliminan del servidor (Cloudflare, Inc.).
- **Proxy:** Es un intermediario entre los usuarios y los recursos de la red. Puede ser un servidor o software que redirige las solicitudes de los usuarios a través de su propia dirección IP (McAfee, LLC, 2021).
- **Push Notification:** Son mensajes enviados desde aplicaciones o servidores a dispositivos móviles o computadoras. Alertan a los usuarios sobre actualizaciones, eventos o información importante, incluso cuando la aplicación no está activa (IBM Corporation).
- **Scripts:** Es un conjunto de instrucciones o comandos escritos en lenguajes de programación como Python, JavaScript o Bash. Los scripts automatizan tareas y procesos, como manipulación de archivos, configuración y tareas repetitivas (SEO Estudios, 2020).

- **SLA:** Service Level Agreement, es un contrato entre proveedores y clientes que define los estándares y expectativas de calidad para los servicios ofrecidos. Especifica métricas como tiempo de actividad, velocidad de respuesta y resolución de problemas (Atlassian).
- **SMTP:** Simple Mail Transfer Protocol, es un protocolo de envío de correo electrónico. Permite a los clientes de correo electrónico enviar mensajes a servidores de correo para su posterior entrega (IBM Corporation, 2021).
- **Sondeo:** Se refiere a la práctica de realizar verificaciones o consultas repetidas a un dispositivo, recurso o sistema para obtener información actualizada (Nmap Software LLC).
- **SSH:** Secure Shell, es un protocolo de red que proporciona un canal seguro para la comunicación y el acceso remoto a sistemas y servidores. Utiliza cifrado y autenticación para proteger la confidencialidad e integridad de los datos transmitidos (Arsys, 2022).
- **Swap:** También conocida como área de intercambio, es un espacio en disco utilizado por el sistema operativo para almacenar temporalmente datos que no caben en la memoria RAM física (Hertzog & Mas, 2017).
- **TCP:** Transmission Control Protocol, es un protocolo de red fundamental que garantiza la entrega confiable y ordenada de datos en redes IP. Divide los datos en segmentos y los envía a través de conexiones establecidas entre emisor y receptor (IONOS, 2020).
- **Tentacle:** Es el protocolo de transferencia de datos que utilizan los Agentes Software y el Satellite Server para enviar datos al servidor de Pandora FMS. Tentacle es multiplataforma y utiliza por defecto el puerto 41121 (asignado por IANA) (Pandora FMS, 2021).
- **Traceroute:** Es una herramienta de diagnóstico de red que rastrea la ruta que toman los paquetes de datos desde un dispositivo origen hasta un destino en una red IP. Utiliza el

protocolo ICMP para enviar paquetes con incrementos de tiempo TTL (Time to Live) que son decrementados en cada salto de red (Fortinet, Inc).

- **Traps SNMP:** Son notificaciones automáticas que los dispositivos envían a un sistema de gestión cuando ocurre un evento significativo. Los eventos pueden incluir problemas, cambios de estado o condiciones predefinidas (IONOS, 2023).
- **Widgets:** Son elementos visuales y funcionales que se integran en interfaces gráficas, como en sistemas operativos, aplicaciones y sitios web (NeoAttack, 2021).
- **WMI:** Windows Management Instrumentation, es un conjunto de tecnologías en sistemas operativos Windows para administrar y monitorear recursos y servicios. Permite a los administradores y aplicaciones acceder a información sobre hardware, software y configuraciones en sistemas locales o remotos (Pandora FMS, 2023).
- **XML:** Extensible Markup Language, es un lenguaje de marcado que estructura y etiqueta datos para su almacenamiento y transmisión. Utilizado en aplicaciones web y sistemas, XML permite la representación jerárquica y flexible de información (Mozilla Corporation's, 2023).

2.7. Limitaciones para el Desarrollo del Proyecto

La primera limitación para el desarrollo del proyecto, fue el no contar con un diagrama de la topología de red de la empresa, lo cual evita tener una representación visual clara de la estructura y componentes de la red. Asimismo, resultaba difícil identificar posibles cuellos de botella y poder optimizar la distribución de dispositivos.

La segunda limitación son las credenciales de acceso a los diferentes dispositivos de comunicación, como el router, firewall, switches; imposibilitando la configuración y activación del protocolo SNMP para poder ser monitoreados en el futuro.

La tercera limitación fue el aprovisionamiento de recursos de hardware del servidor hypervisor Proxmox VE, debido a que en ese momento se contaba con máquinas virtuales

ocupando el 90% de los recursos. Por ello fue necesario realizar el análisis de capacidades para posteriormente realizar una ampliación de memoria y unidades de almacenamiento.

La cuarta limitación ha sido la centralización del monitoreo, es decir, la empresa al contar con servicios en la nube, estos requerían conectarse directamente hacia la plataforma de monitoreo ubicado en el Datacenter de la empresa. Por ello fue necesario adquirir una IP publica, para poder permitir una conexión VPN desde los servicios en la nube hacia la plataforma de monitoreo en la empresa.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

3.1. Ingreso a la Empresa

Quien suscribe, egresó de la Universidad Privada del Norte en el año 2018 en la carrera de Ingeniería de Sistemas Computacionales, Campus Breña. Con 10 años de experiencia laborando de manera independiente, ofreciendo diversos servicios a las empresas, desde mantenimiento a workstations y servidores, hasta implementaciones y configuraciones de entornos GNU/Linux. El rápido avance de la tecnológica me ha aportado diversas habilidades que posteriormente han resultado en potenciales servicios nuevos a ofrecer. Emocionado por comenzar mi carrera en el campo de la tecnología en una empresa en Lima, logré enviar varias solicitudes y realizar entrevistas, recibiendo una oferta de trabajo de la empresa Microtel.Com E.I.R.L., empresa dedicada al diseño e implementación de data centers, redes de networking, electricidad, entre otros. Pasé por un proceso de selección interesante, puesto que incluyó una serie de consultas técnicas y análisis de herramientas para los diversos recursos tecnológicos que la empresa tiene. En ese tiempo la empresa no contaba con un área de sistemas especifico, puesto que, de presentarse algún inconveniente o necesidad de servicios informáticos, recurría a la búsqueda de empresas que pudieran solventar los requerimientos.

Durante estas entrevistas, demostré habilidades en programación, redes y administración de sistemas, lo que me permitió destacar entre los candidatos. En Julio de 2018, comencé a laborar en Microtel.Com E.I.R.L. Fui recibido por el gerente general en ese entonces, José Lazo Moreno, quien me proporcionó una introducción a la empresa y su cultura. Asimismo, me mostró el lugar de trabajo y me presentó al personal de la empresa.

3.2. Funciones

Como encargado del área de sistemas, las responsabilidades incluían:

- Diseño y mantenimiento de la topología de red de la empresa.
- Implementar una solución de monitoreo de infraestructura TI económico.
- Mantenimiento de los servidores de la empresa, asegurando de que funcionaran sin problemas.
- Ayudar a los empleados con problemas técnicos y brindar asistencia en la resolución de problemas.
- Garantizar que todos los sistemas y software estén actualizados y protegidos contra amenazas de seguridad.
- Trabajar en equipo en proyectos de TI que requieran recursos tecnológicos ofrecidos a los clientes de la empresa.

3.3. Impacto en la Empresa

Durante estos años en Microtel.Com EIRL, tuve la oportunidad de participar en cursos de capacitación y desarrollo profesional para mejorar mis habilidades. También asistí a seminarios web relacionados con las últimas tendencias en tecnología de la información y monitorización. Con arduo trabajo y dedicación, he contribuido significativamente al funcionamiento sin problemas de los sistemas de la empresa. Demostrando capacidad para solucionar problemas técnicos y enfoque en la mejora constante, ayudando a la empresa a mantenerse competitiva en el sector.

3.4. Identificación del Problema

En el año 2018, Microtel.Com EIRL, contaba con una creciente infraestructura de TI, compuesta de diversos recursos tecnológicos, entre hardware y software, recursos on-premise y en la nube. Ante la diversidad de tecnologías, la empresa se encontraba en una situación donde la supervisión y gestión de la infraestructura TI eran desafiantes, puesto que enfrentaba varios problemas y limitaciones. La empresa carecía de una solución de monitoreo integral que le proporcionara una visión completa de su infraestructura de TI. Esto

resultaba en la incapacidad de identificar problemas de manera proactiva y tiempos de inactividad inesperados y no planificados.

La falta de una plataforma de monitoreo eficaz, dificultaba la detección temprana de problemas en la red y en los sistemas, dando como resultado retrasos en la resolución de problemas y en la insatisfacción de los empleados de la empresa. La gestión de recursos de TI se realizaba a través de terceros, solicitando a empresas locales la evaluación y resolución de los requerimientos, lo que requería una gran cantidad de tiempo y esfuerzo. A medida que Microtel.Com E.I.R.L. experimentaba un crecimiento constante, la falta de una solución de monitoreo se convertía en un obstáculo para su desarrollo futuro. No había una estrategia clara para abordar las necesidades de supervisión de la infraestructura TI a largo plazo.

Implementar Pandora FMS en la empresa, marcó un cambio significativo en la forma en que la empresa abordaba la supervisión y gestión de su infraestructura de TI. Pandora FMS proporcionó una visión integral de la red y sistemas de la empresa. La empresa ahora tiene la capacidad de detectar problemas antes de que impacten en los servicios, permitiendo tomar medidas proactivas para evitar tiempos de inactividad. La plataforma permitió a la empresa contar con alertas configuradas que notificaban sobre cualquier anomalía en tiempo real. Pandora FMS automatizó la gestión de recursos de TI, reduciendo la carga de las tareas rutinarias, como la asignación de recursos y la generación de informes, se realizaron de manera eficiente. La plataforma de monitoreo resultó ser escalable, permitiendo a la empresa crecer sin problemas, pudiendo establecer una estrategia a largo plazo para adaptarlo a las futuras necesidades de monitorización. Con la documentación detallada de Pandora FMS, pude adquirir habilidades en la administración de la plataforma, mejorando la eficiencia y la confianza de la empresa en la gestión y mantenimiento futuro de la solución.

A modo de resumen, la problemática que enfrentaba la empresa Microtel.Com EIRL era:

- Limitaciones en la supervisión de la infraestructura de TI, generando falta de visibilidad integral.
- Problemas de inactividad no planificada afectan la productividad y satisfacción.
- La demora en la resolución de problemas TI afecta la operatividad.
- Falta de eficiencia en la distribución de recursos de TI.
- Problemas tecnológicos recurrentes afectan la satisfacción y la productividad del personal.

3.5. Objetivo General

Implementar la plataforma de monitoreo open source Pandora FMS para la supervisión de los recursos tecnológicos de la infraestructura TI.

3.6. Objetivos Específicos

- Incrementar la cobertura de supervisión de la infraestructura de TI de la empresa.
- Reducir el tiempo de inactividad de los recursos TI.
- Mejorar el tiempo de respuesta a incidentes suscitados en la infraestructura TI.

3.7. Experiencia.

3.7.1. Participantes del Proyecto.

Para el desarrollo del proyecto, participaron los siguientes responsables:

Tabla 5
Participantes del proyecto

Responsables	
Trabajador	Cargo
Christian López	Coordinador del Proyecto
José Lazo	Representante del Proyecto

Fuente: Elaboración propia

3.7.2. Estrategias.

a) Colaboración Estrecha con Responsable TI

Se estableció una comunicación constante y una coordinación proactiva con el responsable de la Infraestructura TI de Microtel.Com EIRL, cargo ocupado por el Gerente General desde las etapas iniciales del proyecto. Esto permitió alinear las metas del proyecto con las necesidades y prioridades de la empresa. La participación activa del responsable de la Infraestructura TI, garantizó la identificación temprana de obstáculos y la toma de decisiones informadas. Dichas comunicaciones fueron establecidas mediante el uso de correos electrónicos y la plataforma de reuniones virtuales Google Meet.

b) Recopilación de Información Detallada de la Red Empresarial

Se llevó a cabo un minucioso levantamiento de información sobre la red empresarial de Microtel.Com EIRL. Esto incluyó desde la identificación de servidores, dispositivos de red, puntos de acceso, sistemas de almacenamiento y demás componentes críticos, hasta la configuración de los mismos. El análisis exhaustivo permitió comprender la topología de la red y sus interconexiones.

c) Verificación de la Topología y Estado de la Red en el Data Center

Se realizó una verificación minuciosa de la topología de red y el estado de los equipos del data center y gabinetes de comunicaciones de la empresa. Esta estrategia garantizó que la infraestructura estuviera en condiciones óptimas para recibir la implementación de Pandora FMS, evitando problemas futuros.

d) Planificación de Tiempos de Implementación

Se planificaron fechas y horarios específicos para la implementación de Pandora FMS en Microtel.Com EIRL. Estas fechas se establecieron de manera que tuvieran el menor impacto posible en las operaciones regulares de la empresa. Las coordinaciones se realizaron con el Gerente General.

e) Evaluación Post-Implementación y Mejora Continua

Después de la implementación inicial, se llevó a cabo una evaluación exhaustiva para identificar áreas de mejora y oportunidades de optimización a la hora de realizar las actualizaciones de la plataforma. Se estableció un ciclo de actualizaciones, basándonos en el modelo de liberaciones de versión de Pandora FMS.

3.7.3. Metodología.

Para la ejecución de este proyecto, se toma como guía y marco de referencia al Project Management Institute (PMI), una entidad líder en la gestión de proyectos a nivel global. La elección de basarse en las recomendaciones del PMI es fundamental para asegurar una gestión eficiente y efectiva de todo el ciclo del proyecto. A continuación, se describen las fases:

a) Fase de Inicio:

La fase de inicio del PMI es la etapa en la que se definen los objetivos del proyecto, se identifican los interesados clave, se establece una comunicación inicial para alinear expectativas y se establece el alcance. El resultado será el Acta de Inicio del Proyecto, formato que se muestra a continuación:

Figura 28

Acta de inicio del proyecto

DATOS GENERALES					
VERSION	**HECHA POR**	**REVISADA POR**	**APROBADA POR**	**FECHA**	**ID DEL PROYECTO**
1.0	Christian López	José Lazo	José Lazo	15-07-2018	023-2018

ACTA DE INICIO DEL PROYECTO

NOMBRE DEL PROYECTO	**GERENTE DEL PROYECTO**	
Implementación de Pandora FMS Open Source	José Lazo	
NOMBRE DEL CLIENTE	**COSTO ESTIMADO DEL PROYECTO**	
Microtel.Com EIRL	$ 2,000.00 + IGV	

DESCRIPCIÓN DEL PROYECTO

Necesidad y objetivos del negocio:
Implementación de plataforma de monitoreo Pandora FMS Open Source para monitorización de la infraestructura TI de la empresa.

Alcance del proyecto:
- Implementación de Pandora FMS Open Source.

Entregables del proyecto:
- Acta de inicio del proyecto.
- Cronograma Gantt del proyecto.
- Diagrama de arquitectura de red LAN Microtel.Com.
- Implementación de Pandora FMS Open Source.
- Credenciales de acceso a Pandora FMS Open Source.
- Informe técnico del proyecto.
- Acta de aceptación del proyecto.

Hitos del proyecto:
- Inicio.
- Planificación.
- Ejecución.
- Cierre del proyecto.

SUPUESTOS DEL PROYECTO
- El personal de Microtel.Com presentará una actitud colaboradora en todo el desarrollo del proyecto.
- Se dispone de las facilidades de comunicación de los equipos a monitorear.
- Se dispone de los recursos de hardware para la plataforma de monitoreo.

LO QUE NO INCLUYE ESTE PROYECTO.
- Configuración de los equipos de comunicaciones.
- Cambios en la arquitectura de red LAN.
- Integración con otras tecnologías.

RESTRICCIONES DEL PROYECTO
Ninguno.

APROBACIONES			
ROL	**NOMBRE**	**FECHA**	**FIRMA**
SPONSOR	**Microtel.Com EIRL**		
CLIENTE	**Microtel.Com EIRL**		
GERENTE DEL PROY.	**José Lazo Moreno**		
FINANZAS	**Isabel Gonzales**		

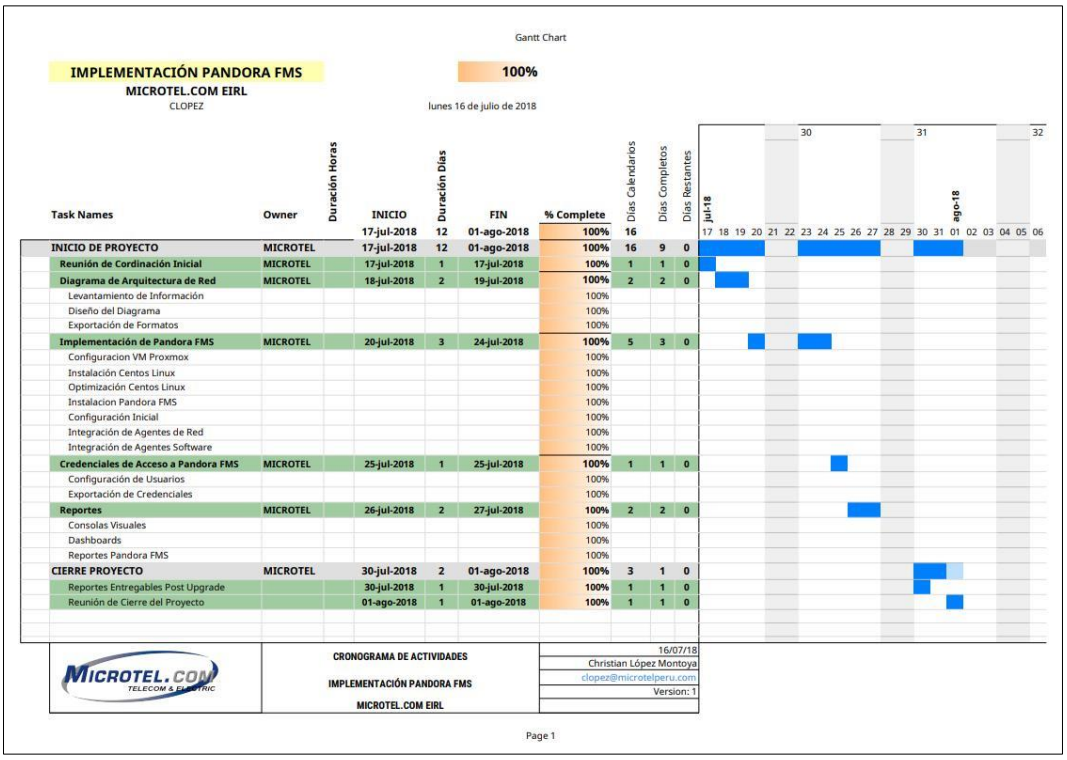
Fuente: Elaboración Propia.

b) Fase de Planificación:

En esta etapa, se desarrolla un plan detallado que incluye la definición de tareas, la programación de actividades. Para ello se elabora un diagrama Gantt con las siguientes etapas:

Figura 29

Diagrama gantt del proyecto



Fuente: Elaboración Propia.

c) Fase de Ejecución:

La fase de ejecución es donde se llevan a cabo las actividades planificadas. En este proyecto, se elabora el diagrama de arquitectura de red de la empresa, también, se instala y configura Pandora FMS en la infraestructura de Microtel.Com EIRL. Durante esta fase, se establecen procedimientos de monitoreo inicial y se comienzan a recopilar datos para su análisis posterior.

d) Fase de Seguimiento y Control:

La fase de seguimiento y control es crucial para mantener el proyecto en curso y en línea con los objetivos. En el contexto de la implementación de Pandora FMS, esta fase involucra el monitoreo continuo de la plataforma para detectar cualquier problema o necesidad de ajuste.

e) Fase de Cierre:

La fase de cierre marca la conclusión del proyecto y se centra en los entregables. En este proyecto, la fase de cierre implica asegurarse de que Pandora FMS esté funcionando de manera efectiva y que se cumplan los objetivos de supervisión de la infraestructura TI. Se realizan pruebas finales y se elabora un informe técnico final.

3.7.4. Diagrama de Arquitectura de Red Empresarial.

a) **Recopilación de Información:** En la siguiente tabla se recopilan los componentes de la arquitectura detallados sobre la infraestructura de red de Microtel.Com EIRL:

Tabla 6
Componentes de la arquitectura

Componente	Tipo de Dispositivo	Ubicación Física	Dirección IP
Router Castlenet Technology CBV384Z4	Router	Data Center	192.168.3.1
Firewall Untangle NG	Firewall	Data Center	192.168.3.2
Switch Core – CISCO SF300	Switch	Data Center	192.168.1.200
Switch – D-Link DGS-1100-24P	Switch	Data Center	192.168.1.201
Switch – D-Link DGS-1100-8P	Switch	Data Center	192.168.1.202
Central VOIP Zycoo	Servidor	Data Center	192.168.1.8
Servidor NVR HIKVISION	Servidor	Data Center	192.168.30.2
Servidor Hypervisor Promox VE	Servidor	Data Center	192.168.20.30

Servidor de Backups	Servidor	Data Center	192.168.20.41
Punto de Acceso TP-LINK TL-WR940N	Access Point	Gerencia	192.168.10.50
Punto de Acceso TP-LINK TL-WA901ND	Access Point	Sala Principal	192.168.10.20
Cámara Exterior HIKVISION	Servidor	Exterior	192.168.30.3
Cámara Interior 1 HIKVISION	Cámara	Sala Principal	192.168.30.8
Cámara Interior 2 HIKVISION	Cámara	Almacén	192.168.30.13

Fuente: Elaboración propia

b) **Identificación de Componentes:** En la siguiente tabla se recopilan los componentes de la arquitectura detallados sobre la infraestructura de red de Microtel.Com EIRL:

- **Router ISP Castlenet Technology CBV384Z4:** Este router es el punto de entrada de la conexión a Internet de la empresa. Gestiona el tráfico de datos entre el firewall y el proveedor de servicios de Internet (ISP) Movistar, permitiendo la comunicación hacia y desde Internet.

Figura 30

Router ISP Castlenet Technology CBV384Z4

Fuente: Elaboración Propia.

- **Firewall Untangle NG:** Es una solución de seguridad que protege la red de la empresa contra amenazas cibernéticas. Filtra y supervisa el tráfico de red, detecta y previene intrusiones, y controla el acceso a sitios web no deseados. También gestiona las conexiones VPN para permitir el acceso remoto a los recursos de la empresa.

Figura 31

Firewall Untangle NG

Fuente: Elaboración Propia.

- **Switch Core – CISCO SF300:** Es el componente central en la infraestructura de red. Actúa como un concentrador principal de la conexión de red entre los switches de dispositivos y comunicaciones, permitiendo que múltiples dispositivos se comuniquen entre sí dentro de la red local.

Figura 32
Switch core CISCO SF300

Fuente: Elaboración Propia.

- **Switch – D-Link DGS-1100-24P:** Este switch proporciona conectividad a los usuarios, puntos de acceso y los telefónos IP, dentro de la red, y además, es capaz de suministrar energía a través de Ethernet (PoE) a dispositivos como cámaras IP y teléfonos VOIP.

Figura 33
Switch D-Link DGS-1100-24P

Fuente: Elaboración Propia.

- **Switch – D-Link DGS-1100-8P:** Se encarga de proporcionar la conectividad de las cámaras de seguridad IP, permitiendo adicionalmente suministrar energía a través de PoE.

Figura 34
Switch D-Link DGS-1100-8P

Fuente: Elaboración Propia.

- **Central Telefonía VOIP Zycoo:** La central telefónica permite realizar llamadas telefónicas a través de la red de datos utilizando el protocolo VOIP (Voice over IP). Esto permite ahorrar costos en llamadas y brinda flexibilidad en la gestión de comunicaciones.

Figura 35
Central telefonía VOIP Zycoo

Fuente: Elaboración Propia.

- **Servidor NVR HIKVISION:** Es el responsable de grabar y almacenar las imágenes de las cámaras de seguridad. Proporciona una plataforma centralizada para el monitoreo y la gestión de videos de seguridad.

Figura 36
Servidor NVR HIKVISION

Fuente: Elaboración Propia.

- **Servidor Hypervisor Proxmox VE:** Este servidor actúa como una plataforma de virtualización que permite la creación y gestión de múltiples máquinas virtuales (VM). Es esencial para consolidar recursos y ejecutar aplicaciones y servicios de manera eficiente. Actualmente cuenta con los siguientes servidores: Servidor de Backups OpenMediaVault, Servidor de Monitoreo Pandora FMS.

Figura 37
Servidor hypervisor Proxmox VE

Fuente: Elaboración Propia.

- **Servidor de Backups OpenMediaVault:** El servidor de backups OpenMediaVault se encarga de realizar copias de seguridad de datos críticos de la empresa. Almacena y protege los archivos para la recuperación en caso de pérdida de datos. Esta virtualizado en el servidor hypervisor Proxmox VE y utiliza discos físicos para almacenar los datos.

- **Punto de Acceso TP-LINK TL-WR940N:** Este punto de acceso proporciona conectividad inalámbrica en la zona de gerencia, permitiendo que dispositivos móviles y laptops se conecten a la red de la empresa de manera inalámbrica.

Figura 38
Punto de acceso TP-LINK TL-WR940N

Fuente: Elaboración Propia.

- **Punto de Acceso TP-LINK TL-WA901ND:** Este dispositivo proporciona conectividad inalámbrica, pero está destinado a la zona de usuarios en general.

Figura 39
Punto de acceso TP-LINK TL-WA901ND

Fuente: Elaboración Propia.

- **Cámara Exterior HIKVISION:** Las cámaras exteriores HIKVISION se utilizan para la vigilancia y la seguridad en áreas exteriores.

Figura 40

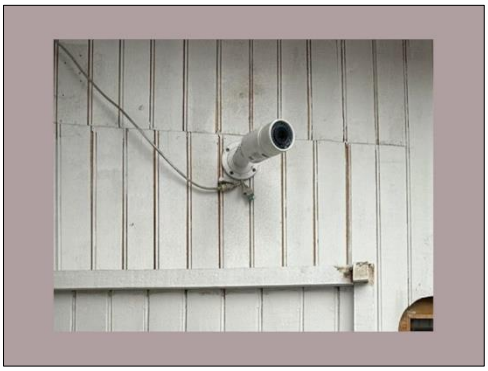
Cámara exterior HIKVISION

Fuente: Elaboración Propia.

- **Cámara Interior 1 HIKVISION:** Se ubica en el área interna, como la sala principal, para monitorear actividades y asegurar la seguridad en el interior de la empresa.

Figura 41

Cámara interior 1 HIKVISION



Fuente: Elaboración Propia.

- **Cámara Interior 2 HIKVISION:** Esta cámara supervisa el almacén de la empresa, garantizando la seguridad de las instalaciones y el inventario.

Figura 42

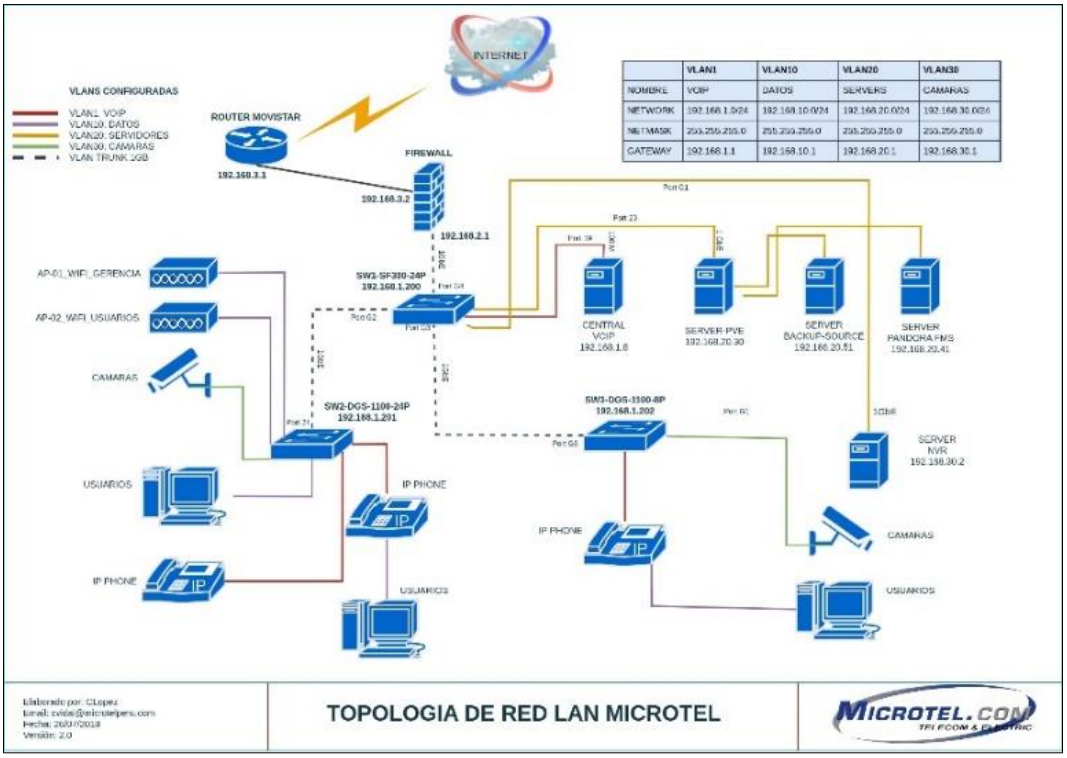
Cámara interior 2 HIKVISION

Fuente: Elaboración Propia.

c) **Diseño del Diagrama:** Utilizando la herramienta de diseño Drawio en la plataforma de colaboración de Microtel.Com EIRL, se crea un diagrama que represente la topología de la red y se establecen las conexiones entre los elementos. A continuación, se muestra dicho diagrama:

Figura 43

Diagrama de topología de la red empresarial



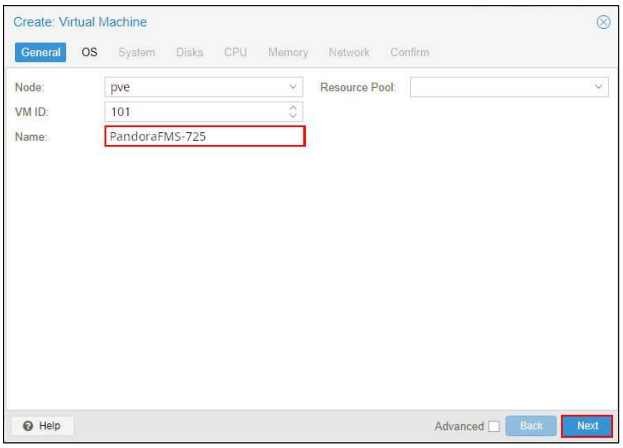
Fuente: Elaboración Propia.

d) **Actualización Continua:** El diagrama se mantiene actualizado a medida que se realizan cambios en la infraestructura de red, lo que garantiza que la representación sea precisa en todo momento.

3.7.5. Instalación de Pandora FMS

a) **Despliegue de VM en Proxmox VE:** Se crea una máquina virtual que contendrá a la plataforma de monitorización Pandora FMS. Se asignan recursos específicos, como almacenamiento, memoria y CPU, para garantizar un rendimiento óptimo. Proxmox VE, como hipervisor, permite gestionar eficazmente estas asignaciones y alojar la VM de Pandora FMS.

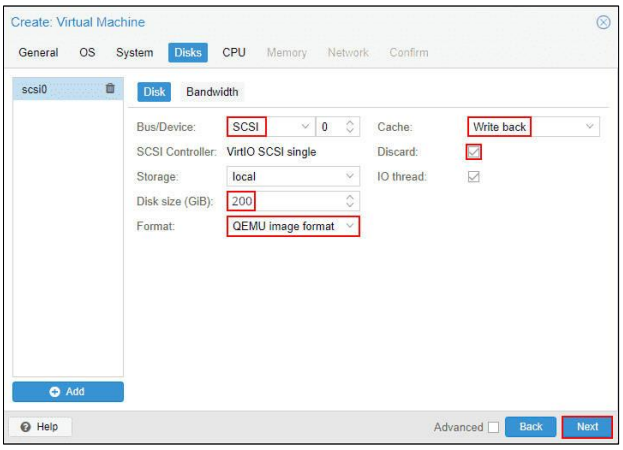
Figura 44
Asistente de creación VM–general



Fuente: Elaboración Propia.

Figura 45

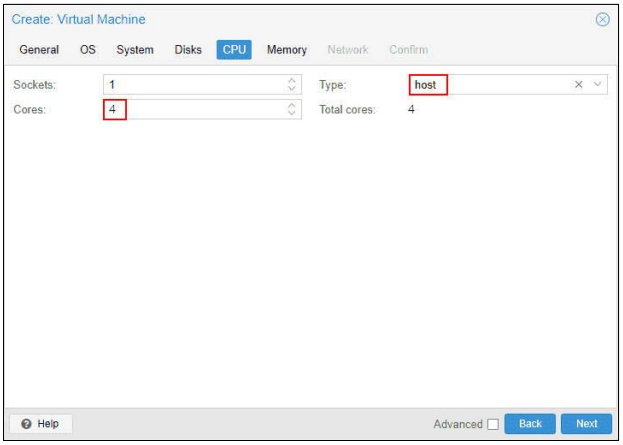
Asistente de creación VM–disco



Fuente: Elaboración Propia.

Figura 46

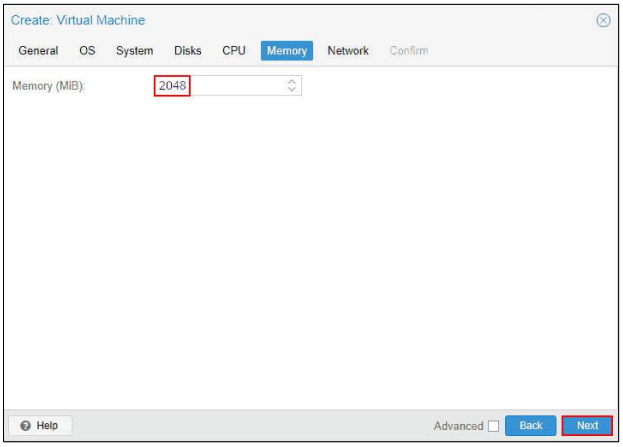
Asistente de creación VM–CPU



Fuente: Elaboración Propia.

Figura 47

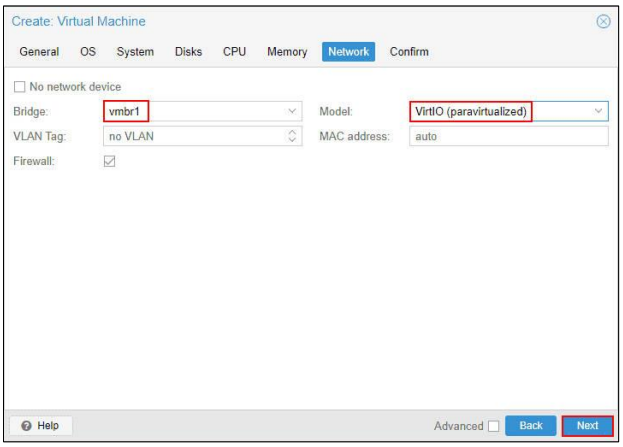
Asistente de creación VM–RAM



Fuente: Elaboración Propia.

Figura 48

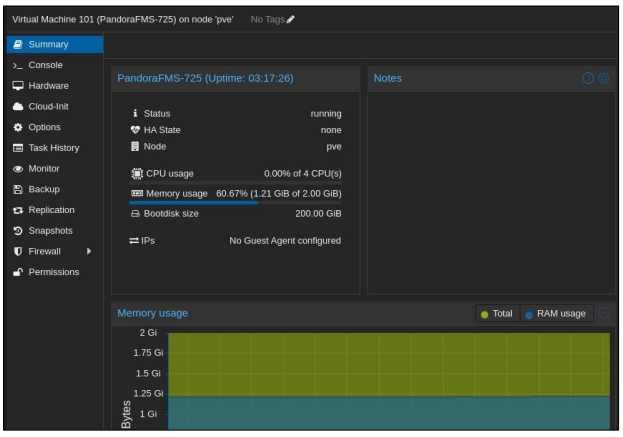
Asistente de creación VM–network



Fuente: Elaboración Propia.

Figura 49

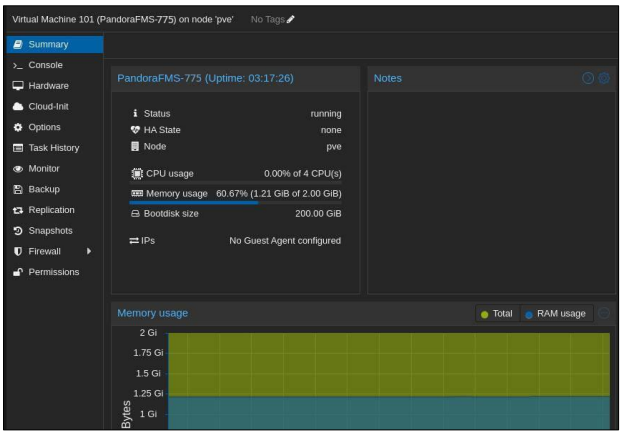
Resumen VM Pandora FMS 725 NG



Fuente: Elaboración Propia.

Figura 50

Resumen VM Pandora FMS 772 LTS

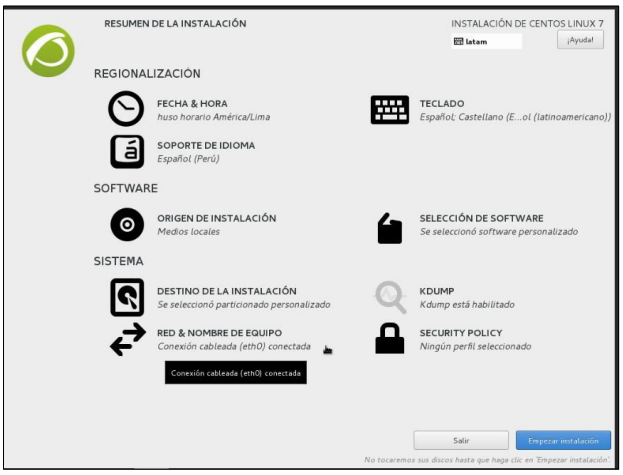


Fuente: Elaboración Propia.

b) **Instalación del Sistema Operativo:** Inicialmente, en 2018, se utilizaba el sistema operativo CentOS 7 para alojar Pandora FMS. Sin embargo, en la actualidad, se ha migrado a Rocky Linux 8, una distribución de Linux compatible con CentOS. Esta transición se realizó para adaptarse a los cambios en el ecosistema de sistemas operativos y garantizar la continuidad y seguridad del entorno.

Figura 51

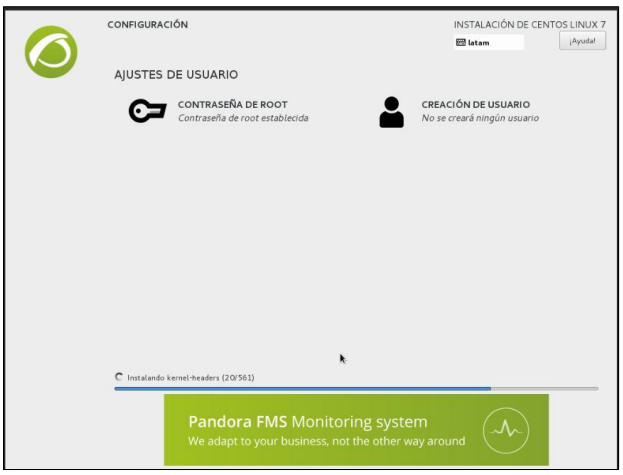
Wizard de instalación ISO Appliance CentOS 7



Fuente: Elaboración Propia.

Figura 52

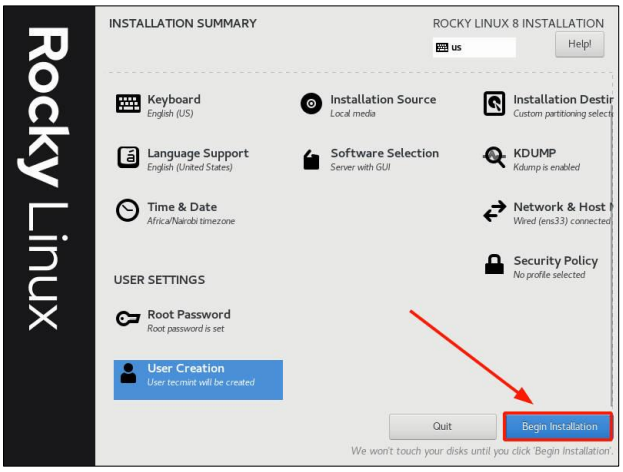
Instalando ISO Appliance CentOS 7



Fuente: Elaboración Propia.

Figura 53

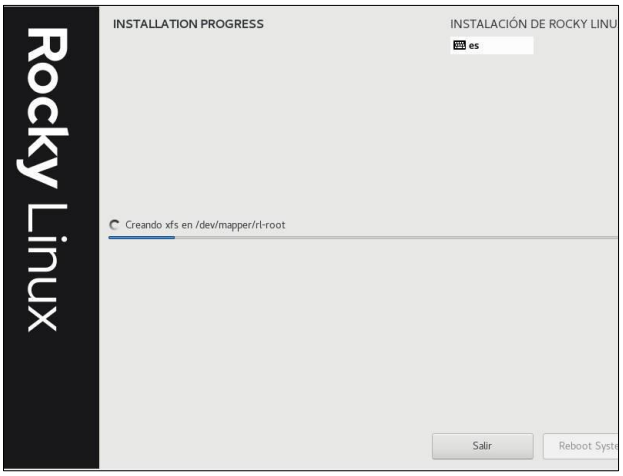
Wizard de instalación Rocky Linux 8



Fuente: Elaboración Propia.

Figura 54

Instalando Rocky Linux 8



Fuente: Elaboración Propia.

c) **Despliegue de Pandora FMS:** En 2018, la versión 725 NG de Pandora FMS fue instalada en Microtel.Com EIRL. A día de hoy, la plataforma se ha actualizado a la versión 772 LTS, que proporciona características mejoradas y soporte a largo plazo. Además, la instalación de Pandora FMS se ha simplificado significativamente mediante la ejecución de un script de instalación automática, lo que agiliza la implementación y mantenimiento de la plataforma. Esta configuración actualizada y simplificada de Pandora FMS en Rocky Linux 8 dentro de una VM gestionada por Proxmox VE

garantiza que Microtel.Com EIRL cuente con una plataforma de monitorización robusta y eficiente para supervisar su infraestructura tecnológica.

Figura 55

Pantalla de sesión en terminal Pandora FMS 725 NG

Fuente: Elaboración Propia.

Figura 56

Script de instalación Pandora FMS 772 LTS

Fuente: Elaboración Propia.

3.7.6. Configuración de Pandora FMS

a) **Configuraciones Generales:** Se configuran las opciones generales de Pandora FMS. Esto incluye la configuración de alertas por correo electrónico para notificar sobre

eventos y problemas de monitoreo. También se realizan configuraciones básicas para asegurar que Pandora FMS esté operativo y listo para la supervisión.

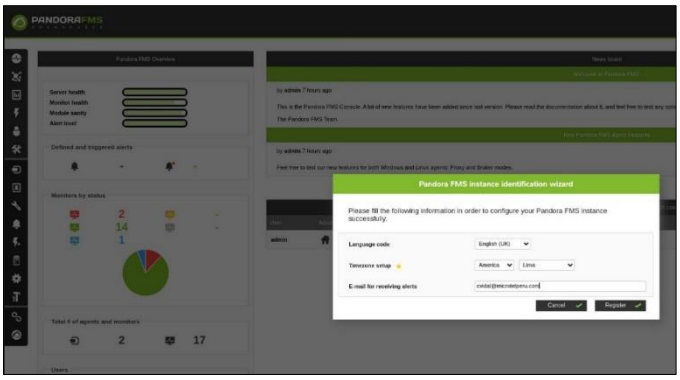
Figura 57

Pantalla de inicio consola web Pandora FMS

Fuente: Elaboración Propia.

Figura 58

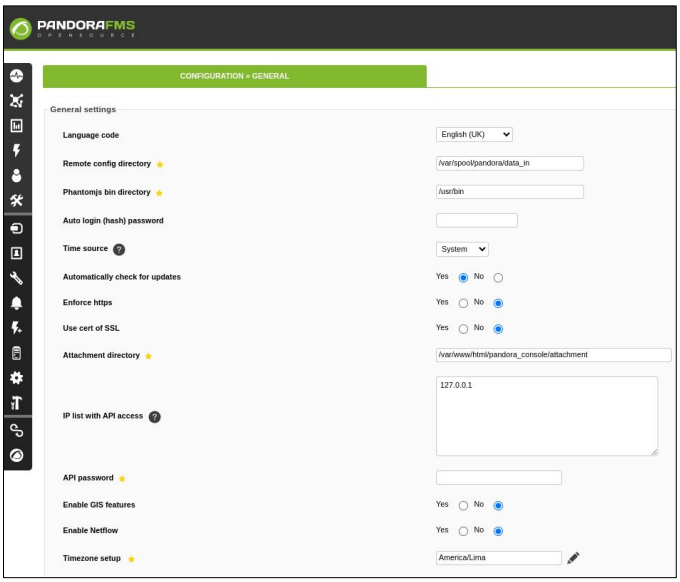
Wizard de inicio consola web Pandora FMS



Fuente: Elaboración Propia.

Figura 59

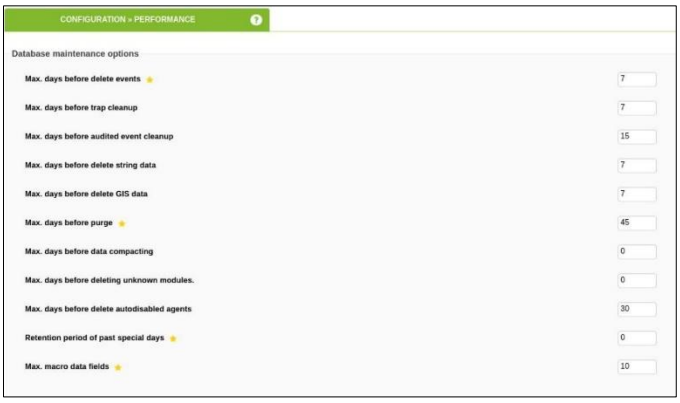
Configuraciones generales Pandora FMS



Fuente: Elaboración Propia.

Figura 60

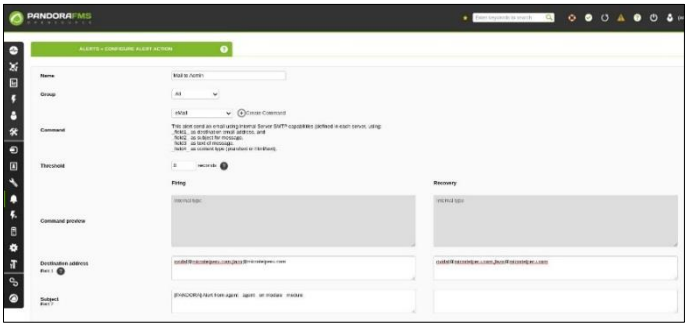
Configuración de base de datos Pandora FMS



Fuente: Elaboración Propia.

Figura 61

Configuración de alerta por email

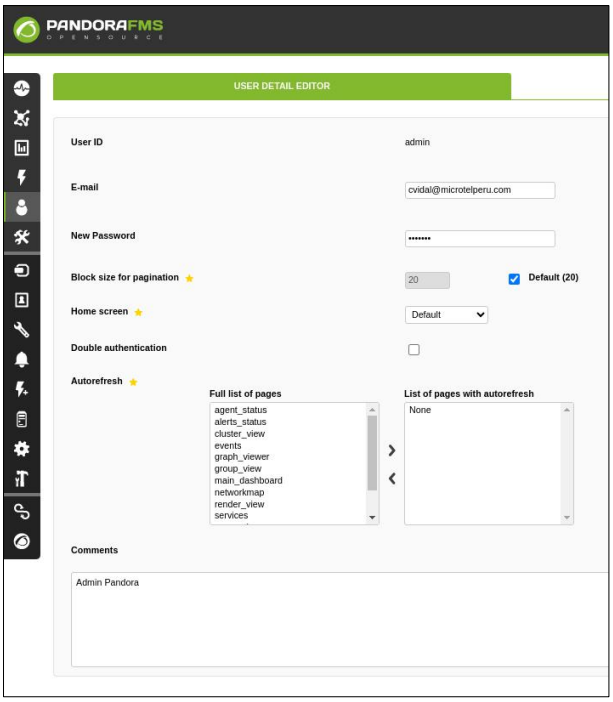


Fuente: Elaboración Propia.

b) **Usuarios:** Se crean los siguientes usuarios en Pandora FMS. Usuario "cvidal", que tiene permisos de administrador, encargado de gestionar la plataforma. Usuario "operador", que tiene permisos de escritura y lectura sobre la monitorización en la plataforma, este usuario no podrá realizar ajustes en la configuración avanzada de Pandora FMS. El otro es el usuario "monitor", que sólo tiene acceso a los dashboards y se usará en las pantallas de monitoreo.

Figura 62

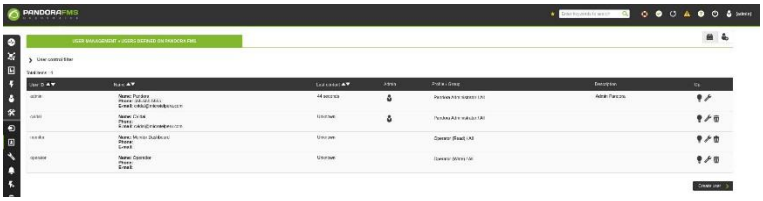
Vista de creación de usuarios



Fuente: Elaboración Propia.

Figura 63

Listado de usuarios en consola

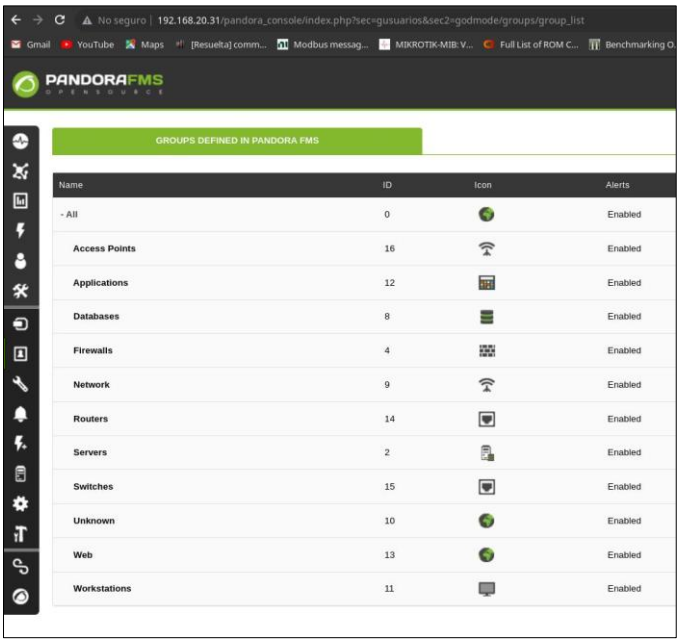


Fuente: Elaboración Propia.

c) **Agentes de Red:** Se agregan todos los agentes de red que se desean supervisar. Se generan los grupos de monitoreo en la plataforma.

Figura 64

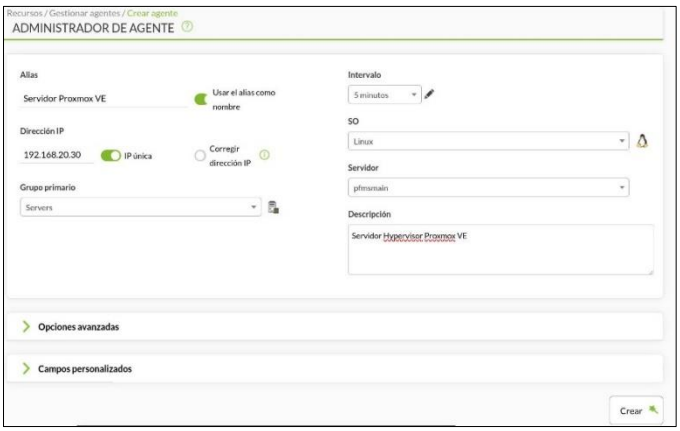
Definición de grupos de agentes



Fuente: Elaboración Propia.

Figura 65

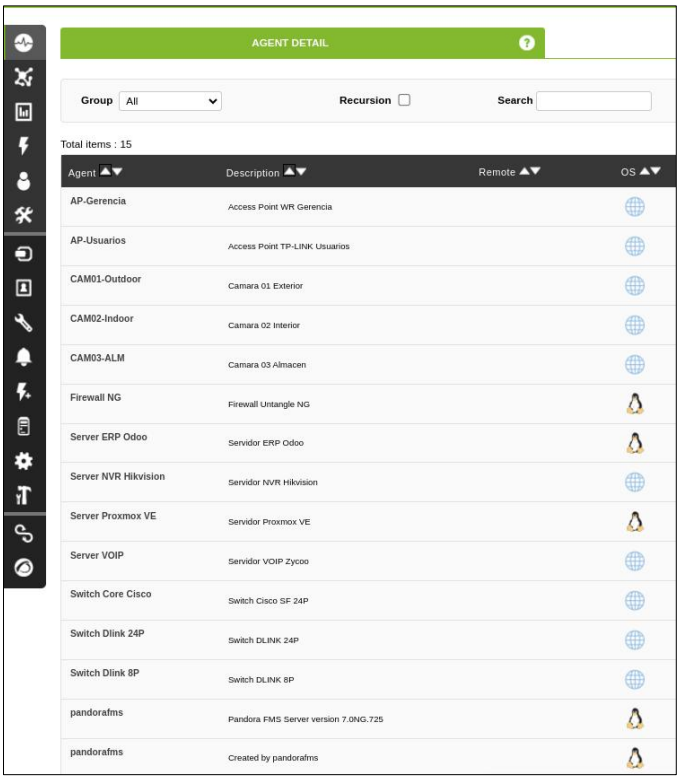
Vista de creación de agentes



Fuente: Elaboración Propia.

Figura 66

Listado de agentes en consola

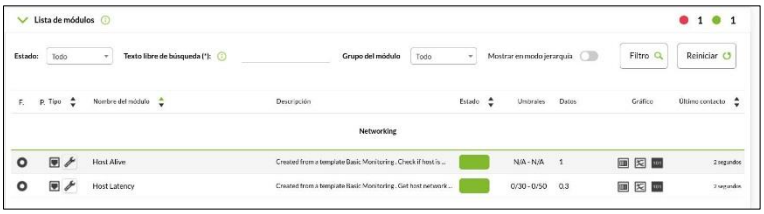


Fuente: Elaboración Propia.

d) **Métricas de Agentes de Red:** Se configuran métricas específicas para dispositivos de red, ICMP y la latencia. Estas métricas ayudan a evaluar la disponibilidad y el rendimiento de la red. También se define los umbrales y el alertado en caso de algún evento crítico.

Figura 67

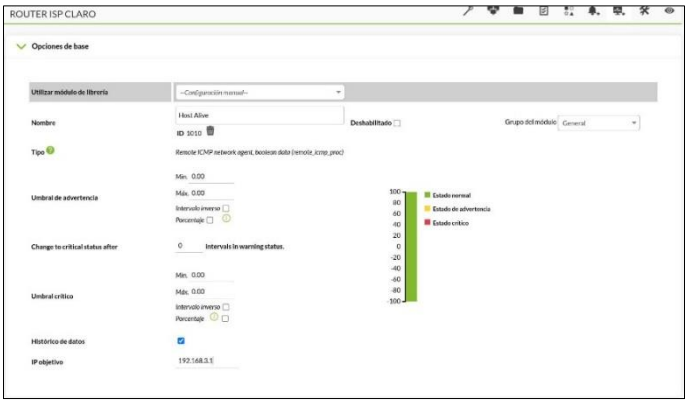
Métricas de los agentes de red



Fuente: Elaboración Propia.

Figura 68

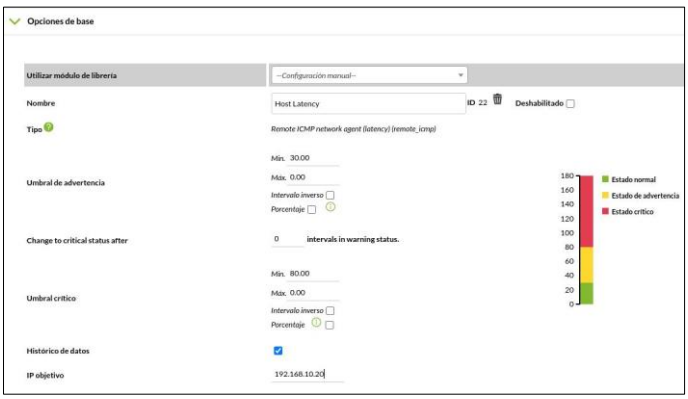
Configuración de métrica Host Alive



Fuente: Elaboración Propia.

Figura 69

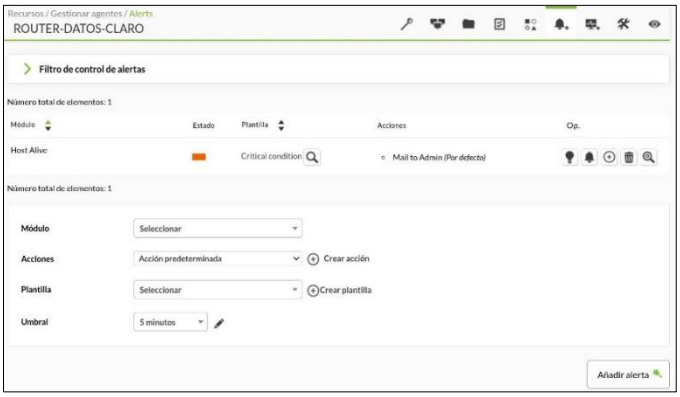
Configuración de métrica Host Latency



Fuente: Elaboración Propia.

Figura 70

Definición de alerta ICMP



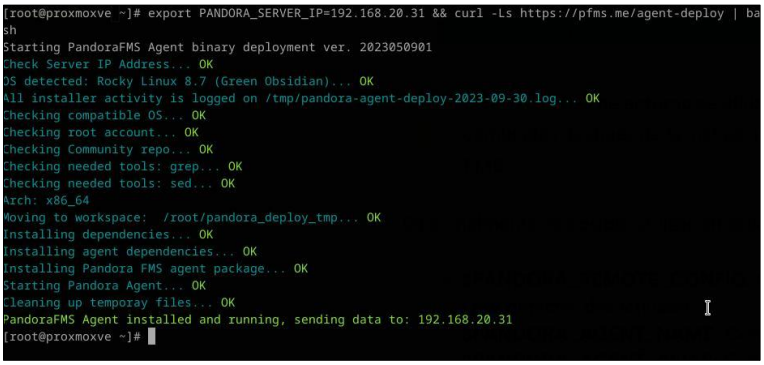
Fuente: Elaboración Propia.

e) **Agentes Software:** Se añaden todos los agentes de tipo servidores, instalando el agente software en los servidores soportados. Estos agentes software recopilan información

detallada sobre el rendimiento y el estado de los servidores, lo que permite un monitoreo completo.

Figura 71

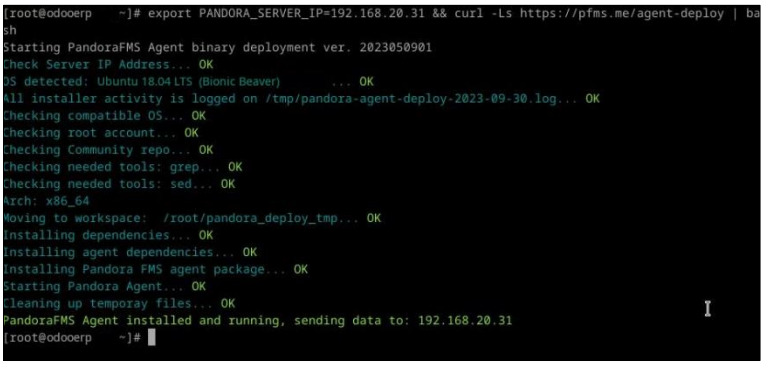
Instalación script en Proxmox VE



Fuente: Elaboración Propia.

Figura 72

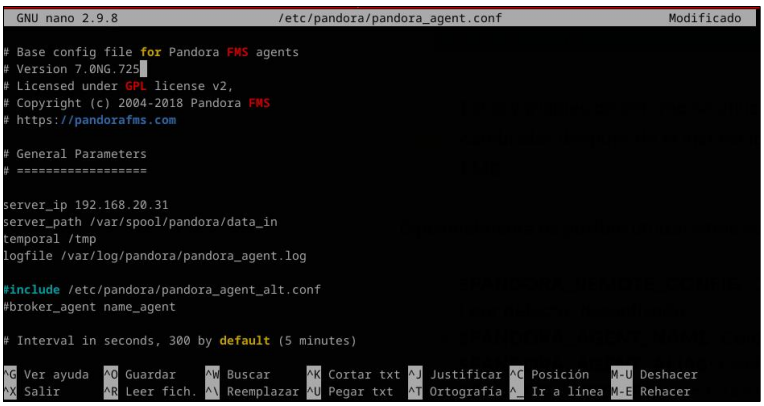
Instalación script en ERP Odoo



Fuente: Elaboración Propia.

Figura 73

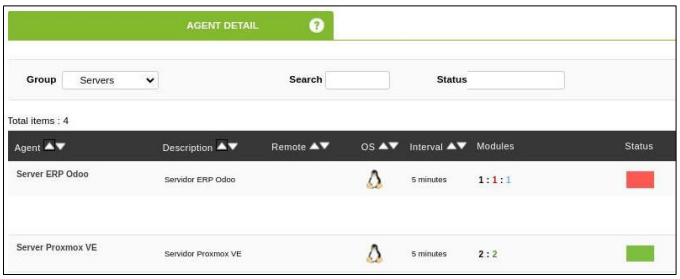
Archivo de configuración agente software



Fuente: Elaboración Propia.

Figura 74

Agentes software en consola Pandora FMS



Fuente: Elaboración Propia.

f) **Métricas de Agentes Software:** Para los servidores, se agregan las métricas: espacio utilizado en disco, el consumo de memoria y el uso del CPU. Tambien se configuran los umbrales y alertado.

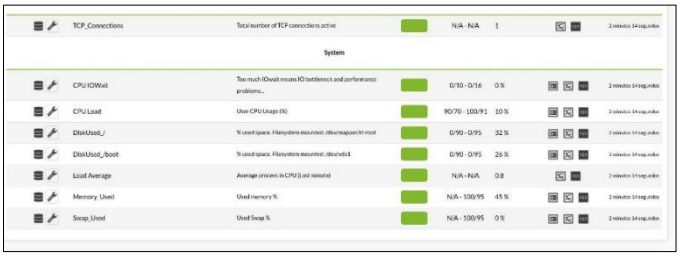
Figura 75

Métricas del agente software Proxmox VE

Fuente: Elaboración Propia.

Figura 76

Métricas del agente software ERP Odoo



Fuente: Elaboración Propia.

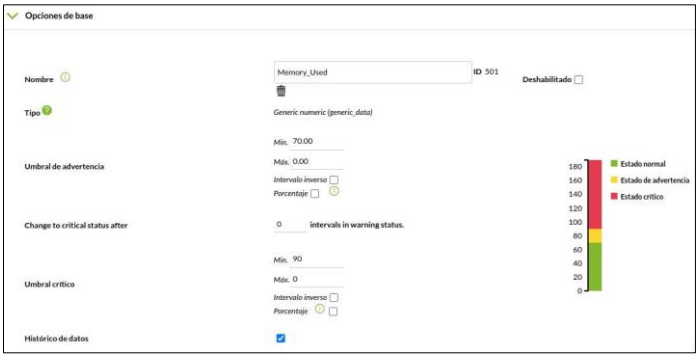
Figura 77

Configuración métrica Cpu Load agente software

Fuente: Elaboración Propia.

Figura 78

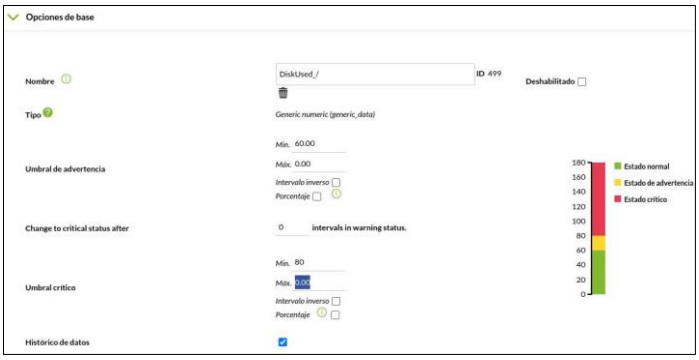
Configuración métrica Memory Used agente software



Fuente: Elaboración Propia.

Figura 79

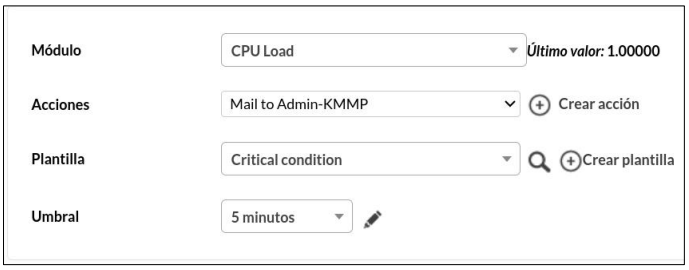
Configuración métrica Disk Used agente software



Fuente: Elaboración Propia.

Figura 80

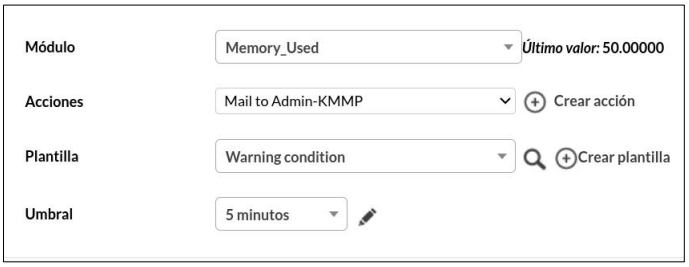
Definición de alerta Critical Cpu Load



Fuente: Elaboración Propia.

Figura 81

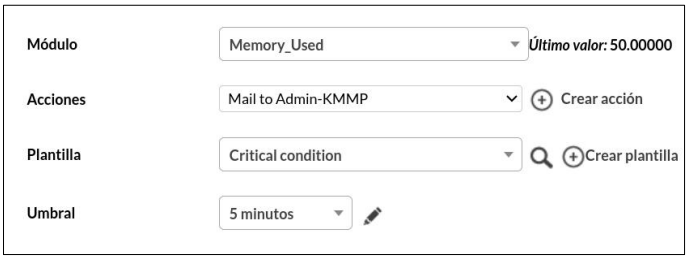
Definición de alerta Warning Memory Used



Fuente: Elaboración Propia.

Figura 82

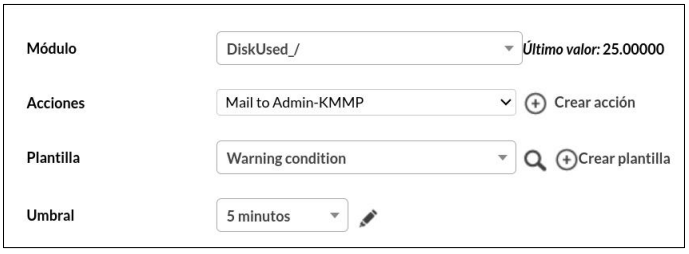
Definición de alerta Critical Memory Used



Fuente: Elaboración Propia.

Figura 83

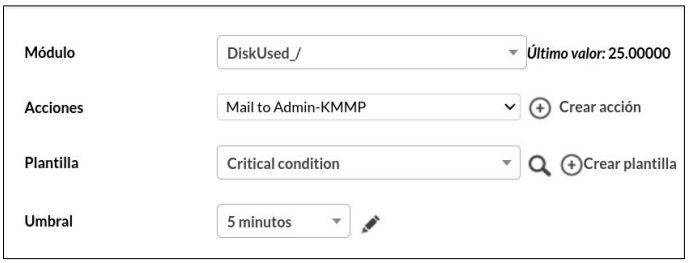
Definición de alerta Warning Disk Used



Fuente: Elaboración Propia.

Figura 84

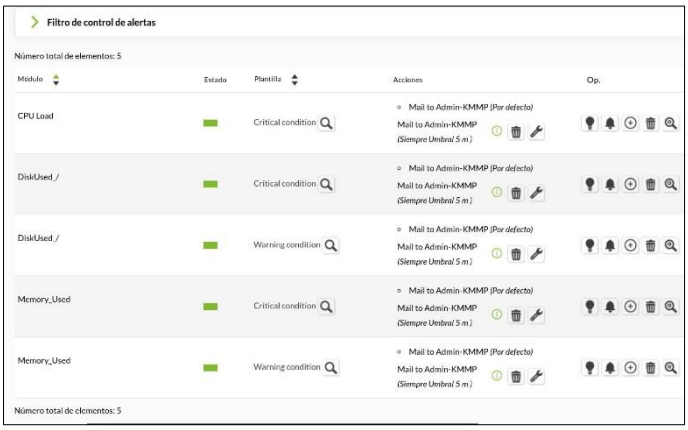
Definición de alerta Critical Disk Used



Fuente: Elaboración Propia.

Figura 85

Listado de alertas para agentes software

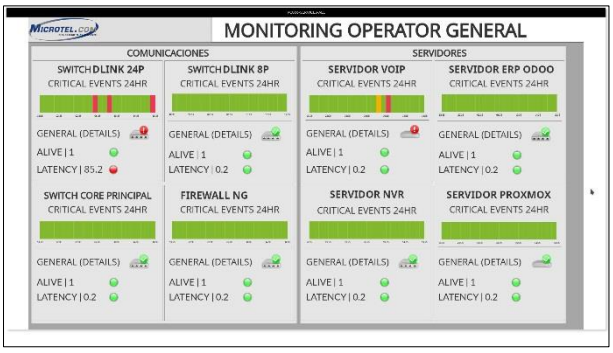


Fuente: Elaboración Propia.

g) **Consolas Visuales:** Se crean consolas visuales personalizados para proporcionar una representación visual de los equipos de red, la topología de red, los servidores y el estado general del sistema. Estas consolas facilitan la supervisión y el análisis de datos en tiempo real. En la primera etapa del primer año de Pandora FMS, se desarrolló un único dashboard que reunía de manera general los principales eventos de los equipos de red y servidores. Actualmente mientras se desarrolla este trabajo de suficiencia, se han venido elaborando diversas consolas visuales que integran la topología de red LAN, vista detallada de servidores, y una consola visual que muestra el ecosistema general de la infraestructura TI de la empresa.

Figura 86

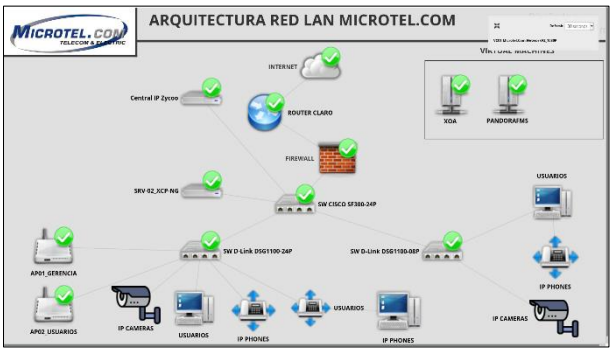
Consola visual monitoreo general



Fuente: Elaboración Propia.

Figura 87

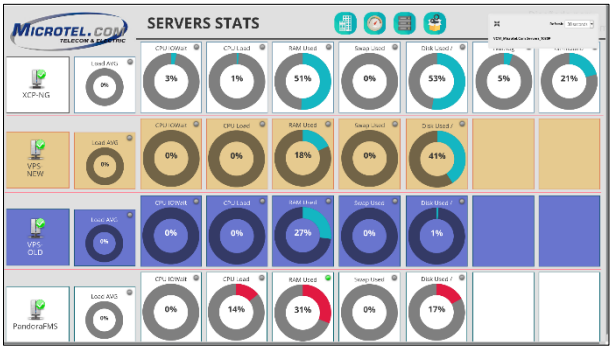
Consola visual topología de red



Fuente: Elaboración Propia.

Figura 88

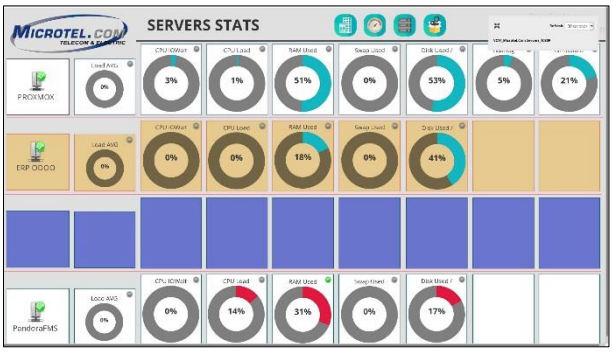
Consola visual servidores 1



Fuente: Elaboración Propia.

Figura 89

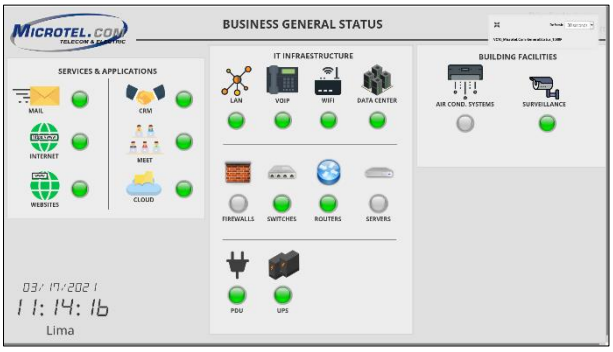
Consola visual servidores 2



Fuente: Elaboración Propia.

Figura 90

Consola visual ecosistema infraestructura TI



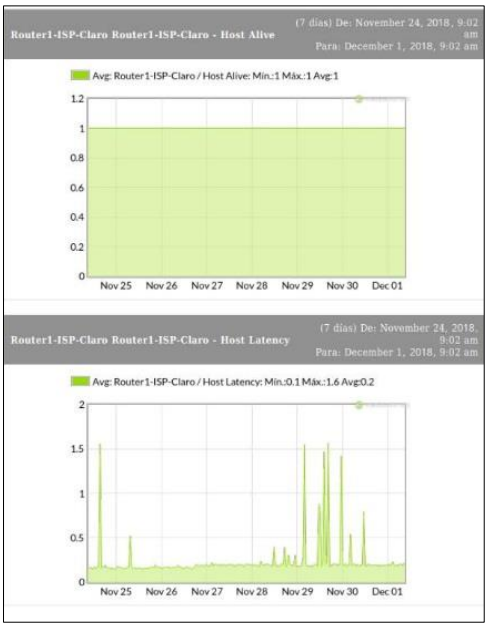
Fuente: Elaboración Propia.

h) **Reportes:** Se generan reportes específicos que muestran la información recopilada sobre ICMP y latencia en dispositivos de red, y en servidores. Adicionalmente se ha integrado las métricas de los agentes software como son el uso del CPU, uso de memoria y uso de disco. Estos reportes son útiles para evaluar el rendimiento a lo largo del tiempo y tomar decisiones informadas.

- **Reporte Semanal Dispositivos de Red:** Se muestran gráficos de tipo área, representando métricas de Host Alive y Latency. La data mostrada corresponde a un rango de 7 días. A continuación, se muestran los gráficos:

Figura 91

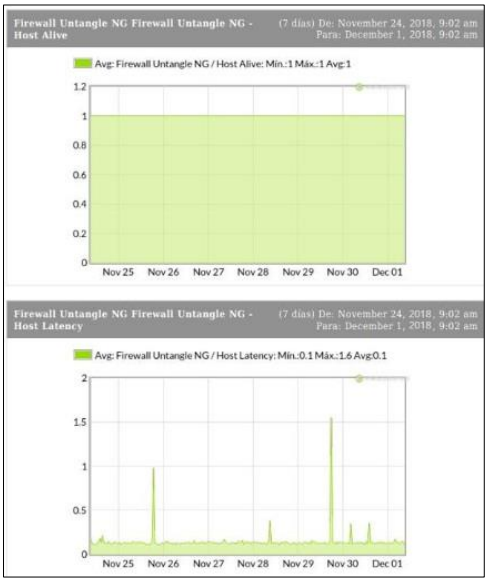
Host Alive y latencia router ISP Claro



Fuente: Elaboración Propia.

Figura 92

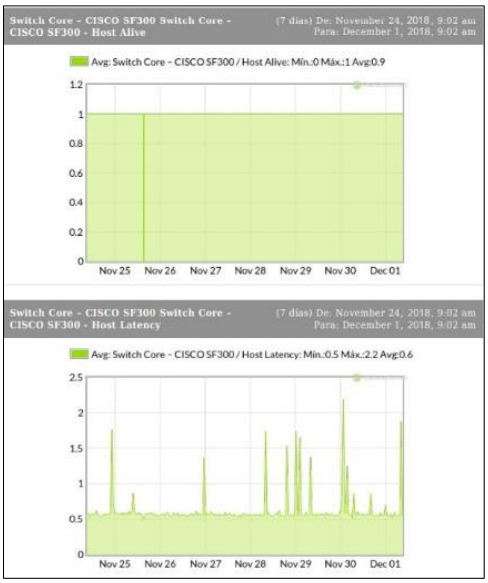
Host Alive y latencia firewall Untangle NG



Fuente: Elaboración Propia.

Figura 93

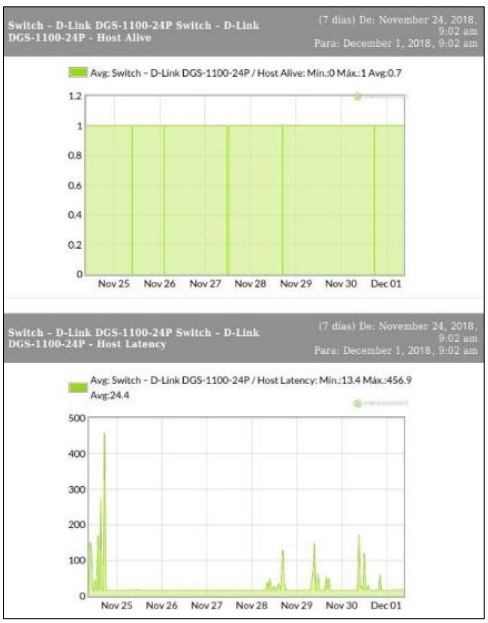
Host Alive y latencia switch core Cisco SF300



Fuente: Elaboración Propia.

Figura 94

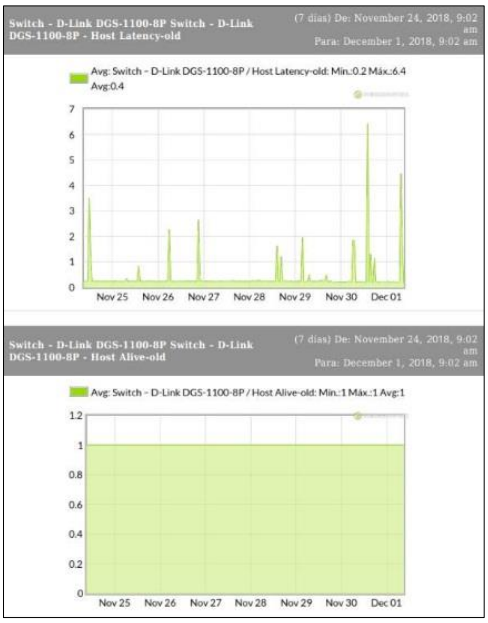
Host Alive y latencia switch D-Link 1100-24P



Fuente: Elaboración Propia.

Figura 95

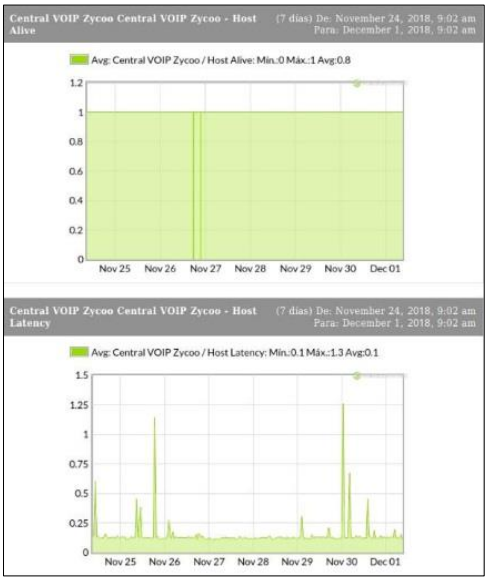
Host Alive y latencia switch D-Link 1100-8P



Fuente: Elaboración Propia.

Figura 96

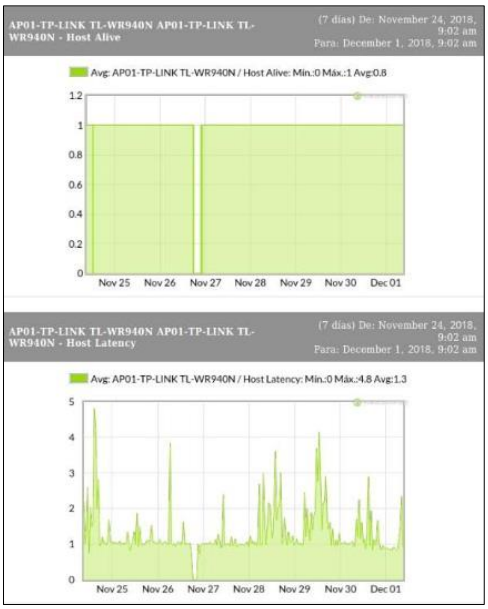
Host Alive y latencia central VOIP Zycoo



Fuente: Elaboración Propia.

Figura 97

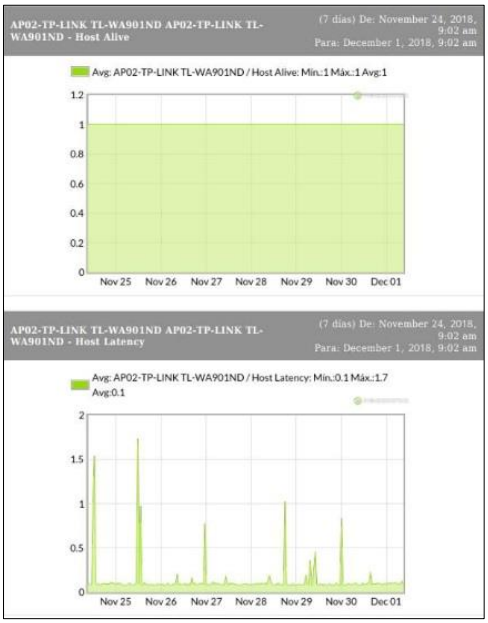
Host Alive y latencia AP01-TP-Link TL-WR940N



Fuente: Elaboración Propia.

Figura 98

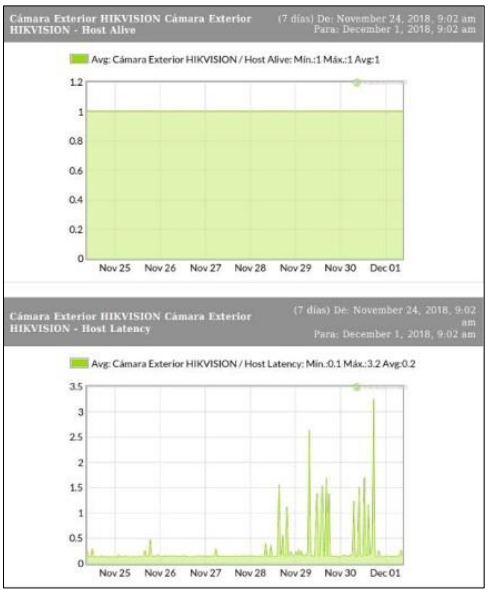
Host Alive y latencia AP02-TP-Link TL-WA901ND



Fuente: Elaboración Propia.

Figura 99

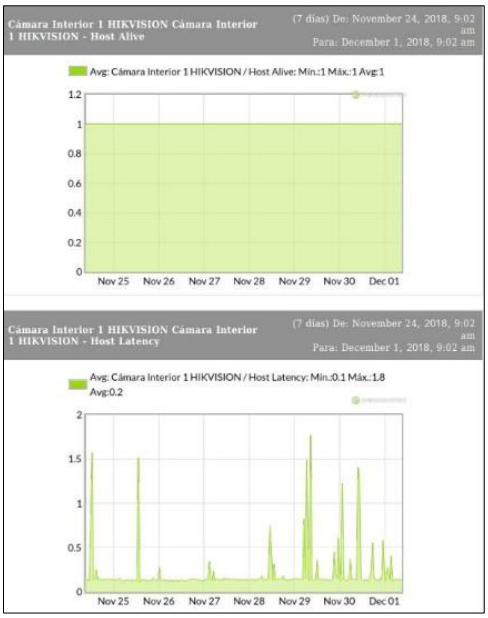
Host Alive y latencia cámara exterior HIKVISION



Fuente: Elaboración Propia.

Figura 100

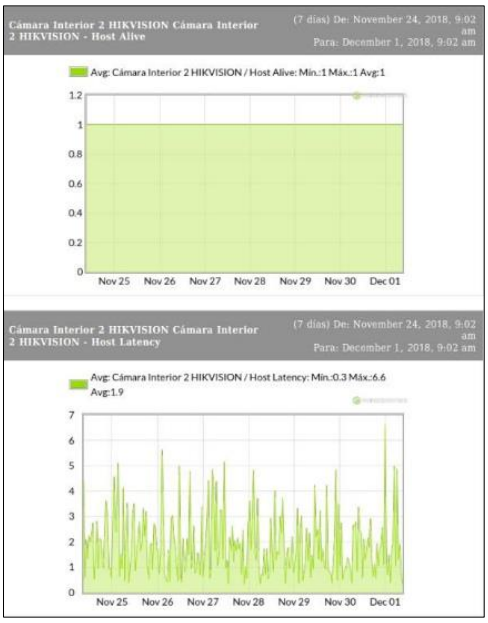
Host Alive y latencia cámara interior 1 HIKVISION



Fuente: Elaboración Propia.

Figura 101

Host Alive y latencia cámara interior 2 HIKVISION

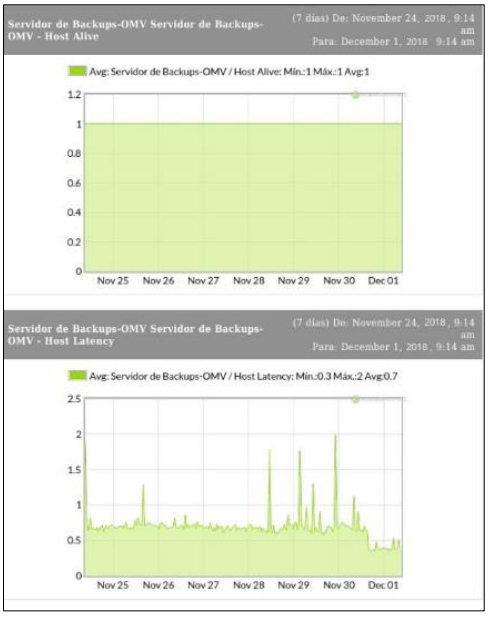


Fuente: Elaboración Propia.

- **Reporte Semanal Servidores:** La información proporcionada corresponde a un rango de 7 días y se muestran las métricas Host Alive, Latency, Cpu Load, Memory Used, Disk Used. A continuación, se muestran los gráficos.

Figura 102

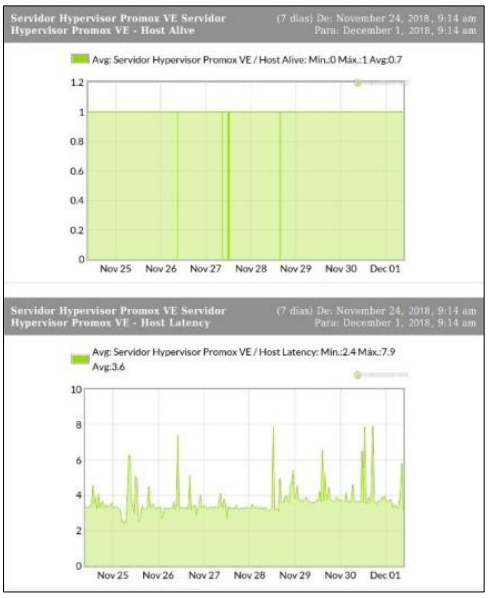
Host Alive y latencia servidor de backups OMV



Fuente: Elaboración Propia.

Figura 103

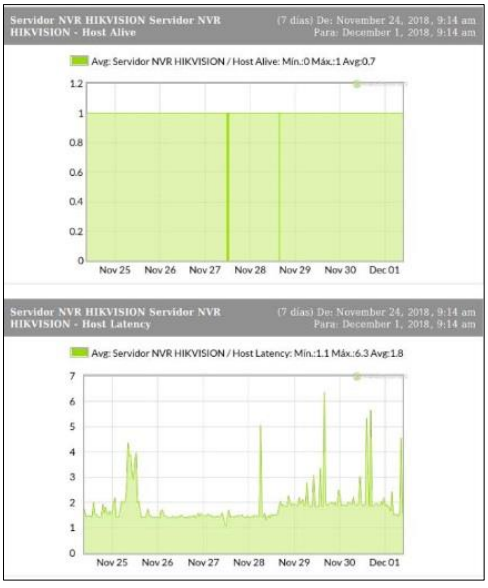
Host Alive y latencia servidor hypervisor Proxmox VE



Fuente: Elaboración Propia.

Figura 104

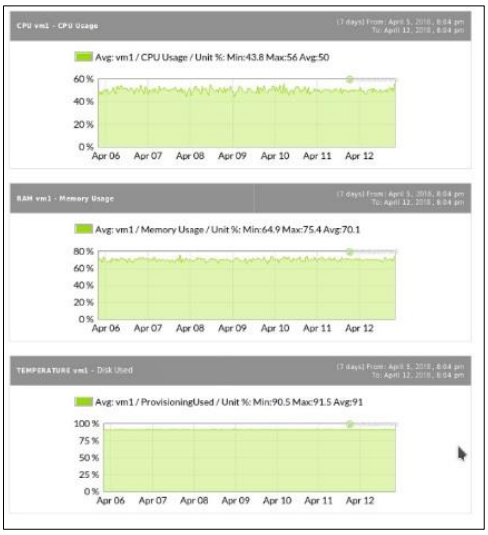
Host Alive y latencia servidor NVR HIKVISION



Fuente: Elaboración Propia.

Figura 105

Promox VE CPU, Memory, Disk



Fuente: Elaboración Propia.

CAPÍTULO IV. RESULTADOS

En este capítulo, se expondrán los resultados obtenidos tras la implementación de Pandora FMS como plataforma de monitoreo de la Infraestructura TI en la empresa Microtel.com EIRL.

Se llevó a cabo procesos de análisis de datos, usando los recursos proporcionados por Microtel.Com EIRL, para la elaboración de este trabajo de suficiencia profesional. Se muestra un panorama de antes y después, usando tablas y gráficas. Cada uno de los objetivos específicos se abordará por separado para ofrecer una comprensión completa:

a) Incrementar la cobertura de supervisión de la infraestructura de TI de la empresa:

Se realizó una comparación antes y después de la implementación de Pandora FMS, registrando los recursos supervisados y su alcance.

Antes de la implementación de Pandora FMS, la empresa supervisaba el 10% de su infraestructura de TI, que sólo corresponden al router del operador y firewall. Esta supervisión es gestionada por el operador. Los otros recursos TI de la empresa, no eran supervisados ni gestionados por terceros.

Tabla 7
Supervisión de recursos TI antes de Pandora FMS

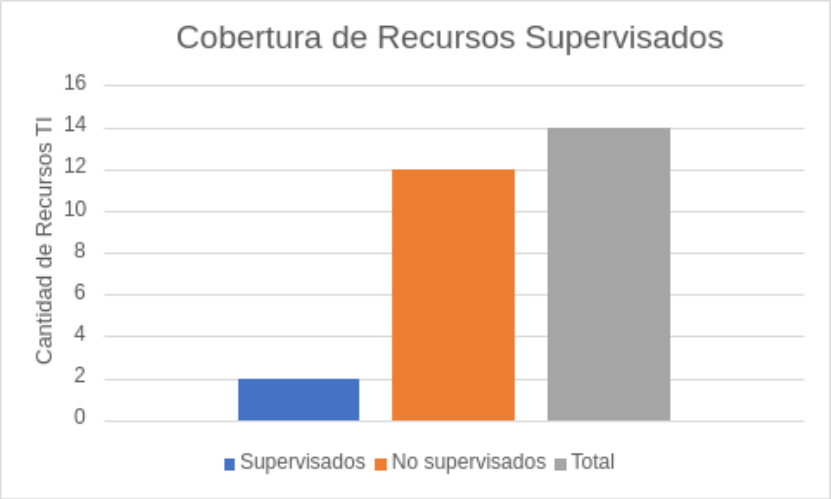
	Elaborado por: José Lazo		Supervisados	2
	Versión: 1 - 07/2018		No supervisados	12
Supervisión de Equipos TI				
Descripción	Tipo de Dispositivo	Dirección IP	Supervisor	Estado
Router Castlenet Technology CBV384Z4	Router	192.168.3.1	Operador Movistar Empresas	Supervisado
Firewall NG	Firewall	192.168.3.2	Operador Movistar Empresas	Supervisado
Switch Core – CISCO SF300	Switch	192.168.1.200	Microtel.Com EIRL	No Supervisado
Switch – D-Link DGS-1100-24P	Switch	192.168.1.201	Microtel.Com EIRL	No Supervisado
Switch – D-Link DGS-1100-8P	Switch	192.168.1.202	Microtel.Com EIRL	No Supervisado
Central VOIP Zycoo	Servidor	192.168.1.8	Microtel.Com EIRL	No Supervisado
Servidor NVR HIKVISION	Servidor	192.168.30.2	Microtel.Com EIRL	No Supervisado
Servidor Hypervisor Promox VE	Servidor	192.168.20.30	Microtel.Com EIRL	No Supervisado
Servidor de Backups	Servidor	192.168.20.41	Microtel.Com EIRL	No Supervisado
AP TP-LINK TL-WR940N	Access Point	192.168.10.50	Microtel.Com EIRL	No Supervisado
AP TP-LINK TL-WA901ND	Access Point	192.168.10.20	Microtel.Com EIRL	No Supervisado
Cámara Exterior HIKVISION	Servidor	192.168.30.3	Microtel.Com EIRL	No Supervisado
Cámara Interior 1 HIKVISION	Cámara	192.168.30.8	Microtel.Com EIRL	No Supervisado
Cámara Interior 2 HIKVISION	Cámara	192.168.30.13	Microtel.Com EIRL	No Supervisado

Fuente: Microtel.com EIRL

La tabla 07 representa el estado de supervisión de los recursos TI de la empresa Microtel.com EIRL, en ella se observa que sólo 2 dispositivos eran supervisados por el operador de servicios de Internet Movistar. El resto de recursos son propiedad de la empresa y no eran supervisados, por ello, de presentarse algún evento crítico, se tenía que recurrir a empresas externas para el diagnóstico y solución. En la siguiente figura se observa la cantidad de cobertura de recursos TI supervisados en la empresa antes de la implementación de Pandora FMS:

Figura 106

Cobertura de recursos TI supervisados antes de Pandora FMS



Fuente: Elaboración Propia.

En la figura observamos que únicamente son 2 recursos supervisados en la empresa, estos corresponden a los dispositivos del operador; quedando 12 recursos sin supervisión.

Después de la implementación, gracias a Pandora FMS, se logró integrar eficientemente todos los recursos de infraestructura TI de la empresa, supervisando su disponibilidad, latencia y otras métricas críticas. Con esto, la cobertura de supervisión se incrementó al 100%, lo que representa un aumento del 90%.

Tabla 8

Supervisión de recursos TI después de Pandora FMS

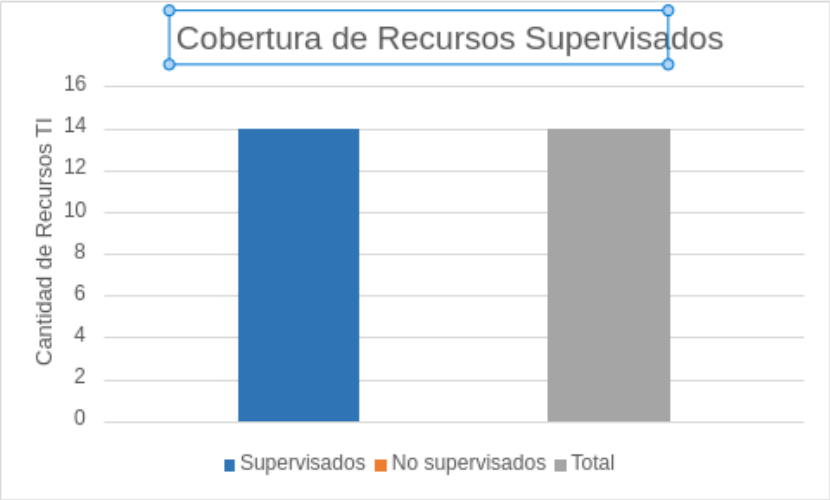
MICROTEL.COM	Elaborado por: José Lazo		Supervisados	14
	Versión: 2 - 08/2018		No supervisados	0
Supervisión de Equipos TI				
Descripción	Tipo de Dispositivo	Dirección IP	Supervisor	Estado
Router Castlenet Technology CBV384Z4	Router	192.168.3.1	Operador Movistar Empresas	Supervisado
Firewall NG	Firewall	192.168.3.2	Operador Movistar Empresas	Supervisado
Switch Core – CISCO SF300	Switch	192.168.1.200	Microtel.Com EIRL	Supervisado
Switch – D-Link DGS-1100-24P	Switch	192.168.1.201	Microtel.Com EIRL	Supervisado
Switch – D-Link DGS-1100-8P	Switch	192.168.1.202	Microtel.Com EIRL	Supervisado
Central VOIP Zycoo	Servidor	192.168.1.8	Microtel.Com EIRL	Supervisado
Servidor NVR HIKVISION	Servidor	192.168.30.2	Microtel.Com EIRL	Supervisado
Servidor Hypervisor Promox VE	Servidor	192.168.20.30	Microtel.Com EIRL	Supervisado
Servidor de Backups	Servidor	192.168.20.41	Microtel.Com EIRL	Supervisado
AP TP-LINK TL-WR940N	Access Point	192.168.10.50	Microtel.Com EIRL	Supervisado
AP TP-LINK TL-WA901ND	Access Point	192.168.10.20	Microtel.Com EIRL	Supervisado
Cámara Exterior HIKVISION	Servidor	192.168.30.3	Microtel.Com EIRL	Supervisado
Cámara Interior 1 HIKVISION	Cámara	192.168.30.8	Microtel.Com EIRL	Supervisado
Cámara Interior 2 HIKVISION	Cámara	192.168.30.13	Microtel.Com EIRL	Supervisado

Fuente: Microtel.com EIRL

La tabla 08, corresponde a la versión 2 del documento de Supervisión de Equipos TI en la empresa Microtel.com EIRL, la cual evidencia la totalidad de recursos supervisados por la herramienta de monitoreo Pandora FMS. La grafica que se muestra a continuación, indica la supervisión total de los recursos TI en la empresa.

Figura 107

Cobertura de recursos TI supervisados después de Pandora FMS



Fuente: Elaboración Propia.

b) Reducir el tiempo de inactividad de los recursos de TI:

Se midieron los tiempos de inactividad que presentaban los recursos TI de la empresa, para ello se hará uso del documento Reporte de Incidencias de Infraestructura TI, proporcionada por el área de Administración de la empresa. Para el análisis se usará

información correspondiente al año 2018 entre los meses de Mayo y Junio. Adicionalmente en los cálculos, promedios y gráficas, se excluye el tiempo de inactividad del incidente "sin correo electrónico", puesto que dicho incidente se venía generando con anterioridad y se había concluido en que el proveedor de webhosting estaba en proceso de migración de sus servicios, por ende, era frecuente tener interrupciones en el servicio de correo durante esos meses.

Antes de la implementación de Pandora FMS, se registraban al mes, diversos incidentes de inactividad de los recursos TI, teniendo un resultado de 32 horas de inactividad durante el periodo de tiempo analizado.

Tabla 9

Reporte de incidencias de recursos TI antes de Pandora FMS

MICROTEL.COM	Elaborado por: José Lazo	Versión	2		
	Responsable: Administración				
Reporte de Incidentes de Infraestructura TI					
Fecha	Tipo Incidente	Descripción	Tiempo Respuest (horas)	Estado	Resolución
03-05-18	Hardware	Sin acceso a WIFI "Gerencia"	2	Resuelto	Reinicio del access point
04-05-18	Hardware	Sin conexión a internet	3	Pendiente	Se reinciaron los sistemas de comunicaciones
04-05-18	Servicio	Conexión Lenta a Internet	3	Resuelto	Se reiniciaron los switches
09-05-18	Servicio	Sin correo electrónico	6	Resuelto	Resuelto por el proveedor de webhosting
10-05-18	Hardware	Sin acceso a WIFI "Gerencia"	3	Resuelto	Reinicio del access point
17-05-18	Hardware	Sin conexión a internet	3	Pendiente	Se reinciaron los sistemas de comunicaciones
17-05-18	Hardware	Sin acceso a WIFI "Gerencia"	2	Resuelto	Reinicio del access point
22-05-18	Servicio	Conexión Lenta a Internet	2	Resuelto	Se reiniciaron los switches
29-05-18	Hardware	Sin conexión a internet	4	Pendiente	Se reinciaron los sistemas de comunicaciones
08-06-18	Hardware	Sin conexión a internet	2	Pendiente	Se reinciaron los sistemas de comunicaciones
12-06-18	Servicio	Conexión Lenta a Internet	2	Resuelto	Se reiniciaron los switches
15-06-18	Servicio	Sin correo electrónico	4	Resuelto	Resuelto por el proveedor de webhosting
19-06-18	Hardware	Sin conexión a internet	3	Pendiente	Se reinciaron los sistemas de comunicaciones
21-06-18	Hardware	Sin conexión a internet	3	Pendiente	Se reinciaron los sistemas de comunicaciones

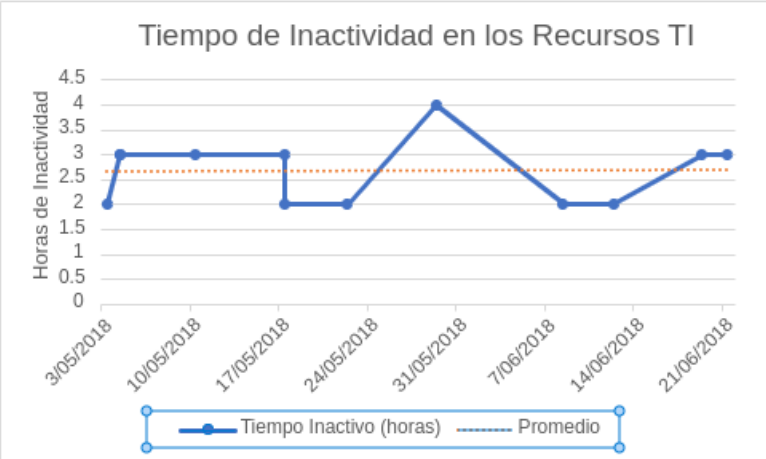
Fuente: Microtel.com EIRL

La tabla 09, evidencia el registro y el tiempo de respuesta cuando se presenta algún incidente en los recursos de infraestructura TI, en ella se observa que tener una respuesta a un incidente puede tomar de 2 a 6 horas. Esto se debe a que la empresa, no disponía de una plataforma que notifique de manera inmediata si algún recurso de TI quedase inactivo, tomando mucho tiempo en saber que recurso TI es el implicado. Los registros mostrados en la tabla 09 corresponden al mes de Mayo y Junio del 2018. En la figura 104 se muestra el

tiempo de inactividad en horas de los recursos TI de la empresa antes de realizar la implementación de Pandora FMS.

Figura 108

Tiempo de inactividad en los recursos TI antes de Pandora FMS



Fuente: Elaboración Propia.

Después de la implementación, no sólo se evidenció la reducción de las incidencias, sino también, la reducción en el tiempo de inactividad que presentaban los recursos TI, teniendo un resultado de 5.4 horas de inactividad durante el periodo de tiempo analizado.

Tabla 10

Reporte de incidencias de recursos TI después de Pandora FMS

MICROTEL.COM	Elaborado por: José Lazo		Versión	2	
	Responsable: Administración				
Reporte de Incidentes de Infraestructura TI					
Fecha	Tipo Incidente	Descripción	Tiempo Respuest (horas)	Estado	Resolución
03-08-18	Hardware	Sin acceso a WIFI "Gerencia"	00:35:00	Resuelto	Reinicio del access point
06-08-18	Hardware	Sin conexión a internet	00:45:00	Pendiente	Se reinciaron los sistemas de comunicaciones
06-08-18	Servicio	Conexión Lenta a Internet	01:00:00	Pendiente	Se reiniciaron los switches
08-08-18	Servicio	Sin correo electrónico	24:00:00	Resuelto	Resuelto por el proveedor de webhosting
14-08-18	Hardware	Sin acceso a WIFI "Usuarios"	00:35:00	Resuelto	Reinicio del access point
16-08-18	Hardware	Sin correo electrónico	07:00:00	Resuelto	Resuelto por el proveedor de webhosting
16-08-18	Hardware	Conexión Lenta a Internet	02:00:00	Pendiente	Se reinciaron los sistemas de comunicaciones
20-08-18	Servicio	Sin correo electrónico	05:00:00	Pendiente	Resuelto por el proveedor de webhosting
21-08-18	Hardware	Sin correo electrónico	03:00:00	Pendiente	Resuelto por el proveedor de webhosting
21-08-18	Hardware	Sin acceso a WIFI "Usuarios"	00:45:00	Pendiente	Reinicio del access point

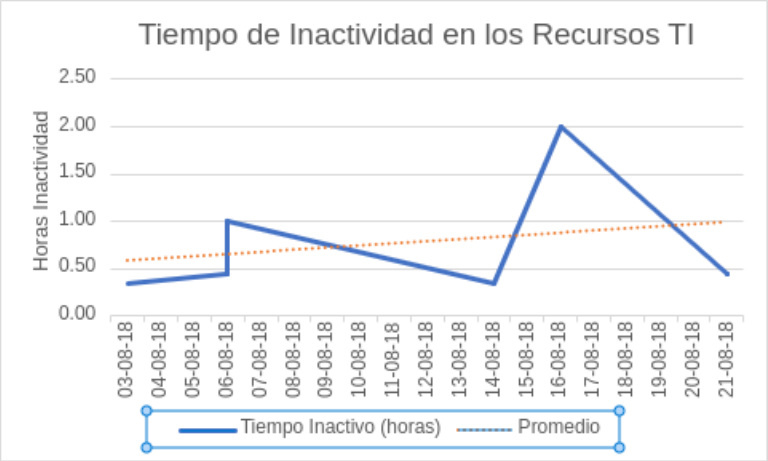
Fuente: Microtel.com EIRL

La información mostrada en la tabla 10, evidencia la reducción de incidencias y el tiempo de respuesta a incidentes suscitados en la infraestructura TI de la empresa después de la implementación de Pandora FMS. Se observa que el tiempo de respuesta ha disminuido significativamente. Este cambio se debe a que Pandora FMS supervisa de manera intensiva,

cada 5 minutos los recursos TI de la empresa, y notificará inmediatamente por correo electrónico si se presenta algún evento crítico. Además el mensaje de alerta por correo electrónico envía todos los detalles necesarios del recurso afectado: Nombre, dirección IP, métrica crítica, hora del evento y una gráfica de 24 horas de la métrica . La tabla muestra registros que corresponden al mes de Agosto del 2018. En la figura 105 se observa el tiempo de inactividad en horas de los recursos TI de la empresa después de implementar Pandora FMS.

Figura 109

Tiempo de inactividad en los recursos TI después de Pandora FMS

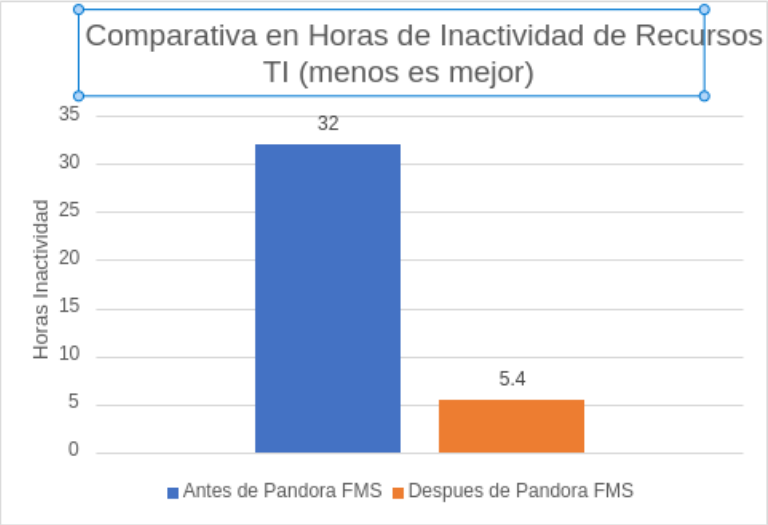


Fuente: Elaboración Propia.

De igual manera, se puede apreciar en la figura 106, el acumulado de horas de inactividad de los recursos TI de la empresa. Correspondiendo a 32 horas antes de Implementar Pandora FMS y 5.4 después de la implementación.

Figura 110

Comparativa en horas de inactividad en los recursos TI



Fuente: Elaboración Propia.

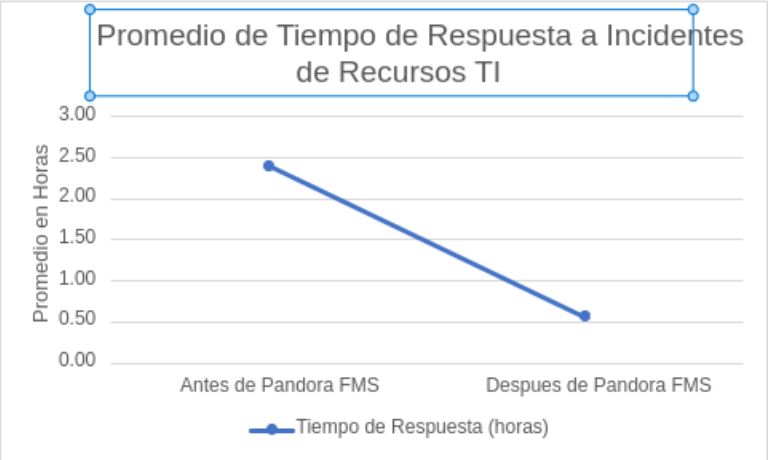
c) Mejorar el tiempo de respuesta a incidentes suscitados en la infraestructura TI:

Se midió comparando el tiempo promedio de respuesta a incidentes antes y después de la implementación de Pandora FMS.

Antes de la implementación, el promedio de tiempo de respuesta a incidentes era de 2.40 horas por incidente. Después de Implementar Pandora FMS, los tiempos de respuesta se han reducido considerablemente, puesto que la herramienta se encarga de realizar los chequeos cada 5 minutos y notificar de inmediato si ocurre un evento crítico. De tal forma, el promedio de tiempo de respuesta a incidentes se redujo a 0.56 horas, como se puede apreciar en la figura 107.

Figura 111

Promedio de tiempo de respuesta a incidentes de recursos TI



Fuente: Elaboración Propia.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El trabajo de investigación desarrollado, ha permitido cumplir satisfactoriamente con los objetivos establecidos al inicio de este estudio.

Se ha logrado implementar con éxito la plataforma de monitoreo Pandora FMS en la empresa Microtel.Com EIRL. Para ello se ha creado una máquina virtual que servirá como base de la plataforma de monitoreo, se utilizó el sistema operativo Rocky Linux versión 8 y se procedió a instalar Pandora FMS, ejecutando el script de instalación automática.

La implementación de Pandora FMS ha logrado ampliar la cobertura total de supervisión de los recursos TI de la empresa, esto optimiza los procesos de resolución de respuesta frente a interrupciones que pueden ocasionar los recursos TI no supervisados.

Gracias a Pandora FMS, Microtel.Com EIRL se entera en tiempo real, si un recurso TI queda inactivo, mediante el alertado por correo electrónico y por Telegram, contribuyendo a minimizar los tiempos de inactividad.

Se logró reducir el tiempo de respuesta a incidentes en los recursos TI de la empresa, pasando de 2.40 horas a 0.56 horas por incidente. Esto se debe a que Pandora FMS alerta y notifica inmediatamente, de presentarse eventos críticos.

5.2. Recomendaciones

Para mantener la efectividad de Pandora FMS como plataforma de monitoreo, se recomienda realizar un mantenimiento regular y mantener el software actualizado. Para ello Pandora FMS ofrece dos modelos de versiones: RRR (Regular Rolling Release), ideal para aquellos usuarios que necesitan tener las últimas características, suelen lanzarme de manera mensual; por otro lado, el modelo que se implementó en Microtel.Com EIRL es la LTS (Long Time Support), lo cual ofrece mayor estabilidad y corrección de errores, suelen lanzarse cada 6 meses, 2 veces por año. A fecha del desarrollo del presente trabajo de suficiencia profesional, Microtel.Com EIRL, cuenta con la versión 772 LTS de Pandora FMS.

Se recomienda analizar las métricas que se desean supervisar, ya que Pandora FMS tiene la capacidad de emplear una variedad de protocolos en su monitoreo, más allá de depender exclusivamente de ICMP y SNMP, además la herramienta también dispone de una extensa colección de plugins que permiten la ampliación de sus funcionalidades de manera exitosa.

Analizar los reportes generados en Pandora FMS favorece el análisis para una futura toma de decisiones sobre los recursos TI de la empresa. Por ello se puede generar informes con rangos de tiempo por horas, días y meses de manera sencilla.

Elegir el correcto método de alertado, puesto que recibir un correo electrónico puede tener limitaciones de recepción, comparado con recibir una notificación inmediata mediante Telegram en el móvil del personal responsable del monitoreo.

Capacitarse de manera continua en Pandora FMS, es la clave para transcender del monitoreo básico al monitoreo proactivo y óptimo. Por ello se cuenta con una extensa documentación libre y de fácil acceso, asimismo se tiene a disposición una amplia la comunidad activa, atentos a cualquier consulta o requerimiento.

REFERENCIAS

Acronis International GmbH. (2020). Las 10 mejores herramientas para monitorizar aplicaciones y servidores. Obtenido de https://www.acronis.com/es-es/blog/posts/monitoring-tools/

Amazon Web Services, Inc. (s.f.). ¿Qué es la latencia de red? Obtenido de https://aws.amazon.com/es/what-is/latency/

Arsys. (2022). SSH: qué es y cómo funciona este protocolo. Obtenido de https://www.arsys.es/blog/ssh#:~:text=SSH%20son%20las%20siglas%20de,como%20v%C3%ADa%20para%20las%20comunicaciones.

Atlassian. (s.f.). Diferencia entre los SLA, los SLO y los SLI. Obtenido de https://www.atlassian.com/es/incident-management/kpis/sla-vs-slo-vs-sli

Cantos San Emeterio, J. (2021). Diseño e implementación de una plataforma de gestión mediante LibreNMS : monitorización y control de la red privada del laboratorio de Telemática (GIT – UNICAN). *Para optar el título de Ingeniería de Tecnologías de Telecomunicación.* Universidad de Cantabria, Santander. Obtenido de http://hdl.handle.net/10902/23014

Clavijo Moran, H. (2021). Propuesta de implementación de una red LAN administrada con servidor CentOS en la I.E. 055 Fidel Oyola Romero del caserío de Garbanzal – Tumbes; 2021. *Tesis para optar el título profesional de Ingenierio de Sistemas.* Universidad Católica los Ángeles, Chimbote. Obtenido de https://hdl.handle.net/20.500.13032/23170

Cloudflare, Inc. (s.f.). ¿Qué es IMAP? Obtenido de https://www.cloudflare.com/es-es/learning/email-security/what-is-imap/

Cloudflare, Inc. (s.f.). ¿Qué es la tenencia múltiple? Obtenido de https://www.cloudflare.com/es-es/learning/cloud/what-is-multitenancy/

DevopsCube. (2023). Best Open Source & Free Monitoring Tools. Obtenido de https://devopscube.com/best-opensource-monitoring-tools/

Fortinet, Inc. (s.f.). ¿Qué es Traceroute? ¿Qué hace y cómo funciona? Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/traceroutes

Free Software Foundation, Inc. (2022). Licencias. Obtenido de https://www.gnu.org/licenses/licenses.es.html

Gobantes Martínez, F. (2023). Laboratorio Docente Virtual basado en el simulador GNS3 para la Gestión y Operación de Redes mediante el protocolo SNMP. *Para optar el título de Ingeniería de Tecnologías de Telecomunicación.* Universidad de Cantabria, Santander. Obtenido de https://hdl.handle.net/10902/29520

GoDaddy. (2021). ¿Cuál es la diferencia entre HTTP y HTTPS? Obtenido de https://es.godaddy.com/blog/diferencia-entre-http-y-https/

Harithsa, V. (2023). Learn the history — The Path to Observability. *The Technologist*. Obtenido de https://thetechnologist.in/learn-the-history-the-path-to-observability-a677f49fd4af

Hertzog, R., & Mas, R. (2017). *El manual del Administrador de Debian.* Freexian SARL. Obtenido de https://debian-handbook.info/browse/es-ES/stable/

Hostinger. (2023). ¿Qué es Apache? Descripción completa. Obtenido de https://www.hostinger.es/tutoriales/que-es-apache/

IBM Corporation. (s.f.). ¿Qué es una notificación push? Obtenido de https://www.ibm.com/es-es/topics/push-notifications

IBM Corporation. (2021). Protocolo simple de transferencia de correo (SMTP). Obtenido de https://www.ibm.com/docs/es/i/7.3?topic=information-smtp

IBM Corporation. (2022). Identificador de objeto (OID). Obtenido de https://www.ibm.com/docs/es/svd/10.0?topic=schema-object-identifier-oid

Infranetworking Internacional. (2018). MySQL vs Percona. Obtenido de https://blog.infranetworking.com/mysql-vs-percona/

International IT. (2021). Monitoreo de Red: Beneficios y Ventajas. Obtenido de https://www.internationalit.com/post/monitoreo-de-red-beneficios-y-ventajas?lang=es

Intriago et al., (2022). Evaluación de herramientas de monitoreo para mejorar la seguridad de la red. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, 8(4)*. Obtenido de https://cienciamatriarevista.org.ve/index.php/cm/article/view/1053

IONOS. (2020). Qué es TCP (Transport Control Protocol). Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/que-es-tcp-transport-control-protocol/

IONOS. (2023). ¿Qué es un Backup? Obtenido de https://www.ionos.es/digitalguide/servidores/seguridad/que-es-un-backup/

IONOS. (1 de Marzo de 2023). ¿Qué es un servidor? Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

IONOS. (2023). SNMP (Simple Network Management Protocol). Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/snmp/#:~:text=SNMP%20trap%3A%20las%20SNMP%20traps,pueden%20distinguirse%20de%20dos%20maneras.

Lamana Núñez, D. (2022). Puesta en marcha de una plataforma de monitorización red. *Para optar el título de Ingeniería Informática.* Universidad Politécnica de Madrid, Madrid. Obtenido de https://oa.upm.es/69895/

Leira Osuna, R. (2019). Aplicación de Big Data al análisis, monitorización y seguridad de redes de comunicaciones. *Para optar el título de Tesis Doctoral.* Universidad Autónoma de Madrid, Madrid. Obtenido de https://dialnet.unirioja.es/servlet/tesis?codigo=261532

Livaction. (2022). A Brief History of Network Monitoring Tools. Obtenido de https://www.liveaction.com/blog/a-brief-history-of-network-monitoring-tools/

Marañón Martín, J. (2013). Implementación de una plataforma de servidores de aplicaciones. *Para optar el título de Ingeniería en Informática de Sistemas.* Universitat Autònoma de Barcelona, Sabadell. Obtenido de https://ddd.uab.cat/record/118619

Marcos García, S. (2021). Análisis y aplicación del protocolo SNMP en el ámbito de la monitorización de recursos. *Para optar el título de Ingeniería Informática.* Universidad de Alcalá, Madrid. Obtenido de http://hdl.handle.net/10017/47330

McAfee, LLC. (2021). ¿Qué es un proxy? Obtenido de https://www.mcafee.com/blogs/es-es/privacy-identity-protection/que-es-un-proxy//

Michis, S. V. (2022). Gestión centralizada de Logs. Herramientas de código abierto. *Grado en Ingeniería Informática.* Universitat Politècnica de València, Valencia. Obtenido de http://hdl.handle.net/10251/188016

Montero Cadena, H. (2022). Implementación de un sistema de monitoreo y control de la infraestructura de ti para la gestión de incidencias en la red interna de la empresa avícola Pollo Favorito S.A. (POFASA). *Para optar el título de Ingeniería en Sistemas Informáticos y de Computación.* Escuela Politécnica Nacional, Quito. Obtenido de https://bibdigital.epn.edu.ec/handle/15000/23196

Mozilla Corporation's. (2023). Introducción a XML. Obtenido de https://developer.mozilla.org/es/docs/Web/XML/XML_introduction

NeoAttack. (2021). Widgets. Obtenido de https://neoattack.com/neowiki/widgets/

Nmap Software LLC. (s.f.). Técnicas de sondeo de puertos. Obtenido de https://nmap.org/man/es/man-port-scanning-techniques.html

Paessler AG. (s.f.). ¿Qué es Ping? Obtenido de https://www.paessler.com/es/it-explained/ping

Pandora FMS. (2021). Mapa de Funcionalidades. Obtenido de https://pandorafms.com/wp-content/uploads/2021/12/Mapa-de-funcionalidades.pdf

Pandora FMS. (2021). Mayor que el Génesis bíblico: el Génesis del Protocolo Tentacle. Obtenido de https://pandorafms.com/blog/es/protocolo-tentacle/

Pandora FMS. (2023). ¿Qué es WMI? Windows Management Instrumentation, ¿lo conoces? Obtenido de https://pandorafms.com/blog/es/que-es-wmi/

Pandora FMS. (2023). Monitorización SNMP: claves para aprender a usar el Protocolo Simple de Administración de Red. Obtenido de https://pandorafms.com/blog/es/monitorizacion-

snmp/#:~:text=El%20polling%20consiste%20en%20lanzar,preconfigurada%20y%20de%20forma%20as%C3%ADncrona.

Pandora FMS. (s.f.). Arquitectura. Obtenido de https://pandorafms.com/manual/!current/es/documentation/01_understanding/02_architecture

Pandora FMS. (s.f.). Arquitectura. *Topologías, esquemas y modelos de monitorización*. Obtenido de https://pandorafms.com/manual/!current/es/documentation/01_understanding/02_architecture#topologias_esquemas_y_modelos_de_monitorizacion

Pandora FMS. (s.f.). Consolas Visuales. Obtenido de https://pandorafms.com/manual/!current/es/documentation/04_using/05_data_presentation_visual_maps

Pandora FMS. (s.f.). Eventos. Obtenido de https://pandorafms.com/manual/!current/es/documentation/04_using/02_events

Pandora FMS. (s.f.). Instalación. *Requisitos mínimos hardware*. Obtenido de https://pandorafms.com/manual/!current/es/documentation/02_installation/01_installing#requisitos_minimos_hardware

Pandora FMS. (s.f.). Instalación. *Requisitos mínimos de software*. Obtenido de https://pandorafms.com/manual/!current/es/documentation/02_installation/01_installing#requisitos_minimos_de_software

Pandora FMS. (s.f.). Instalación Agentes Pandora FMS. *Requisitos para el Agente*. Obtenido de https://pandorafms.com/manual/!current/es/documentation/07_technical_annexes/32_pfms_install_software_agent#requisitos_para_el_agente

Pandora FMS. (s.f.). Introducción a la monitorización. *Módulos*. Obtenido de https://pandorafms.com/manual/!current/es/documentation/03_monitoring/01_intro_monitoring#modulos

Pandora FMS. (s.f.). Introducción a la monitorización. *Monitorización de estados*. Obtenido de https://pandorafms.com/manual/!current/es/documentation/03_monitoring/01_intro_monitoring#monitorizacion_de_estados

Pandora FMS. (s.f.). La historia de Pandora FMS. Obtenido de https://pandorafms.com/es/historia-de-pandora-fms/

Pandora FMS. (s.f.). Personalización de la consola: Dashboard. Obtenido de https://pandorafms.com/manual/!current/es/documentation/04_using/09_dashboard

Pandora FMS. (s.f.). Sistema de alertas. Obtenido de https://pandorafms.com/manual/!current/es/documentation/04_using/01_alerts

Portero López, D. (2021). Unificación de herramientas de monitoreo de componentes y servicios de ti. *Para optar el título de Ingeniería en Sistemas Informáticos y de Computación.* Escuela Politécnica Nacional, Quito. Obtenido de https://bibdigital.epn.edu.ec/handle/15000/21817

Red Hat, Inc. (2022). ¿Qué es la alta disponibilidad? Obtenido de https://www.redhat.com/es/topics/linux/what-is-high-availability

Red Hat, Inc. (2023). ¿Qué es el open source? Obtenido de https://www.redhat.com/es/topics/open-source/what-is-open-source

Red Hat, Inc. (2023). ¿Qué es un hipervisor? Obtenido de https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor

Rodríguez Trujillo et al., (2022). Sistema Integrado de Gestión de conmutadores LAN empleando el protocolo SNMP. *RIELAC, 43, 3*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282022000300001

SEO Estudios. (2020). Qué es un script: cómo funciona, cómo crearlo o eliminarlo. Obtenido de https://www.seoestudios.es/que-es-un-script/

TechTarget. (2023). IT monitoring. Obtenido de https://www.techtarget.com/searchitoperations/definition/IT-monitoring

The PHP Group. (s.f.). ¿Qué es PHP? Obtenido de https://www.php.net/manual/es/intro-whatis.php

Trigo Caparros, F. (2021). Desarrollo de un sistema web para la monitorización de redes en tiempo real. *Para optar el título de Ingeniería Informática.* Universitat Autònoma de Barcelona, Barcelona. Obtenido de https://ddd.uab.cat/record/238444

Vega Picon, G. (2018). Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última milla. *Para optar el título de Magíster en Telecomunicaciones.* Universidad Católica de Santiago de Guayaquil, Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/11890

Zidek, M. (2022). The History and Future of Network Monitoring. *International Journal of Engineering Research and Reviews, 10(3)*. Obtenido de https://zenodo.org/records/7060322