EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico de Zitácuaro

INSTITUTO TECNOLÓGICO DE ZITÁCUARO

DIVISIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

MAESTRÍA EN SISTEMAS COMPUTACIONALES

“CENTRALIZACIÓN DE REGISTROS Y AUTOMATIZACIÓN DE PROCESO DE REPORTEO EN ANÁLISIS FORENSE DIGITAL”

T E S I S

PARA OBTENER EL GRADO DE:

MAESTRO EN SISTEMAS COMPUTACIONALES

PRESENTA:

Enrique Alanís Hernández

DIRECTOR DE TESIS

Dr. Eduardo López Sandoval

CODIRECTOR

M. en I.S.C. SAMUEL EFRÉN VIÑAS ALVAREZ

LUGAR Y FECHA

H. Zitácuaro, Mich. a 01 de diciembre de 2024

Carta de Autorización	Revisión:	001	Fecha de emisión:	21-10-2024
ITZ-AC-TL-FO-003	Elaborado por:		Jefatura de la DEPI	
	Revisado por:		Sistema de Gestión Integrado	
	Autorizado por:		Subdirección académica	

H. Zitácuaro, Mich., 13/Noviembre/2024

CARTA DE AUTORIZACIÓN

ING. DANIEL HERNÁNDEZ DURÁN
SUBDIRECTOR ACADÉMICO
PRESENTE

De acuerdo con los Lineamientos para la Operación de los Estudios de Posgrado en el Tecnológico Nacional de México, en donde se establecen los requisitos para la obtención del grado de Maestría; el H. Comité Tutorial **del C. ENRIQUE ALANÍS HERNÁNDEZ,** estudiante del programa de **MAESTRÍA EN SISTEMAS COMPUTACIONALES**, con número de control: **M22650431,** después de haber realizado la revisión del contenido y formato de tesis **"CENTRALIZACIÓN DE REGISTROS Y AUTOMATIZACIÓN DE PROCESO DE REPORTEO EN ANÁLISIS FORENSE DIGITAL"** emite su consentimiento para continuar con el proceso de obtención de grado académico correspondiente.

Por ese motivo se solicita a usted Autorizar al **C. ENRIQUE ALANÍS HERNÁNDEZ** la impresión y reproducción de la tesis *in comento*.

A T E N T A M E N T E
Excelencia en Educación Tecnológica®

H. Comité Tutorial

Director de tesis

Dr. Eduardo López Sandoval

Codirector de Tesis

Mtro. Samuel Efrén Viñas Álvarez

Dr. Noel Enrique Rodríguez Maya
Revisor

Dra. Irna Zukeyt Garduño Jaimes
Revisora

SECRETARIA DE EDUCACION PUBLICA
INSTITUTO TECNOLOGICO DE ZITACUARO
DEPTO DE DIVISION DE ESTUDIOS DE POSGRADO E INVESTIGACION

Autorización de Impresión de Tesis	Revisión:	001	Fecha de emisión:	21-10-2024
ITZ-AC-TL-FO-006	Elaborado por:		Jefatura de la DEPI	
	Revisado por:		Sistema de Gestión Integrado	
	Autorizado por:		Subdirección académica	

H. Zitácuaro, Mich., 19/noviembre/2024

AUTORIZACIÓN DE IMPRESIÓN DE TESIS

C. ENRIQUE ALANÍS HERNÁNDEZ
NO. DE CONTROL: M22650431
MAESTRÍA EN SISTEMAS COMPUTACIONALES
PRESENTE

Conforme los Lineamientos para la Operación de los Estudios de Posgrado en el Tecnológico Nacional de México y por recomendación del H. Comité Tutorial, esta División le autoriza imprimir y reproducir la tesis: **"CENTRALIZACIÓN DE REGISTROS Y AUTOMATIZACIÓN DE PROCESO DE REPORTEO EN ANÁLISIS FORENSE DIGITAL".**

Ruego a Usted dar puntual seguimiento al formato en vigor que, para tal caso, indica las características de diseño que deberá contener tan importante documento.

ATENTAMENTE
Excelencia en Educación Tecnológica®

ING. DANIEL HERNÁNDEZ DURÁN
SUBDIRECTOR ACADÉMICO
INSTITUTO TECNOLÓGICO DE ZITÁCUARO

EDUCACIÓN | SECRETARÍA DE EDUCACIÓN PÚBLICA | TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE ZITÁCUARO
SUBDIRECCIÓN ACADÉMICA

CARTA DE CESIÓN DE DERECHOS

En H. Zitácuaro, Michoacán, a **14 de noviembre de 2024**, el que suscribe, **Enrique Alanís Hernández**, estudiante del programa de **Maestría en Sistemas Computacionales** del Instituto Tecnológico de Zitácuaro, con número de control: **M22650431**, manifiesto que soy autor intelectual de la presente tesis, la cual fue dirigida por el **Dr. Eduardo López Sandoval** y cedo íntegramente los derechos de trabajo de tesis titulado: "**CENTRALIZACIÓN DE REGISTROS Y AUTOMATIZACIÓN DE PROCESO DE REPORTEO EN ANÁLISIS FORENSE DIGITAL**" al Tecnológico Nacional de México / Instituto Tecnológico de Zitácuaro para su uso con fines académicos y de investigación.

Los usuarios pueden consultar y reproducir el contenido para todos los usos que tengan finalidad académica siempre y cuando sea citada la fuente información.

ATENTAMENTE

Enrique Alanís Hernández

Declaración de Originalidad	Revisión:	001	Fecha de emisión:	21-10-2024
ITZ-AC-TL-FO-005	Elaborado por:		Jefatura de la DEPI	
	Revisado por:		Sistema de Gestión Integrado	
	Autorizado por:		Subdirección académica	

DECLARACIÓN DE ORIGINALIDAD DE LA TESIS

En H. Zitácuaro, Michoacán, a **14** de **noviembre** de **2024**, el que suscribe, **Enrique Alanís Hernández**, estudiante del programa de Maestría en **Sistemas Computacionales** del Instituto Tecnológico de Zitácuaro, con número de control: **M22650431**, manifiesto que soy autor intelectual de la presente tesis, la cual fue dirigida por **Dr. Eduardo López Sandoval** con nombre: **"CENTRALIZACIÓN DE REGISTROS Y AUTOMATIZACIÓN DE PROCESO DE REPORTEO EN ANÁLISIS FORENSE DIGITAL"**.

Declaro que la tesis es una obra original, que es de mi autoría y que toda la información y materiales extraídos de otras fuentes han sido debidamente referenciados. Que a la obra no ha sido previamente publicada y que, en caso de violación de derechos de autor, me hago responsable y exonero de toda responsabilidad al Instituto Tecnológico de Zitácuaro.

ATENTAMENTE

Enrique Alanís Hernández

DEDICATORIA:

A mi amada esposa Ana Karen y a mi querida hija Emma Valentina,

A Ana Karen, tu amor incondicional, paciencia y apoyo constante han sido la base sobre la cual he construido este logro. Tu comprensión en los momentos difíciles, tu aliento en los momentos de duda y tu fe inquebrantable en mis capacidades me han dado la fuerza para seguir adelante. No podría haberlo logrado sin ti a mi lado. Esta tesis es tanto tuya como mía, un testimonio de nuestro trabajo en equipo y de nuestro amor.

A Emma Valentina, aunque eres pequeña, tu risa, tu alegría y tu inocencia me han proporcionado la motivación diaria para esforzarme y ser mejor. Quiero que sepas que cada página está impregnada de mi amor y esperanza por tu futuro, Espero que este trabajo sea un recordatorio de que, con esfuerzo y dedicación, cualquier meta es alcanzable. Que siempre persigas tus sueños con la misma pasión y determinación que me han inspirado a lo largo de este camino.

A ambas, les dedico este logro con todo mi amor y gratitud. Gracias por ser mi fortaleza y mi razón de ser.

Enrique.

AGRADECIMIENTO:

Quiero agradecer al Consejo Nacional de Humanidades Ciencias y Tecnología (CONAHCYT) por el apoyo financiero brindado a través de la beca durante mi maestría. Este apoyo ha sido esencial para la realización de mis estudios y la consecución de este objetivo académico. Su compromiso con el desarrollo de la ciencia y la tecnología en nuestro país es invaluable, y me siento honrado de haber sido beneficiario de su programa.

Contenido

Lista de tablas

Lista de figuras

RESUMEN

En la actualidad, la administración eficiente de infraestructuras de TI es crucial para garantizar la continuidad y calidad de los servicios. En este trabajo de tesis se desarrolla un prototipo que utiliza Nagios para el monitoreo de sistemas y Syslog-NG para la recopilación y análisis de logs montado sobre una Raspberry PI. El objetivo principal es integrar ambas herramientas para ofrecer una solución robusta y escalable que facilite la detección y resolución de problemas en tiempo real. La metodología incluye una revisión bibliográfica, el diseño y configuración del prototipo, su integración, y pruebas en un entorno controlado con infraestructura de seguridad FW. Los resultados esperados incluyen la mejora en la detección de incidentes, la generación de informes y una guía práctica para futuras implementaciones. En esta investigación demuestra la viabilidad y beneficios de integrar herramientas de monitoreo y análisis de datos, contribuyendo significativamente a la optimización de la gestión de infraestructuras de TI.

Se hace notar la importancia de contar con un sistema de detección de eventos accesible para cualquier persona, pequeña empresa o mediana empresa que desee proteger la integridad y disponibilidad de su información. Este sistema de seguridad debe proporcionar una visión clara y estrategias para proteger lo que fluye dentro de su red y dispositivos de cómputo.

Finalmente, se enfatiza la necesidad de una colaboración continua para desarrollar tecnologías innovadoras y regulaciones efectivas que enfrenten el constante cambio y la sofisticación de las amenazas cibernéticas en el futuro.

Palabras clave: *Ciberseguridad; Ciberdelincuentes; vulnerabilidad; redes*

ABSTRACT

Currently, efficient IT infrastructure management is crucial to ensuring the continuity and quality of services. This thesis develops a prototype that uses Nagios for system monitoring and Syslog-NG for log collection and analysis, mounted on a Raspberry Pi. The main objective is to integrate both tools to offer a robust and scalable solution that facilitates real-time problem detection and resolution. The methodology includes a literature review, prototype design and configuration, integration, and testing in a controlled environment with FW security infrastructure. The expected results include improved incident detection, report generation, and a practical guide for future implementations. This research demonstrates the feasibility and benefits of integrating monitoring and data analysis tools, significantly contributing to the optimization of IT infrastructure management.

The importance of having an event detection system accessible to anyone, small business, or medium-sized enterprise wishing to protect the integrity and availability of their information is highlighted. This security system must provide a clear vision and strategies to protect what flows within their network and computing devices.

Finally, the need for ongoing collaboration is emphasized to develop innovative technologies and effective regulations that address the constant change and sophistication of future cyber threats.

Keywords: *Cybersecurity; Cybercriminals; Vulnerability; Networks*

INTRODUCCIÓN

En la actualidad, es fundamental monitorear y registrar eventos en sistemas informáticos para garantizar la operatividad y seguridad de las redes y dispositivos. Los sistemas de monitoreo y syslog (registro de sucesos) (Microsoft Learn, 2023) permiten a los administradores de sistemas identificar y solucionar problemas de manera proactiva, además de mantener registros detallados de eventos para auditorías y análisis forenses. La Raspberry PI, con su bajo costo y flexibilidad, se presenta como una opción viable para implementar un sistema de monitoreo y syslog accesible y eficiente.

La investigación actual se enfoca en la ciberdelincuencia y el análisis forense digital. Dentro de la informática forense, se encuentran la respuesta a incidentes (Incident Response) y el análisis forense digital (Digital Forensics) (Alamillo, 2022), que en conjunto forman el DFIR (Digital Forensics Incident Response).

Los profesionales especializados en estas disciplinas buscan responder rápidamente a incidentes de ciberseguridad, minimizando su impacto en las organizaciones. Estos expertos en DFIR se encargan de identificar, investigar y remediar los efectos de un ciberataque, determinando cómo ocurrió, evaluando su alcance y verificando la exfiltración de información, entre otros aspectos como lo menciona el DFIR (Cyberzaintza, s.f.)

Para abordar este tema, es esencial considerar su impacto. Las ciber amenazas han evolucionado e incluyen fraudes en línea, robo de propiedad intelectual, sustracción de información personal, interrupción de servicios, daños a la propiedad y la creación de noticias falsas. Por lo tanto, es crucial contar con una estrategia adecuada para la contención de incidentes y una evaluación continua de riesgos.

Esta investigación se realizó para entender la evolución de la ciberdelincuencia, identificar vectores de ataque y tipos de atacantes, y proteger la integridad y seguridad de la información de los usuarios activos en el ámbito digital. Se pretende ofrecer una visión general del impacto del secuestro de información.

Desde una perspectiva de seguridad informática, profundizar en esta indagación fue un interés profesional. Como trabajador orientado a la seguridad, es importante mantener protegida la información privada de las personas.

En el contexto educativo, las instituciones dependen cada vez más de redes robustas y seguras para garantizar el acceso a información y servicios críticos. El Tecnológico Nacional de México (TecNM), campus Zitácuaro, se enfrenta a una creciente demanda de conectividad y seguridad debido al aumento en el volumen de usuarios, dispositivos conectados y la complejidad de las operaciones diarias que dependen de una red confiable y protegida. En este entorno, la infraestructura de red se convierte en un pilar fundamental, en el que los firewalls juegan un papel crucial al garantizar la seguridad y disponibilidad del tráfico de datos.

El firewall Fortinet, encargado de filtrar, monitorizar y controlar el tráfico entrante y saliente en el TecNM campus Zitácuaro, ha experimentado problemas de saturación y un elevado consumo de recursos debido al incremento de las demandas de la red. Esta sobrecarga ha generado cuellos de botella en la gestión del tráfico, lo que afecta la eficiencia, la seguridad y la continuidad operativa de los servicios digitales. Entre las principales complicaciones que se presentan están la ralentización del tráfico, fallos en la inspección de paquetes y, en casos extremos, la caída parcial o total de la conectividad de la red.

Con el objetivo de abordar estos problemas, surge la necesidad de implementar una solución que permita monitorear de manera efectiva el rendimiento del firewall y, en consecuencia, optimizar el uso de los recursos de red.

El objetivo de este trabajo es evaluar cómo la implementación de este sistema de monitoreo integral puede aliviar la carga del firewall Fortinet, mejorar la visibilidad del tráfico de red y asegurar un entorno más estable y seguro para los usuarios del TecNM campus Zitácuaro. Además, se analizará el impacto de esta solución en términos de eficiencia operativa, reducción de costos y mejora de la seguridad informática.

Este caso de estudio no solo busca resolver una problemática específica dentro del TecNM campus Zitácuaro, sino también servir como referencia para otras instituciones que enfrentan desafíos similares. A través de la investigación, pruebas y análisis realizados, se espera demostrar que una solución basada en herramientas de código abierto, combinada con hardware accesible como la Raspberry Pi, es una alternativa viable para optimizar la infraestructura de red y garantizar su sostenibilidad en el tiempo.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 Análisis del problema

En un entorno cada vez más conectado y dependiente de las tecnologías de la información, la seguridad cibernética se ha convertido en una preocupación fundamental para las organizaciones sector público, sector privado, sector médico, sector educativo por igual.

En el entorno académico del Tecnológico Nacional de México (TecNM) campus Zitácuaro, la seguridad informática es una prioridad esencial para proteger la integridad de los datos y la continuidad operativa de sus sistemas. La red de TecNM es extensa y compleja, abarcando múltiples campus y alojando una gran cantidad de dispositivos conectados, lo que la convierte en un objetivo potencial para ciberdelincuentes que buscan explotar vulnerabilidades en la infraestructura.

A pesar de contar con medidas de seguridad existentes, la creciente sofisticación de los métodos de ataque y el volumen de tráfico en la red dificultan la detección y respuesta oportuna a incidentes de seguridad. Además, la diversidad de dispositivos y la falta de integración de las herramientas de monitoreo actuales limitan la visibilidad y capacidad de respuesta ante posibles amenazas.

En el particular caso del TecNM campus Zitácuaro nos enfrentamos a la creciente asistencia de alumnos a las instalaciones para poder realizar sus actividades cotidianas como parte de la plantilla y alumnado del instituto. Esto deriva en estar pendientes de las capacidades tecnológicas de sus dispositivos de seguridad mismo que se cuenta con un firewall de la marca Fortinet modelo Fortigate 100E en modo stand alone que tiene como finalidad la protección de la red del tecnológico, distribución de DHCP (Gerend, 2023) y salida a internet en general.

Dicho lo anterior, la problemática de no contar con una herramienta de monitoreo del dispositivo de calidad que pueda ofrecernos una vista de uso de recursos y resguardo de bitácoras de syslog del dispositivo.

Los Firewalls Fortinet desempeñan un papel crítico en la distribución de carga de red y la protección de los servicios, y generan una gran cantidad de registros de eventos o registros que contienen información valiosa sobre el rendimiento y la seguridad de la red. (Fortinet, s.f.).

Sin embargo, el análisis efectivo de estos registros de Firewalls el contexto de ciberseguridad se ha vuelto un desafío para las organizaciones. Existen varios obstáculos que dificultan la detección temprana de amenazas y la respuesta oportuna a incidentes de seguridad.

Problemas identificados son los siguientes:

- Volumen y complejidad de los registros: Los Firewall generan una gran cantidad de registros debido a la gran cantidad de transacciones y conexiones que manejan. Estos registros pueden contener información relevante sobre eventos de seguridad, pero su volumen y diversidad de formatos dificultan su análisis eficiente. Además, la falta de una estructura uniforme dificulta la extracción de información significativa y la identificación de eventos importantes.

- Falta de herramientas especializadas: Aunque existen herramientas de análisis de registros en el mercado, la mayoría de ellas están diseñadas para registros genéricos y no se centran específicamente en los registros del firewall Fortinet. Esto limita la capacidad de las organizaciones para realizar un análisis profundo y detallado de los eventos de seguridad específicos de estos dispositivos. La

falta de herramientas especializadas dificulta la identificación de patrones de comportamiento malicioso y la detección temprana de ataques cibernéticos.

- Dificultad en la correlación de eventos: La correlación de eventos es esencial para comprender la secuencia de acciones y eventos relacionados en los registros de los firewalls Fortinet. Sin embargo, la correlación manual de eventos dispersos en diferentes registros y formatos puede ser un proceso complejo y propenso a errores. La falta de herramientas adecuadas de correlación dificulta la identificación de relaciones causales y patrones de comportamiento sospechoso, lo que limita la capacidad de detección y respuesta ante ataques cibernéticos.

- Respuesta lenta a incidentes: La falta de un software de análisis de registros especializado en ciberseguridad para Firewalls Fortinet puede resultar en una respuesta lenta a incidentes de seguridad. La identificación tardía de actividades maliciosas o la dificultad para determinar la causa raíz de un incidente puede llevar a una demora en la mitigación y en la adopción de medidas correctivas. Esto aumenta el tiempo de exposición a posibles amenazas y el impacto de los ataques.

En conjunto, estos desafíos destacan la necesidad de implementar un sistema de monitoreo con Nagios Core y Syslog dentro de una Raspberry PI para el análisis de registros de Firewalls Fortinet enfocado en la ciberseguridad para el tecnológico nacional de México campus Zitácuaro (TecNM). Esto ayudará no solo al tecnológico sino a todas las organizaciones a fortalecer su postura de seguridad y mitigar los riesgos asociados con las amenazas cibernéticas.

1.2 Justificación

La implementación de un sistema de monitoreo y syslog es crucial para la gestión eficiente de redes y sistemas informáticos. Utilizar una Raspberry Pi para este prototipo ofrece una solución accesible, flexible y de bajo costo, especialmente adecuada para pequeñas y medianas empresas, entornos educativos y proyectos personales.

En un entorno de TI, la capacidad de monitorear, gestionar y responder a eventos es crucial para mantener la operatividad y seguridad de la infraestructura.
Ante la creciente importancia de proteger las infraestructuras de red de posibles amenazas y ataques cibernéticos.

A continuación, se presentan las principales razones para respaldar este proyecto:

Detección Proactiva de Problemas

- Nagios permite la monitorización continua de la red y servicios, alertando sobre problemas antes de que afecten gravemente la operatividad.
- Syslog centraliza los logs de diferentes dispositivos, facilitando la detección de patrones anómalos y problemas recurrentes.

Seguridad Mejorada

- La recolección centralizada de logs ayuda a identificar intentos de acceso no autorizados, ataques y otros incidentes de seguridad.
- Permite una rápida respuesta ante eventos sospechosos, minimizando el riesgo de violaciones de seguridad.

Optimización del Rendimiento

- El monitoreo del rendimiento de la red y servicios permite identificar y resolver cuellos de botella.
- Provee datos históricos para el análisis de tendencias y planificación de capacidad.

Cumplimiento Normativo

- Muchas regulaciones requieren la conservación y análisis de logs para auditorías y cumplimiento normativo. Syslog centraliza estos datos, facilitando el cumplimiento.
- Nagios proporciona registros detallados del estado de los sistemas, contribuyendo a los informes de auditoría.

Pequeñas y Medianas Empresas (PYMES), las PYMES pueden implementar una solución de monitoreo efectiva sin necesidad de una gran inversión en infraestructura, mejorando la gestión y seguridad de sus sistemas de TI.

Entornos Educativos, las instituciones educativas pueden usar la Raspberry Pi para enseñar conceptos de monitoreo de redes y gestión de logs, proporcionando una herramienta práctica para los estudiantes, poder ser una referencia para futuros proyectos y despliegues de desarrollos del alumnado.

Hogares y Proyectos Personales, los entusiastas de la tecnología pueden usar la Raspberry Pi para monitorear sus redes domésticas, aprender sobre administración de sistemas y experimentar con proyectos de seguridad.

Laboratorios y Centros de Investigación, monitoreo de equipos y redes en laboratorios de investigación, permitiendo una gestión eficiente de la infraestructura y la recolección de datos para análisis.

Reducción de Costos, implementar un sistema de monitoreo en una Raspberry Pi reduce significativamente los costos iniciales y operativos comparado con soluciones comerciales más grandes.

Eficiencia Operativa Mejorada, monitoreo continuo y alertas automáticas permiten una respuesta rápida a problemas, mejorando la eficiencia operativa y reduciendo el tiempo de inactividad.

Escalabilidad, la solución basada en Raspberry Pi puede escalarse fácilmente agregando más dispositivos según sea necesario, adaptándose al crecimiento de la infraestructura sin grandes inversiones adicionales.

Aumento en la Confiabilidad del Sistema, la capacidad de detectar y resolver problemas rápidamente mejora la confiabilidad general del sistema, asegurando un funcionamiento más estable y predecible.

La implementación de un sistema de monitoreo con Nagios y syslog utilizando una Raspberry Pi por sus múltiples beneficios. Las ventajas específicas de la Raspberry Pi, como su bajo costo, bajo consumo energético, flexibilidad, tamaño compacto y el respaldo de una amplia comunidad, la convierten en una opción ideal para diversos entornos y aplicaciones. Implementar este sistema no solo optimiza la gestión de la infraestructura de TI, sino que también ofrece un enfoque accesible y práctico para mejorar la operatividad y seguridad de las redes y sistemas informáticos.

El presente trabajo reduce considerablemente los costos de creación comparado con otros servicios que existen en el mercado, marcando una diferencia considerable entre los precios de administración, soporte y mantenimiento de las plataformas.

Adicionalmente, no será necesario tener un especialista en redes o con conocimientos avanzados en herramienta de análisis de datos para comprender de manera ágil el

uso de la aplicación. Se considera que la aplicación sea amigable y entendible para la mayoría de las personas con conocimientos básicos de computación.

1.3 Objetivos

1.3.1 Objetivo general

Implementar un sistema de monitoreo en una Raspberry PI utilizando Nagios Core y un servidor Syslog para centralizar, gestionar y analizar los logs y eventos de diversos dispositivos y servicios en la red, mejorando así la administración, seguridad y eficiencia operativa de la infraestructura de TI.

1.3.2 Objetivos específicos

a) Realizar un análisis comparativo de los actuales sistemas que realizan el reporte de incidencias de forma automatizada.
b) Diagnosticar las causas del alto uso de recursos y la saturación del firewall Fortinet
c) Realizar el reporte de eventos mediante correo electrónico.
d) Desarrollar funcionalidades de generación automática de informes de seguridad, que proporcionen detalles técnicos sobre los eventos relevantes detectados en los registros.
e) Crear visualizaciones que permitan a los usuarios explorar y comprender de manera efectiva los datos analizados, facilitando la detección de anomalías y actividades sospechosas.

1.4 Pregunta de investigación

¿Cómo impacta la implementación de un sistema de monitoreo basado en Nagios, Syslog y un servidor NAS, montado en una Raspberry Pi 4B, en la optimización del uso de recursos y la resolución de problemas de saturación del firewall Fortinet en el TecNM campus Zitácuaro?

1.5. Hipótesis

La implementación de un sistema de monitoreo basado en Nagios, Syslog y un servidor NAS, montado en una Raspberry Pi 4B, mejorará significativamente la gestión de los recursos y reducirá los problemas de saturación del firewall Fortinet en el TecNM campus Zitácuaro, optimizando su rendimiento y estabilidad.

1.6. Caso de estudio TecNM Campus Zitácuaro

Estudio de caso en el TecNM Campus Zitácuaro sobre la saturación y uso elevado de recursos en un firewall Fortinet, y la solución con un sistema de monitoreo con Nagios, syslog y un servidor NAS montado en una Raspberry Pi 4B.

La seguridad y el rendimiento de la infraestructura de red son fundamentales en instituciones educativas, especialmente en aquellos entornos que manejan gran cantidad de datos y tráfico, como es el caso del TecNM Campus Zitácuaro. El uso de firewalls, como los dispositivos Fortinet, es esencial para proteger estos entornos de amenazas externas y gestionar el acceso a los recursos internos. Sin embargo, a medida que la red del campus ha crecido, el firewall Fortinet comenzó a presentar síntomas de saturación y elevado uso de recursos, lo que derivó en una reducción del rendimiento y afectó la calidad del servicio para estudiantes, docentes y personal administrativo.

Se presenta un análisis del problema de sobrecarga del firewall Fortinet en el TecNM Campus Zitácuaro, causado por el incremento en la cantidad de dispositivos conectados y el volumen de tráfico. Como solución a esta problemática, se propone la implementación de un sistema de monitoreo y almacenamiento externo basado en una Raspberry Pi 4B, que integra tres componentes clave: Nagios, para la monitorización de los recursos del firewall; Syslog, para la centralización de los registros de eventos; y un servidor NAS, para el almacenamiento seguro de los logs generados por el firewall.

A medida que la demanda sobre la red ha aumentado con el crecimiento de la institución, el firewall Fortinet ha comenzado a experimentar una carga excesiva de trabajo, resultando en varios problemas de rendimiento.

Los principales síntomas observados son los siguientes:

Elevado uso de CPU y memoria, el firewall Fortinet está diseñado para procesar un alto volumen de tráfico de red, pero ante el creciente número de conexiones simultáneas y la cantidad de datos que deben filtrarse, los niveles de uso de CPU y memoria han alcanzado valores críticos. Este uso prolongado de recursos ha llevado a una ralentización en la capacidad de procesamiento de las reglas de firewall, afectando negativamente el rendimiento global de la red.

Como dato estadístico nos encontramos que normalmente en horarios pico tenemos un conteo de usuarios concurrentes de 965 considerando al menos un par de dispositivos por alumno y/o personal administrativo, además de, tener un promedio de 76000 sesiones establecidas en horarios pico.

Saturación del almacenamiento de logs, El firewall genera registros (logs) constantes de eventos de red, incluyendo intentos de conexión, accesos bloqueados y detecciones de posibles amenazas. Estos logs son cruciales para el análisis de seguridad y auditoría. Sin embargo, el almacenamiento interno del firewall ha

comenzado a saturarse debido a la gran cantidad de registros generados. Esto no solo pone en riesgo la capacidad de almacenamiento, sino que también afecta la capacidad del firewall para generar y almacenar nuevos logs, lo que es esencial para la vigilancia continua de la red.

Degradación del rendimiento de la red, los usuarios del campus han comenzado a reportar tiempos de respuesta prolongados en las conexiones a internet y a los recursos internos, especialmente durante las horas pico. Esta degradación en el rendimiento es un síntoma directo de la sobrecarga en el firewall, que no puede procesar eficientemente el tráfico de red debido a la falta de recursos disponibles.

Fallas en la gestión de incidentes de seguridad, debido a la saturación del almacenamiento y la sobrecarga del procesador, existe el riesgo de que se pierdan registros importantes de eventos de seguridad, lo que compromete la capacidad del equipo de TI para identificar y responder adecuadamente a incidentes. Además, la falta de un sistema de monitoreo en tiempo real dificulta la detección temprana de problemas, aumentando la vulnerabilidad de la red ante posibles ataques.

Estos problemas, causados por la saturación de recursos del firewall, amenazan no solo la seguridad de la red del campus, sino también la calidad del servicio que ofrece a su comunidad académica. Por lo tanto, es crucial implementar una solución que no solo monitoree y alerte sobre el uso excesivo de recursos, sino que también descargue parte del trabajo del firewall, asegurando una gestión eficiente de la infraestructura de red.

CAPÍTULO II. MARCO TEÓRICO

El monitoreo y registro de eventos en sistemas informáticos son componentes esenciales para mantener la operatividad, seguridad y eficiencia de una red. Este marco teórico se centra en los fundamentos del monitoreo de sistemas, la gestión de logs (syslog), y la utilización de la Raspberry Pi como plataforma para implementar estas funciones.

2.1 Monitoreo de Sistemas

El monitoreo de sistemas implica la observación continua de los recursos de hardware y software en una red para asegurar que funcionen de manera óptima. Este proceso incluye la supervisión de parámetros como el uso de CPU, memoria, almacenamiento, disponibilidad de servicios, y el rendimiento de aplicaciones.

Objetivos del Monitoreo

A. Detección de Problemas: Identificar fallos y cuellos de botella antes de que afecten a los usuarios.
B. Mantenimiento Predictivo: Predecir y prevenir fallos futuros mediante el análisis de tendencias de rendimiento.
C. Optimización de Recursos: Asegurar que los recursos del sistema se utilicen de manera eficiente.
D. Seguridad: Detectar actividades inusuales que puedan indicar un problema de seguridad.

2.2 Syslog: Sistema de Gestión de Logs

Syslog es un estándar para la transmisión de mensajes de registro en una red. Se utiliza para capturar y almacenar logs de eventos generados por dispositivos y aplicaciones, facilitando el monitoreo y la auditoría del sistema.

Componentes de Syslog

A. Syslog Cliente: Genera y envía mensajes de log a un servidor syslog.
B. Syslog Servidor: Recibe, almacena y analiza los mensajes de log.
C. Syslog Daemon: Un servicio que corre en segundo plano para gestionar los logs.

Beneficios del Uso de Syslog

1. Centralización de Logs: Permite la recopilación de logs de múltiples dispositivos en un solo lugar.
2. Análisis de Seguridad: Facilita la identificación de patrones de ataque y la realización de auditorías de seguridad.
3. Cumplimiento Normativo: Ayuda a cumplir con regulaciones que requieren el registro y almacenamiento de eventos.

2.3 Raspberry Pi

La Raspberry Pi es una computadora de bajo costo y tamaño reducido que se puede utilizar para diversos proyectos de computación. Sus características incluyen una CPU ARM, memoria RAM, puertos USB, interfaz de red, y capacidades de almacenamiento a través de tarjetas microSD. Como se hace mención dentro de la página oficial del componente (Raspberry Pi, 2022).

Ventajas de Utilizar una Raspberry Pi

1. Costo-Efectividad: Su bajo costo hace que sea accesible para proyectos pequeños y medianos.
2. Flexibilidad: Soporta diversos sistemas operativos y software, incluyendo herramientas de monitoreo y syslog.
3. Tamaño y Consumo Energético: Su pequeño tamaño y bajo consumo energético la hacen ideal para despliegues en lugares con limitaciones de espacio y energía.

Implementación de Nagios Core en Raspberry Pi

Nagios Core es una herramienta de monitoreo de código abierto que permite supervisar la disponibilidad y el rendimiento de recursos y servicios en una red.

Funcionalidades de Nagios Core

1. Monitoreo de Servicios y Recursos: Verifica la disponibilidad y estado de servicios como HTTP, FTP, SSH, y recursos como el uso de CPU y memoria.
2. Notificaciones de Alertas: Envía alertas a administradores de sistemas mediante correo electrónico, SMS, u otros métodos.
3. Informes y Gráficos: Genera informes detallados y gráficos sobre el rendimiento del sistema y la disponibilidad de servicios.

Integración de Syslog con Nagios Core en Raspberry Pi

Integrar syslog con Nagios Core en una Raspberry Pi permite una solución completa de monitoreo y gestión de logs, combinando las capacidades de alerta y supervisión de Nagios con la centralización y análisis de logs de syslog.

1. Instalación de Nagios Core y Syslog
2. Configuración inicial de la Raspberry Pi con el sistema operativo Raspberry Pi OS.

3. Instalación de Nagios Core y un servidor de syslog (por ejemplo, rsyslog).

Configuración de Dispositivos para Syslog

1. Configuración de dispositivos en la red para que envíen sus logs al servidor syslog en la Raspberry Pi.
2. Definición de reglas de filtrado y almacenamiento de logs en el servidor syslog.

Configuración de Monitoreo con Nagios Core

Configuración de hosts y servicios en Nagios Core para la supervisión.
Establecimiento de umbrales y condiciones para alertas y notificaciones.

2.4 Visualización y Análisis

Utilización de interfaces web y herramientas adicionales para visualizar el estado de los sistemas y analizar los logs.

Beneficios de la Solución Propuesta

1. Costo Reducido: Utilización de hardware económico sin comprometer funcionalidades críticas.
2. Monitoreo Centralizado: Capacidad de supervisar múltiples dispositivos y servicios desde una única plataforma.
3. Respuesta Proactiva: Identificación y resolución temprana de problemas antes de que afecten la operación del sistema.
4. Seguridad Mejorada: Detección y análisis de eventos de seguridad a través de logs centralizados.

El uso de una Raspberry Pi para implementar un sistema de monitoreo con Nagios Core y un servidor de syslog ofrece una solución eficiente y accesible para la gestión y supervisión de redes y sistemas. Esta configuración proporciona a los administradores de sistemas las herramientas necesarias para mantener la operatividad, seguridad y rendimiento de sus infraestructuras tecnológicas.

2.5 Servicios utilizados

2.5.1 Nagios Core

Nagios Core es una herramienta de monitoreo de sistemas de código abierto que permite a los administradores de sistemas monitorear sus infraestructuras de TI y redes. Puede realizar las siguientes funcionalidades:

Monitoreo de Servicios y Recursos: Nagios Core puede monitorear una variedad de servicios y recursos del sistema, como el uso de CPU, memoria, disco, servicios de red (HTTP, SMTP, etc.), y mucho más.

Alertas y Notificaciones, Cuando se detecta un problema, Nagios Core puede enviar alertas a los administradores a través de varios métodos, incluyendo correo electrónico y mensajes de texto. (Nagios Core, s.f.).

Interfaz Web, Ofrece una interfaz web que permite a los administradores ver el estado de los sistemas monitoreados en tiempo real, revisar históricos de alertas y generar informes.

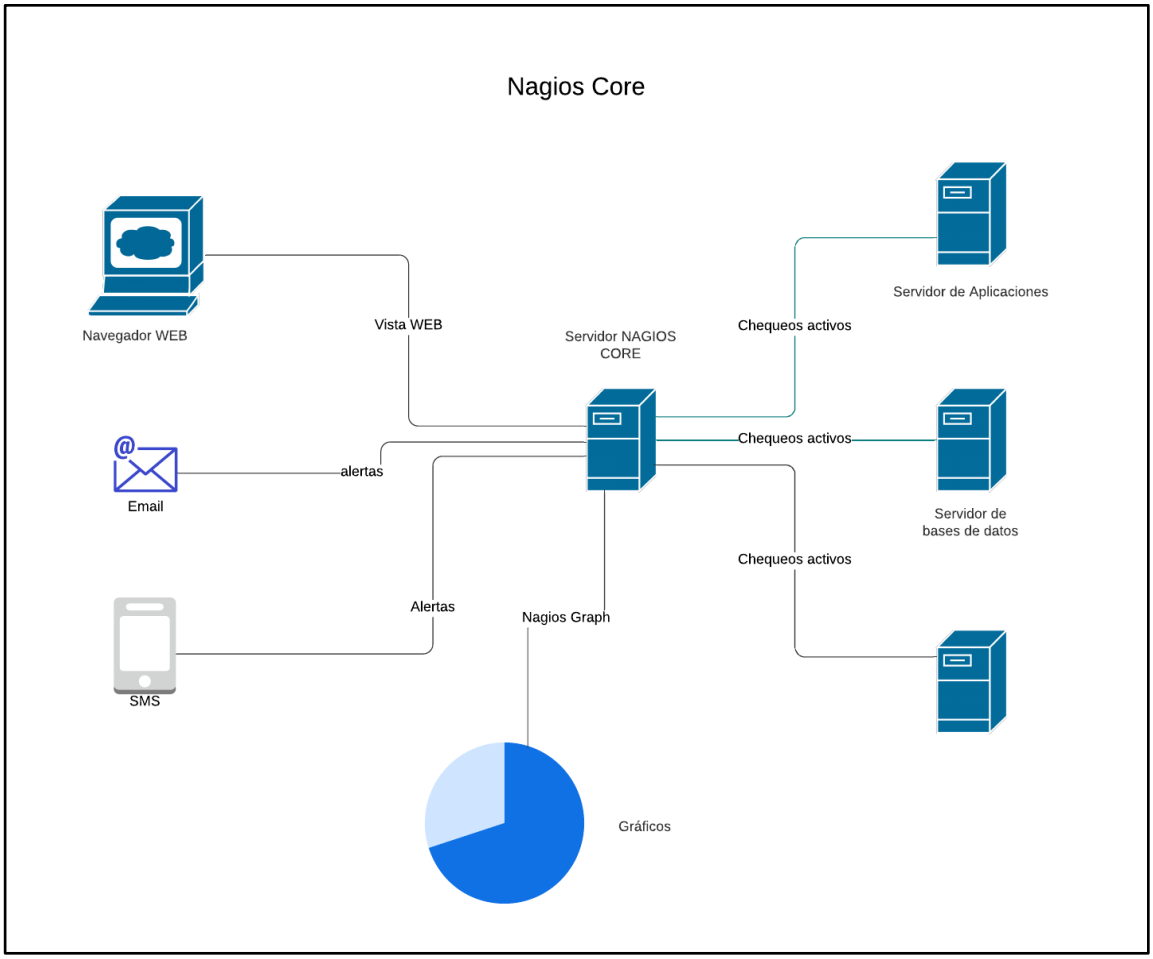
Extensible, Es altamente configurable y extensible mediante plugins, lo que permite monitorear casi cualquier aspecto de la infraestructura de TI.

Comunidad Activa, Como proyecto de código abierto, cuenta con una comunidad activa que contribuye con plugins, configuraciones y soporte.

Nagios Core es una solución robusta para el monitoreo de la infraestructura de TI, que puede ayudar a prevenir problemas y reducir el tiempo de inactividad al alertar a los administradores sobre los problemas potenciales antes de que se conviertan en fallas críticas.

Para mejor comprensión del tema, se tiene como referencia la figura 1 que representa en modo grafico la manera de desplegar un sistema de Nagios:

Figura 1. Diagrama conceptual de Nagios Core. Autor: Elaboración propia.



Nota. Imagen representativa del diagrama de arquitectura de un despliegue de Nagios Core.

2.5.2 Syslog

Syslog es un estándar para el envío de mensajes de registro (logs) en una red IP. Este estándar permite la captura, almacenamiento y análisis de mensajes de log generados por diferentes dispositivos y aplicaciones, facilitando así el monitoreo y la administración de sistemas y redes.

Aquí están algunos puntos clave sobre Syslog:

Formato de Mensajes, los mensajes de Syslog generalmente contienen información sobre el origen del mensaje, la fecha y hora, el nivel de severidad, y el contenido del mensaje.

Niveles de Severidad, syslog define varios niveles de severidad para los mensajes, que van desde emergencias críticas (nivel 0) hasta mensajes de depuración (nivel 7).

1. Emergencia (0):
    a. Descripción: El sistema no es utilizable. Esta es la más alta prioridad.
    b. Ejemplo: Fallo total del sistema o del hardware.

2. Alerta (1):
    a. Descripción: Debe ser corregido inmediatamente.
    b. Ejemplo: Fallo en la integridad de la base de datos o pérdida de datos críticos.

3. Crítico (2):
    a. Descripción: Condiciones críticas.
    b. Ejemplo: Error en una aplicación importante, fallo en un disco duro.

4. Error (3):
    a. Descripción: Condiciones de error.
    b. Ejemplo: Error en un servicio, fallo en una solicitud.

5. Advertencia (4):
    a. Descripción: Condiciones de advertencia.
    b. Ejemplo: Espacio en disco bajo, umbrales de uso de CPU o memoria excedidos.

6. Aviso (5):
    a. Descripción: Condiciones normales pero significativas.
    b. Ejemplo: Reinicio de un servicio, cambios de configuración.

7. Información (6):
    a. Descripción: Información general sobre el funcionamiento del sistema.
    b. Ejemplo: Mensajes de inicio/parada de servicios, información de estado.

8. Depuración (7):
    a. Descripción: Mensajes de depuración detallados.
    b. Ejemplo: Información de trazas de programas, detalles internos de la aplicación.

Facilidades, los mensajes de Syslog también pueden clasificarse por "facilidades" que indican el tipo de proceso que generó el mensaje, como el sistema operativo, el correo, el daemon, etc.

Protocolo de Transporte, syslog típicamente utiliza UDP en el puerto 514 para el transporte de mensajes, aunque también puede usar TCP o TLS para una transmisión más confiable y segura.

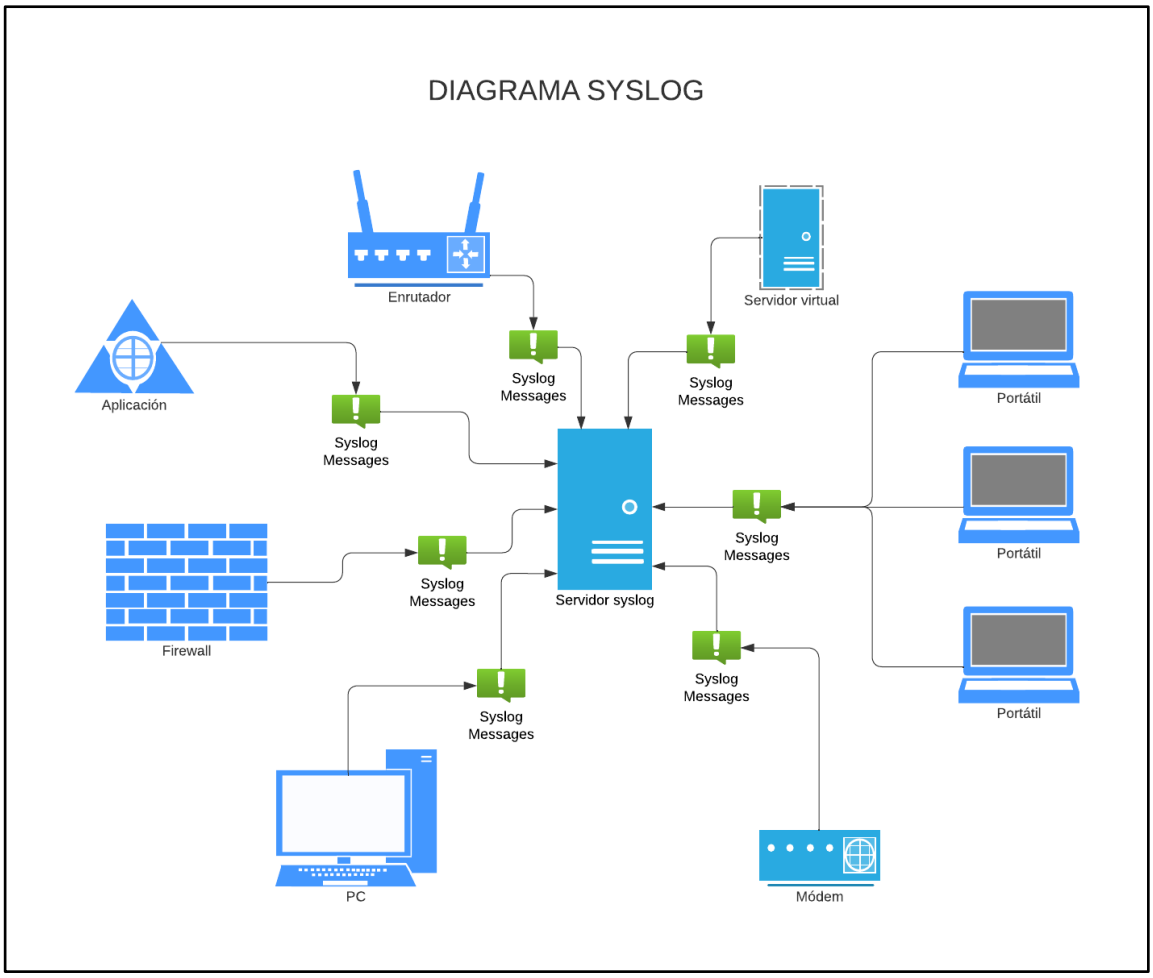
Servidores y Clientes, los sistemas que generan mensajes de log actúan como clientes de Syslog, mientras que los sistemas que reciben y procesan estos mensajes son servidores de Syslog.

Aplicaciones, syslog es ampliamente utilizado en entornos de TI para la gestión de logs de servidores, dispositivos de red, y aplicaciones, permitiendo la centralización de logs y facilitando su análisis.

Ejemplos de implementaciones de Syslog incluyen el demonio syslogd en sistemas Unix/Linux y herramientas como rsyslog y syslog-ng (utilizado). (IBM, 2022).

A continuación, presentamos el diagrama conceptual de la solución de Syslog:

Figura 2. Diagrama conceptual de Syslog. Autor: Elaboración propia.



Nota. Diagrama conceptual de despliegue de un servidor de Syslog.

2.5.3 NAS

Un NAS (Network Attached Storage) es un dispositivo de almacenamiento conectado a la red que permite a múltiples usuarios y dispositivos acceder y compartir archivos desde una ubicación centralizada. Es esencialmente un servidor de archivos

especializado que proporciona almacenamiento y acceso a datos a través de una red, generalmente mediante el protocolo SMB/CIFS (Server Message Block/Common Internet File System) o NFS (Network File System). (IBM, s.f.).

Características principales de un NAS:

los dispositivos NAS se conectan a una red local (LAN) y permiten a los usuarios acceder a los archivos desde cualquier dispositivo en la misma red, ya sea un ordenador, una tableta o un smartphone.

Proporciona una ubicación centralizada para almacenar y gestionar archivos, lo que facilita la administración de datos y mejora la eficiencia del trabajo colaborativo.

Ofrecen diversas características de seguridad, como control de acceso basado en usuario y cifrado de datos, para proteger la información almacenada.

Muchos dispositivos NAS incluyen funcionalidades de copia de seguridad y recuperación de datos, permitiendo programar backups automáticos y restaurar archivos en caso de pérdida de datos.

Se pueden expandir agregando discos duros adicionales o mediante el uso de tecnologías como RAID (Redundant Array of Independent Disks) (Dell, 2021) para mejorar la capacidad de almacenamiento y la redundancia de datos.

Algunos NAS permiten el acceso remoto a los archivos a través de Internet, facilitando el trabajo desde cualquier lugar.

Usos comunes de un NAS

Hogar: Almacenamiento de fotos, videos, música y documentos importantes. También puede usarse para hacer copias de seguridad de todos los dispositivos del hogar.

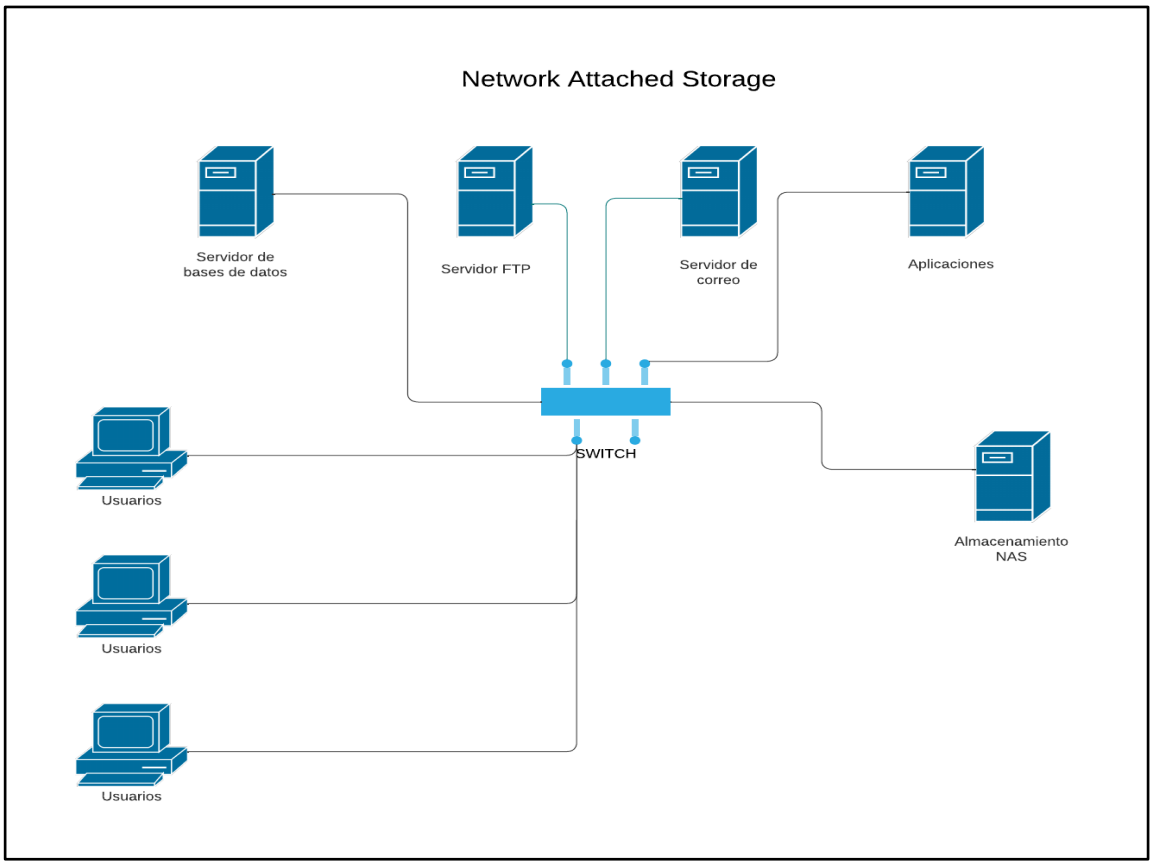
Pequeñas y medianas empresas: Compartir y almacenar documentos, realizar copias de seguridad de datos importantes y mejorar la colaboración entre empleados.

Entornos empresariales: Gestión de grandes cantidades de datos, realización de copias de seguridad y recuperación de desastres, y almacenamiento de archivos de forma segura y centralizada.

Un NAS es una solución práctica y eficiente para el almacenamiento y la gestión de datos en redes locales, ofreciendo flexibilidad, seguridad y facilidad de acceso.

A continuación, se muestra a nivel de arquitectura la solución:

Figura 3. Diagrama conceptual de NAS. Autor: Elaboración propia.



Nota. Diagrama conceptual de integración de un servidor NAS.

2.6 Ciberdelincuencia

2.6.1 Tipos de amenazas

2.6.1.1 Principales amenazas de ciberseguridad

Con respecto a la seguridad informática, es importante estar constantemente actualizado, ya que cada día se desarrollan nuevas maneras de explotar las vulnerabilidades de sistemas y equipos. En este sentido, te mostraremos las principales amenazas de ciberseguridad a las que debes estar atento para garantizar la seguridad de los datos confidenciales de la empresa.

2.6.1.2 Ataques de phishing

El phishing es uno de los ataques cibernéticos más utilizados por ciberdelincuentes para obtener información confidencial (números de tarjetas de crédito, contraseñas, nombre de usuario, etc) de los usuarios en internet.

En este caso, los atacantes se hacen pasar por una institución verificada (como por ejemplo una entidad bancaria) o personas de confianza y redactan un correo electrónico con lenguaje formal para solicitar al usuario que ingrese en un enlace que será muy parecido al de una página oficial de cualquier empresa o banco legítimo.

Una vez dentro de esta página, se le pedirá al usuario que inicie sesión como lo haría normalmente, ingresando su nombre de usuario y contraseña. El objetivo principal es hacerle creer a los usuarios que es una operación de rutina, para no levantar ningún tipo de sospecha.

Es por ello por lo que las empresas suelen resaltar que nunca solicitarán ningún tipo de información o datos confidenciales por vía telefónica o por correo, para evitar que los usuarios caigan en este tipo de estafas cibernéticas. (Microsoft, s.f.).

2.6.1.3 Ataque de Ransomware

Cuando hablamos de ataque de ransomware o secuestro de datos, nos referimos a un tipo de software malicioso que suele ser utilizado por ciberdelincuentes para robar información confidencial y mantenerla encriptada bajo un código de acceso.

De esta forma, el usuario que ha sufrido el ciberataque no solo ha sido víctima del robo de información, sino que adicionalmente no podrá recuperarla hasta que pague un monto de dinero específico al hacker para que libere dicha información. (Jnguyen, 2023).

2.6.1.4 Malware

Un malware también se corresponde con un software malicioso que tiene como objetivo explotar las vulnerabilidades de un sistema informático para obtener ciertos permisos sin autorización, como, por ejemplo:

A. Ejecutar o desinstalar programas
B. Acceder a funciones del equipo o sistema en el que está instalado
C. Permitir la extracción de información
D. Entre otros.

Este tipo de software es común encontrarlo en los sitios web que nos llenan la ventana de anuncios o cuando instalamos programas cuyo desarrollador es desconocido. (McAfee, 2020).

2.6.1.5 Spam o correo no deseado

El spamming se refiere a la acción de enviar múltiples mensajes no solicitados para promover ciertas campañas de marketing, política o en el caso de las ciber amenazas, para difundir un virus informático o malware.

En estos casos, el objetivo de los ciberdelincuentes es que alguno de los usuarios se atreva a abrir el enlace o descargar el archivo malicioso por curiosidad y, de esta forma, podrá acceder a la información personal que tiene en su equipo.

Esta práctica también se utiliza frecuentemente en redes sociales (Facebook, Twitter, Instagram, Whatsapp), donde los *hackers* envían múltiples mensajes haciendo creer a las personas que ganaron cierta cantidad de dinero o algún producto y que para reclamarlo solo deben hacer clic en un link. (Belcic, 2024).

2.6.1.6 Amenazas internas

Una de las amenazas internas más importantes de la ciberseguridad para las empresas son los hábitos que tienen sus empleados a la hora de ingresar al sistema.

Al ser quienes tienen autorización para acceder a la información de la empresa, cualquier error pequeño que cometan, puede traducirse en una brecha de la seguridad de la información, que será aprovechada por terceros.

También es posible que alguno de los empleados sea el responsable directo de las filtraciones de datos, ya sea de forma involuntaria o no. En este sentido, es importante educar a todos los empleados en seguridad cibernética para minimizar las brechas de seguridad. (RedHat, 2022)

2.6.1.7 Inyección SQL

En este tipo de ciberataque, el hacker se encarga de introducir un código SQL (Lenguaje de Consulta Estructurada) corrupto en una página web, para poder acceder a la información de su base de datos sin necesitar una contraseña.

El lenguaje SQL es utilizado para diseñar y administrar bases de datos y por lo general, para acceder a la información almacenada en ellas, se necesita un usuario y una contraseña específica.

Los ciber atacantes analizan las bases de datos en búsqueda de vulnerabilidades específicas para ingresar comandos especiales que permiten la ejecución de un código SQL que les otorgue acceso al sistema sin autorización.

De esta forma, los ciberdelincuentes pueden tomar el control total de una base de datos utilizando un ataque de inyección SQL, ya sea para extraer información o modificarla sin ser detectado. (Microsoft, 2024).

2.6.1.8 Ataques de denegación de servicios (DDoS)

Para llevar a cabo el ataque DDoS y burlar la seguridad informática de un sistema, los hackers envían múltiples solicitudes a un servidor o red con el objetivo de superar la capacidad de respuesta a dichas solicitudes, cuyo desenlace será el colapso de la red objetivo.

Desde el momento en que la red deja de funcionar, se convierte en un blanco fácil para los ciber atacantes. (INCIBE, 2018).

2.7 Principales ataques realizados a empresas lideres en su sector

Para dimensionar el impacto que generan los ciberdelincuentes y las amenazas que evolucionan día con día tendremos que revisar la siguiente tabla como antecedente de los ataques realizados con mayor relevancia.

Tabla 1. Principales ataques cibernéticos a empresas lideres en su sector. Tomada de (Santillán, s.f.).

Ataque	Descripción
Log4j	Es el nombre que se le dio a una vulnerabilidad que permite que un atacante ejecute un código abierto y tome control de los dispositivos afectados. Este ataque afectó a 5 víctimas en las industrias de finanzas, banca y software en países como Israel, Estados Unidos, Corea del Sur, Suiza y Chipre.
Ataque de servidor Exchange	De acuerdo con el ciber reportero Brian Krebs, al menos 30,000 organizaciones en USA, fueron atacadas por una unidad china de espionaje cibernético que se enfoca en robar correo electrónico de sus víctimas. La unidad explotó cuatro fallas descubiertas en el servidor de correo de Microsoft Exchange Server.
SolarWinds	Es una compañía de software basada en USA, la cual proporciona herramientas para monitoreo de redes e infraestructura y otros servicios. Los ciber-actores lograron tener acceso a las redes, sistemas y datos de miles de clientes de SolarWinds, Más de 30,000 organizaciones públicas y privadas usan sus servicios de esta compañía.

Kaseya	Kaseya sufrió un ataque de Ransomware que afectó a varios de sus clientes. De acuerdo con la compañía de mandiant, unos 60 clientes fueron afectados por este ataque. Sin embargo, estos clientes a su vez prestan sus servicios a otras organizaciones, lo que ocasionó una afectación cerca de 1,500 compañías que prestan sus servicios a usuarios finales.
Colonial Pipeline	Una de las más grande compañías de oleoductos en USA sufrió un ataque de Randsomware. Se dice que Darside es una organización detrás de este ataque. Debido a la amenaza de escasez, cuatro estados de EE.UU. (Carolina del Norte, Virginia, Georgia y Florida) declararon el estado de emergencia. Por primera vez desde 2014, el precio promedio de un galón de gasolina en los EE.UU. aumentó a casi $3. Esto es un ejemplo de cómo la infraestructura de servicios críticos de un país puede ser víctima de un ataque y afectar a todo un país.
Twitch	Esto es un ejemplo de lo que se denomina activismo. De acuerdo con la información disponible, la personas que llevó a cabo este ataque, buscaba dañar a la empresa por no haber tomado medidas contra el odio en internet. El atacante publicó en el sitio web 4chan, unos 125GB de datos de Twitch, entre los cuales estaban el código fuente de la compañía, documentos internos, salarios y otra

	información personal de algunas de las mayores estrellas y operadores de canales de la plataforma.

Nota. Referencia de ataques más relevantes en industrias.

2.8 Informática Forense

La informática forense se refiere a un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias del equipamiento de computación de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo en un juzgado.

La informática es una parte vital en la investigación forense en el ámbito digital, pues está específicamente focalizada en los delitos cometidos mediante dispositivos de computación, como redes, ordenadores y medios de almacenamiento digital, especialmente en aquellos casos que involucran a la tecnología como fuente o víctima de un delito. (Dominguez, 2014).

La informática forense es esencial para:

A. Asegurar la integridad y disponibilidad de la infraestructura de red cuando sucede un incidente de ciberseguridad o ataque informático.
B. Identificar y obtener evidencias de los cibercrímenes de manera apropiada.
C. Asegurar la protección adecuada de los datos y el cumplimiento regulatorio.
D. Proteger a las organizaciones para que no vuelvan a suceder en el futuro los incidentes ocurridos.
E. Ayudar en la protección de crímenes online, como abusos, bullying…
F. Minimizar las pérdidas tangibles o intangibles de las organizaciones o individuos relativas a incidentes de seguridad.
G. Soportar el proceso judicial de enjuiciamiento de los criminales.

Principales ámbitos de aplicación

Como hemos comentado anteriormente la informática forense es de ayuda cuando se producen delitos o incidentes de seguridad de la información que involucran sistemas o tecnologías de la información y las comunicaciones. La mayoría de las organizaciones buscan en la informática forense:

A. Prepararse contra los incidentes de ciberseguridad mediante la securización de sus mecanismos de defensa y subsanar las vulnerabilidades encontradas en ellos.
B. Para asegurar el cumplimiento de las regulaciones y leyes al respecto que le son de aplicación.
C. Reportar los incidentes de seguridad de la información de manera adecuada y detallada.
D. Identificar las acciones necesarias de respuesta ante incidentes.
E. Actuar contra el robo o la utilización ilegal de la propiedad intelectual.
F. Resolver disputas entre los empleados o con ellos.
G. Estimar o minimizar los daños sufridos en un incidente de seguridad.
H. Crear las normas y/o procedimientos de investigación forense.

El perfil de especialista en informática forense

Las funciones de un especialista en informática forense son:

A. Identificar, obtener y preservar las evidencias o pruebas de un cibercrimen.
B. Rastrear y enjuiciar a los culpables.
C. Interpretar, documentar y presentar las evidencias para que sean admisibles judicialmente.
D. Estimar el impacto potencial de la actividad maliciosa para la víctima o los activos.
E. Encontrar vulnerabilidades o brechas de seguridad que ayudan a los atacantes.

F. Entender las técnicas y métodos utilizados por los atacantes para evitar ser cazados.
G. Recuperar archivos borrados, ocultos y datos temporales que pueden utilizarse como evidencias.
H. Realizar la respuesta ante incidentes de seguridad de la información para prevenir la pérdida de información, económica y de reputación.
I. Disponer de conocimiento sobre las leyes de aplicación en diferentes áreas y regiones relativas al crimen digital.
J. Conocer el proceso de manipulación para la investigación forense de múltiples plataformas, tipos de datos y sistemas operativos.
K. Manejar herramientas específicas de investigación forense.

Las fases de la investigación forense en informática son:

A. Pre-investigación

Todas las tareas realizadas de manera previa al inicio de la investigación. Comprende, entre otras, la instalación o preparación del laboratorio forense, la configuración del ordenador de trabajo para la investigación y las herramientas necesarias, la designación del equipo de investigación, la autorización para la investigación, la planificación del proceso a realizar, objetivos, segurizar el perímetro del caso y los dispositivos involucrados.

B. Investigación

Adquisición, preservación y análisis de las evidencias para identificar el origen del crimen o incidente y los culpables. En esta fase hay que poner en juego los conocimientos técnicos necesarios para encontrar las evidencias, examinarlas, documentarlas y preservar los hallazgos. Es crucial asegurar la calidad (inequívocos, claros y exactos) e integridad (no han sido manipulados, se ha asegurado la cadena de custodia) de los hallazgos para que no sean desestimados en el juzgado.

C. Post investigación

Reporte y documentación de todas las acciones llevadas a cabo para la obtención de los hallazgos. El informe debe ser claro, conciso, exacto y, por lo tanto, fácilmente entendible por la audiencia y proveer las evidencias adecuadas.

La informática forense es un proceso clave para rastrear y enjuiciar a los culpables de haber cometido un crimen en el que se vean involucrados dispositivos de computación y también para los incidentes de seguridad de la información. Además, desde un punto de vista de ciberseguridad la informática forense ayuda también en la prevención y respuesta ante ciber incidentes.

2.9 Antecedentes

Los antecedentes de la centralización de registros y la automatización de procesos de reporteo en análisis forense digital se relacionan con la evolución de las tecnologías de seguridad de la información y la necesidad de abordar de manera más eficiente los desafíos asociados con la detección, respuesta y mitigación de incidentes de seguridad cibernética.

Aquí hay algunos hitos clave en este contexto:

1. Desarrollo de Herramientas Forenses:

    - En las últimas décadas, se han desarrollado y perfeccionado herramientas forenses digitales para investigar incidentes de seguridad. Estas herramientas permiten a los analistas recopilar evidencia digital de sistemas y redes.

2. Crecimiento Exponencial de Datos:

    - Con la proliferación de dispositivos conectados y sistemas en red, la cantidad de datos generados ha aumentado exponencialmente. Gestionar y analizar estos datos de manera manual se volvió impracticable, lo que llevó a la necesidad de soluciones de centralización.

3. Aparición de Sistemas SIEM:

    - Los sistemas SIEM (Security Information and Event Management) se convirtieron en una respuesta a la necesidad de centralizar registros. Estos sistemas permiten la recopilación, correlación y análisis de eventos de seguridad desde múltiples fuentes en tiempo real. (Microsoft, s.f.).

4. Regulaciones de Cumplimiento:

    - El aumento de las regulaciones de cumplimiento en el ámbito de la seguridad de la información (por ejemplo, GDPR, HIPAA) ha obligado a las organizaciones a implementar medidas más efectivas para monitorear y proteger sus activos digitales.

5. Complejidad de Amenazas Cibernéticas:

    - La sofisticación de las amenazas cibernéticas, como el malware avanzado y los ataques dirigidos, ha llevado a una mayor conciencia sobre la importancia de la detección temprana y la respuesta rápida.

6. Necesidad de Automatización:

    - La automatización se ha vuelto esencial para lidiar con la velocidad y la complejidad de los ataques cibernéticos. La automatización en el análisis

forense digital ayuda a acelerar la identificación y mitigación de amenazas.

7. Enfoque en Tiempo Real:

    - La necesidad de respuestas en tiempo real ante incidentes de seguridad ha llevado a la adopción de tecnologías que permiten la monitorización continua y la generación automática de alertas.

8. Integración de Tecnologías Emergentes:

    - La integración de tecnologías emergentes como la inteligencia artificial y el aprendizaje automático ha mejorado la capacidad de detección de anomalías y patrones en grandes conjuntos de datos.

9. Centralización en la Nube:

    - Con la adopción generalizada de soluciones en la nube, la centralización de registros también se ha expandido para incluir datos generados en entornos en la nube.

10. Enfoque Holístico de Seguridad:

    - Las organizaciones están adoptando un enfoque holístico de la seguridad, reconociendo la importancia de la integración y centralización de datos para una visibilidad completa de la postura de seguridad.

Estos antecedentes ilustran la evolución de la necesidad de centralización y automatización en el análisis forense digital, destacando la importancia de adaptarse a un entorno de amenazas en constante cambio. La centralización de registros y la

automatización no solo mejoran la eficiencia, sino que también permiten una respuesta más rápida y efectiva a los incidentes de seguridad.

2.10 ISO/IEC 27000

La norma ISO/IEC 27000 proporciona un marco común para la terminología y los conceptos asociados con la gestión de la seguridad de la información (SGSI). Es una norma fundamental que ayuda a entender y aplicar las normas y directrices dentro de la serie ISO/IEC 27000.

La norma define términos clave como seguridad de la información, confidencialidad, integridad, disponibilidad y otros conceptos esenciales. Esto asegura una comprensión uniforme y consistente en toda la organización y entre partes interesadas.

Proporciona una visión general del sistema de gestión de la seguridad de la información (SGSI), incluyendo su propósito, sus beneficios y su estructura general.

Explica el contexto en el que se implementa un SGSI y cómo se interrelaciona con otros sistemas de gestión, como los de calidad (ISO 9001) o medioambientales (ISO 14001). También establece cómo el SGSI debe adaptarse a las necesidades específicas de la organización.

Sirve como una introducción a otras normas de la serie ISO/IEC 27000, como ISO/IEC 27001 (requisitos para el SGSI), ISO/IEC 27002 (prácticas recomendadas) y otras, facilitando su comprensión e implementación.

Presenta la estructura y el propósito de cada norma dentro de la serie ISO/IEC 27000. Esto ayuda a las organizaciones a identificar qué normas son relevantes para sus necesidades específicas.

La norma proporciona un lenguaje común y una base conceptual que ayuda a asegurar que todos los stakeholders tienen una comprensión uniforme de la seguridad de la información.

Al comprender los términos y conceptos básicos, las organizaciones pueden implementar y mantener de manera más efectiva otros estándares en la serie ISO/IEC 27000.

Ofrece una base para la mejora continua al proporcionar una comprensión clara de los conceptos y términos fundamentales relacionados con la gestión de la seguridad de la información.

En resumen, ISO/IEC 27000 actúa como un punto de partida esencial para las organizaciones que desean implementar y mantener un sistema de gestión de seguridad de la información, proporcionando las bases conceptuales necesarias para el éxito en la aplicación de los estándares más detallados de la serie. (ISO, 2022).

CAPÍTULO III. METODOLOGÍA

La centralización de registros y la automatización de procesos de reporteo en análisis forense digital son iniciativas clave para mejorar la eficiencia y la capacidad de respuesta en la investigación de incidentes y la gestión de la seguridad. Aquí hay una metodología general que puedes seguir para llevar a cabo un proyecto de este tipo:

3.1 Enfoque Metodológico

El presente trabajo sigue una metodología cualitativa con un diseño de estudio de caso aplicado al problema de saturación y elevado uso de recursos del firewall Fortinet en la red del TecNM campus Zitácuaro. El objetivo es implementar una solución de monitoreo utilizando tecnologías accesibles como Nagios, syslog y un servidor NAS, todas integradas en una Raspberry Pi 4B.

3.2 Tipo de Estudio

El estudio de caso es el diseño elegido, ya que permite un análisis detallado y profundo de la situación particular de la red del campus, lo que contribuye a generar una comprensión integral de los factores que causan la saturación del firewall y cómo se puede mitigar este problema con una solución de monitoreo de bajo costo.

3.3 Fases del Proyecto

El desarrollo de la solución propuesta se realizó en varias fases:

3.3.1 Fase 1: Diagnóstico de la situación actual

En esta fase se llevó a cabo un análisis del estado actual del firewall Fortinet. Esto incluyó:

A. Revisión de logs y estadísticas de rendimiento del firewall.
B. Identificación de los picos de uso de CPU y memoria.
C. Detección de posibles cuellos de botella y causas de la saturación.

Las herramientas utilizadas para el diagnóstico incluyen las interfaces nativas del firewall Fortinet y la recolección de datos históricos de su desempeño.

3.3.2 Fase 2: Diseño de la solución

Se diseñó una arquitectura de monitoreo basada en:

- Nagios como sistema principal de monitoreo.
- Syslog para la centralización y análisis de logs.
- Servidor NAS como almacenamiento de respaldo.

Todos estos componentes fueron montados sobre una Raspberry Pi 4B por ser una solución de bajo costo y alto rendimiento, ideal para entornos educativos.

3.3.3 Fase 3: Implementación

La implementación se realizó en los siguientes pasos:

1. Instalación y configuración de Nagios: Se configuraron los servicios de monitoreo para supervisar el uso de CPU, memoria y estado de los servicios del firewall.

2. Integración de syslog: Se redirigieron los logs del firewall hacia la Raspberry Pi mediante el protocolo syslog para centralizar su almacenamiento y análisis.

3. Configuración del servidor NAS: Se implementó un servidor NAS en la Raspberry Pi para almacenar los logs y respaldos de configuración del firewall.

4. Pruebas: Se realizaron pruebas de funcionamiento de cada componente y del sistema completo, verificando la correcta recolección de datos y la respuesta ante eventos críticos de saturación.

3.3.4 Fase 4: Validación y análisis de resultados

Para evaluar la efectividad de la solución, se utilizó un método comparativo:

A. Comparación de métricas de rendimiento del firewall antes y después de la implementación del sistema de monitoreo.
B. Análisis de logs recolectados para verificar la reducción de eventos de saturación y picos de uso de recursos.
C. Entrevistas y consultas con el personal de TI del campus para evaluar la satisfacción con la solución.

3.4 Herramientas y Tecnologías

Las herramientas empleadas fueron:

A. Nagios: Para el monitoreo en tiempo real de recursos y servicios.
B. Syslog: Para la centralización de logs.
C. Servidor NAS: Para la gestión de backups y almacenamiento de logs.
D. Raspberry Pi 4B: Como plataforma hardware para el despliegue de la solución.

3.5 Evaluación

El éxito de la solución se evaluará mediante los siguientes indicadores:

A. Disminución de picos de CPU y memoria en el firewall.
B. Mejora en la estabilidad y rendimiento de la red del campus.
C. Capacidad de monitoreo y alertas en tiempo real ante problemas de saturación.
D. Satisfacción del personal de TI con la facilidad de uso y mantenimiento de la solución.

La implementación de un sistema de monitoreo y syslog en una Raspberry Pi es una solución viable y efectiva para gestionar la operatividad y seguridad de redes informáticas, proporcionando a los administradores de sistemas una herramienta poderosa y accesible para supervisar y analizar el rendimiento y eventos de la red en tiempo real.

3.6 Variables

En un proyecto de centralización de registros y automatización de procesos de reporteo en análisis forense digital, varias variables juegan un papel crucial. Estas variables pueden clasificarse en diversas categorías, abarcando desde aspectos técnicos hasta consideraciones organizativas.

A continuación, se enumeran algunas variables clave:

3.6.1 Variables Técnicas

Fuentes de Datos:

- Identificación y selección de las fuentes de datos relevantes, como logs de servidores, registros de firewalls, registros de aplicaciones, etc.

Sistema de Centralización (SIEM):

- Elección del sistema SIEM o plataforma de centralización de registros que mejor se adapte a las necesidades de la organización.

Herramientas Forenses:

- Selección de herramientas forenses digitales para la recolección, análisis y presentación de evidencia digital.

Automatización de Flujos de Trabajo:

- Diseño y desarrollo de flujos de trabajo automatizados para tareas forenses específicas, como la detección de malware o la investigación de incidentes.

Integración de Sistemas:

- Integración efectiva de sistemas de centralización, herramientas forenses y otras soluciones de seguridad existentes.

Seguridad de la Infraestructura:

- Implementación de medidas de seguridad para proteger la infraestructura de análisis forense y la plataforma de centralización contra amenazas internas y externas.

Capacidad de Escalabilidad:

- Diseño de la arquitectura para ser escalable a medida que aumentan los volúmenes de datos y las necesidades de análisis.

3.6.2 Variables Operativas y de Procesos

Procesos Forenses Estándar:

- Establecimiento de procesos estandarizados para la realización de investigaciones forenses, desde la identificación hasta la presentación de informes.

Recursos Humanos:

- Disponibilidad y habilidades del personal de análisis forense, así como su capacidad para adaptarse a nuevos procesos y tecnologías.

Capacitación:

- Programas de capacitación para analistas forenses y personal de seguridad para asegurar la correcta utilización de las herramientas y la comprensión de los flujos de trabajo automatizados.

Gestión de Incidentes:

- Procesos y procedimientos para la gestión efectiva de incidentes, incluyendo la identificación, contención, erradicación y recuperación.

3.6.3 Variables Organizacionales

Cultura de Seguridad:

- La cultura de seguridad organizacional, que puede influir en la adopción y éxito de las iniciativas de análisis forense digital.

Políticas y Normativas:

- Adherencia a políticas internas y regulaciones externas relacionadas con la privacidad, la gestión de datos y la seguridad de la información.

Presupuesto:

- Disponibilidad de recursos financieros para implementar y mantener las soluciones de centralización y automatización.

Colaboración Interdepartamental:

- Grado de colaboración entre departamentos, especialmente entre los equipos de seguridad, TI y cumplimiento normativo.

Evaluación de Riesgos:

- Evaluación continua de riesgos y amenazas para ajustar las estrategias y tácticas de análisis forense.

Cumplimiento:

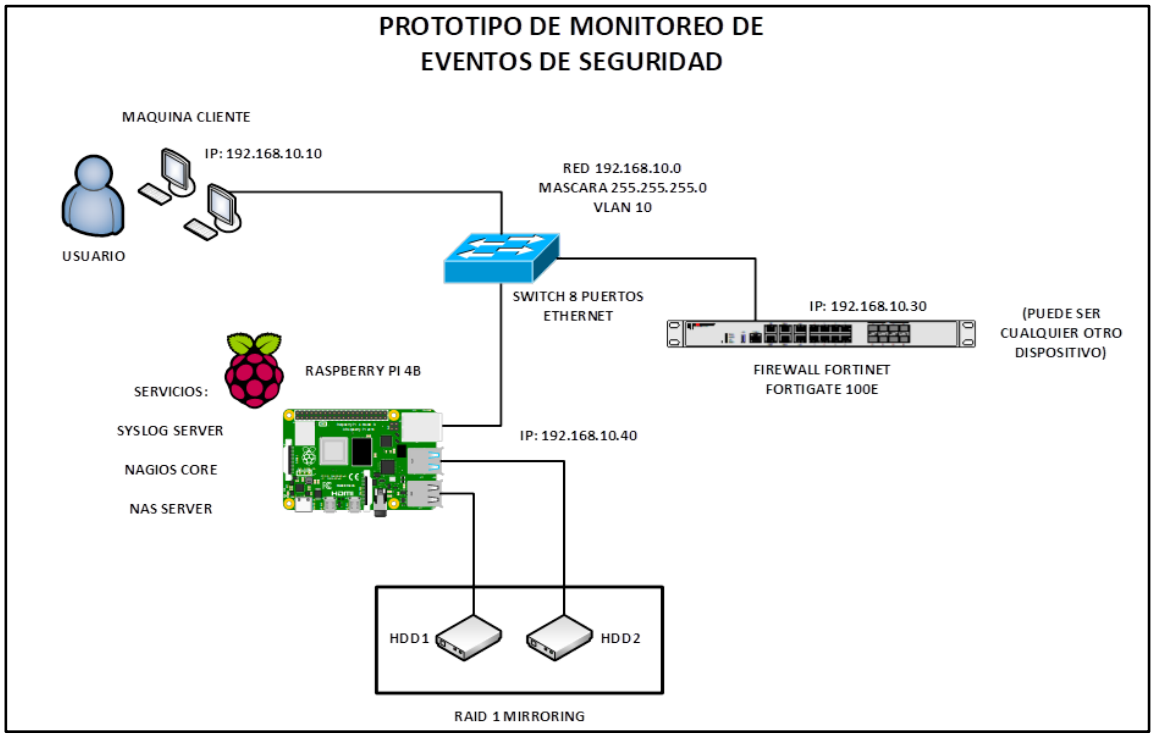
- Adherencia a regulaciones específicas de la industria y normativas gubernamentales en relación con la gestión de incidentes y la privacidad de los datos.

Cada una de ellas afecta directa o indirectamente la eficacia y la eficiencia del sistema implementado.

3.7 Sistema de monitoreo de eventos

El prototipo de monitoreo y detección de eventos fue pensado crearse dentro de un sistema de tarjeta de Raspberry PI 4 con las siguientes características:

Figura 4. Diagrama de red del prototipo Autor: Elaboración propia.



Nota. Arquitectura de prototipo.

Se utilizaron los siguientes componentes para el desarrollo:

- Switch capa 2 (8 puertos cobre)
- Servidor para alojar software prototipo
- Máquina de consulta (endpoint)
- Raspberry PI 4 o superior

- FW Fortinet virtual o físico (es posible considerar cualquier dispositivo compatible)
- Dos discos duros (1TB) RAID 0

La arquitectura descrita ofrece varios beneficios clave para el TecNM Campus Zitácuaro:

Reducción de la carga en el firewall: Al trasladar las tareas de monitoreo y almacenamiento de registros a la Raspberry Pi, se reduce considerablemente el uso de CPU y memoria en el firewall Fortinet, optimizando su rendimiento.

Monitoreo en tiempo real: Nagios proporciona alertas instantáneas cuando se detecta un uso crítico de los recursos del firewall, permitiendo una respuesta rápida ante posibles problemas.

Almacenamiento escalable: La capacidad de conectar discos duros externos a la Raspberry Pi asegura que el sistema pueda escalarse a medida que crece la cantidad de registros generados por el firewall.

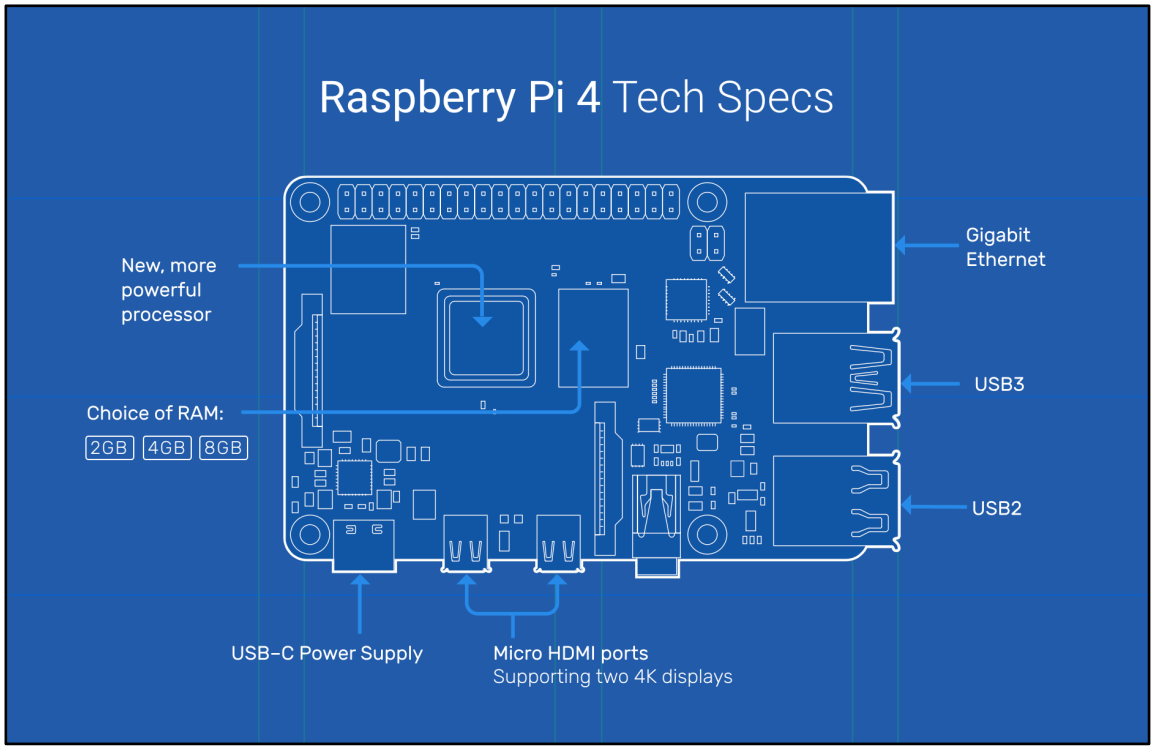
Solución de bajo costo: La utilización de la Raspberry Pi 4B, un dispositivo económico y eficiente, minimiza los costos en comparación con la adquisición de hardware más costoso.

Acceso centralizado a los registros: Syslog y el servidor NAS ofrecen un punto único de acceso a todos los logs generados por el firewall, facilitando su análisis y auditoría.

3.8 Descripción de componentes

3.8.1 Raspberry Pi 4 Modelo B

Figura 5. Raspberry Pi 4B (mapa de puertos). Tomado de: (Raspberry Pi, 2024).



Nota. Diagrama de arquitectura de tarjeta Raspberry PI.

- Broadcom BCM2711, SoC de cuatro núcleos Cortex-A72 (ARM v8) de 64 bits a 1.8GHz
- 4GB SDRAM LPDDR4-3200
- Red inalámbrica IEEE 802.11ac de 2.4 GHz y 5.0 GHz, Bluetooth 5.0, BLE Ethernet Gigabit
- 2 puertos USB 3.0; 2 puertos USB 2.0
- Encabezado GPIO estándar de 40 pines de Raspberry Pi (totalmente compatible con las placas anteriores)
- 2 puertos micro-HDMI® (hasta 4kp60 soportado)
- Puerto de pantalla MIPI DSI de 2 carriles
- Puerto de cámara MIPI CSI de 2 carriles
- Puerto de audio estéreo de 4 polos y video compuesto

- H.265 (decodificación 4kp60), H264 (decodificación 1080p60, codificación 1080p30)
- OpenGL ES 3.1, Vulkan 1.0
- Ranura para tarjeta Micro-SD para cargar el sistema operativo y almacenamiento de datos
- 5V DC a través del conector USB-C (mínimo 3ª*)
- 5V DC a través del encabezado GPIO (mínimo 3ª*)
- Compatible con Power over Ethernet (PoE) (requiere un HAT PoE separado)
- Temperatura de funcionamiento: 0 – 50 grados C ambiente

3.8.2 Switch 8 puertos Ethernet

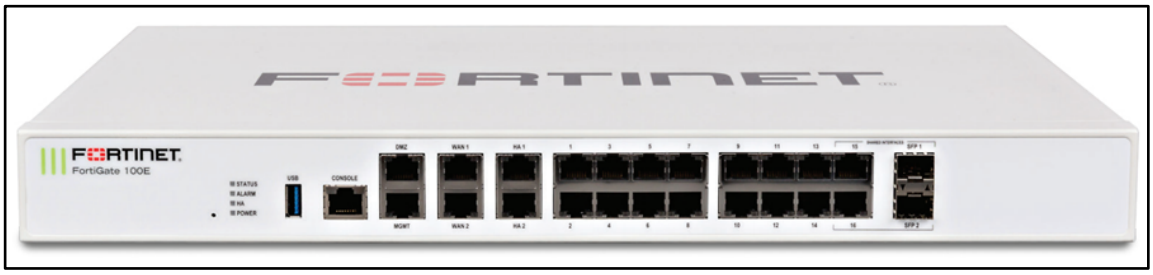
Figura 6. Switch 8 puertos Ethernet. Tomado de (TP- Link, s.f.).

Nota. Imagen visual de switch en puerto Ethernet.

- 8 puertos RJ45 de negociación automática a 10/100/1000 Mbps

3.8.3 Firewall Fortinet Fortigate 100E

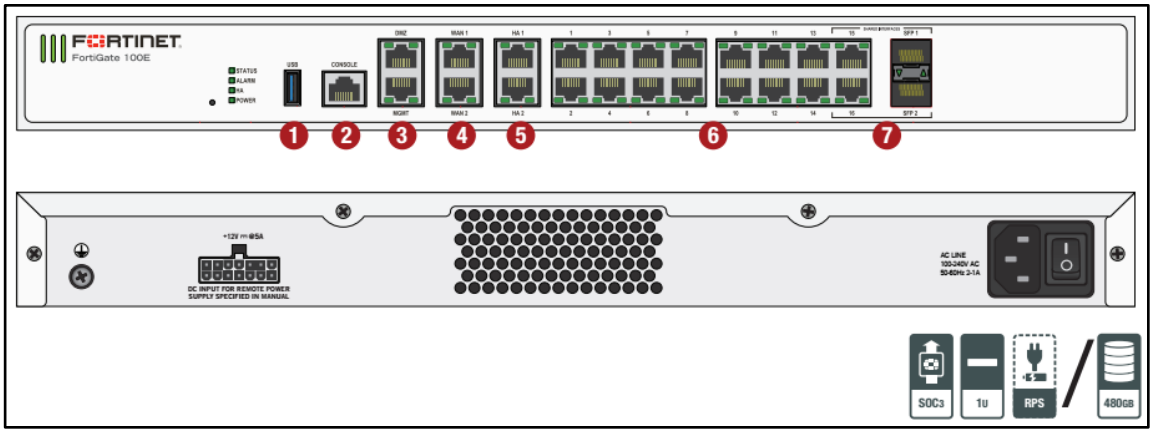
Figura 7. Fortinet Fortigate 100E. Tomado de (Fortinet, 2024).



Nota. Chassis de firewall Fortinet (Front).

Las características de hardware que tiene el equipo Fortinet Fortigate 100E, mostrado con el siguiente esténcil:

Figura 8. Fortinet Fortigate 100E Mapa de puertos Tomada de (Fortinet, s.f.).



Nota. Stencil (back & front) de equipo FW Fortinet.

Interfaces

- Puerto USB
- Puerto de consola
- 2x Puertos GE RJ45 MGMT/DMZ

- 2x Puertos GE RJ45 WAN
- 2x Puertos GE RJ45 HA
- 14x Puertos GE RJ45
- 2x Pares de medios compartidos GE RJ45/SFP

3.8.4 RAID (Redundant Array Of Independent Disks)

Los arreglos de discos, también conocidos como RAID (Redundant Array of Independent Disks), son una tecnología que permite combinar múltiples discos duros en una sola unidad lógica para mejorar el rendimiento, la redundancia, o ambas. Aquí una descripción de los tipos más comunes de arreglos de discos. (Curti, Podesta, Constanzo, Iturriaga, & Castellote, 2015).

RAID 0 (Striping)

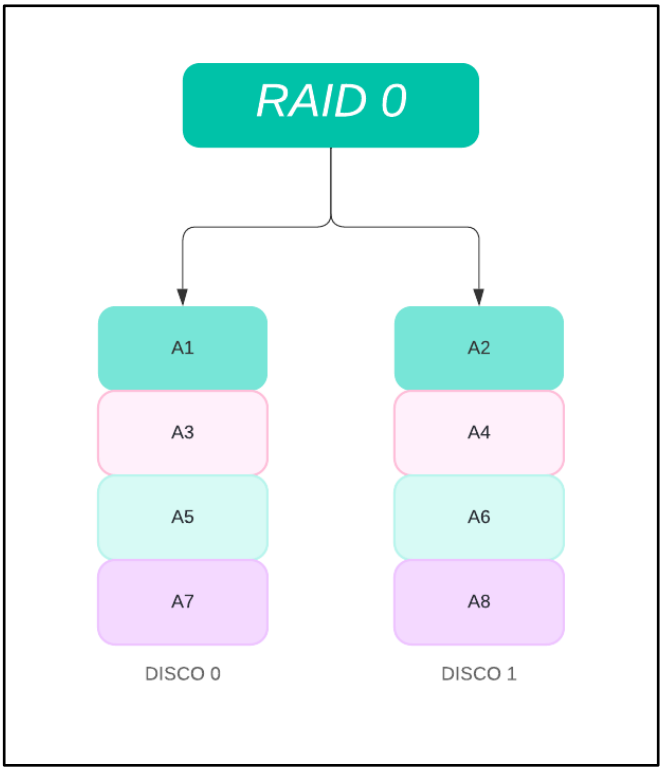
Descripción: Los datos se dividen en bloques y se distribuyen (striped) a través de varios discos.

Ventajas: Mejora significativa del rendimiento debido a que las operaciones de lectura/escritura se realizan en paralelo.

Desventajas: No ofrece redundancia. Si un solo disco falla, se pierde toda la información.

Aplicaciones: Ideal para aplicaciones que requieren alta velocidad de lectura/escritura, pero no es adecuado para datos críticos.

Figura 9. Esquema de arreglo RAID 0 Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 0 con colores por sectores.

RAID 1 (Mirroring) Opción utilizada

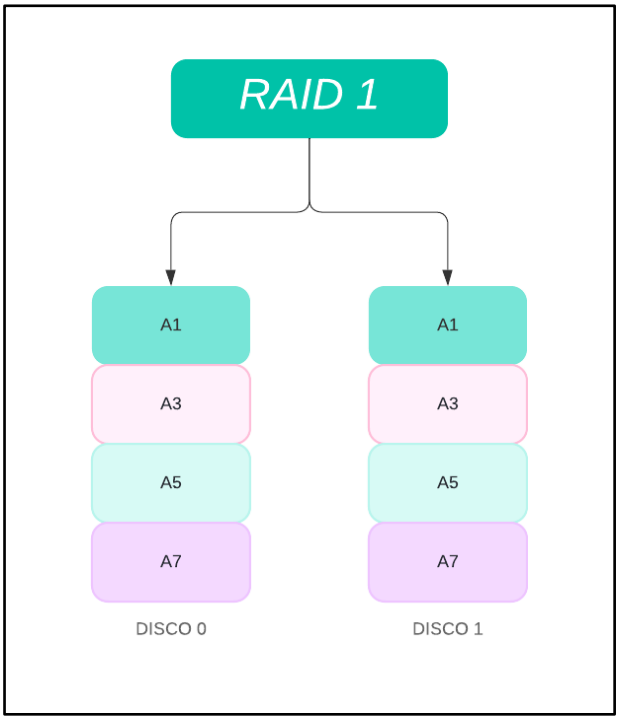
Descripción: Los datos se duplican (mirror) en dos discos. Cada disco contiene una copia exacta de los datos.

Ventajas: Alta redundancia. Si un disco falla, los datos aún están disponibles en el otro disco.

Desventajas: El costo de almacenamiento se duplica, ya que se necesita el doble de capacidad para almacenar los datos.

Aplicaciones: Adecuado para datos críticos donde la redundancia es esencial, como en sistemas operativos y bases de datos.

Figura 10. Esquema de arreglo RAID 1 Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 1 con colores por sectores.

RAID 5 (Striping con Paridad)

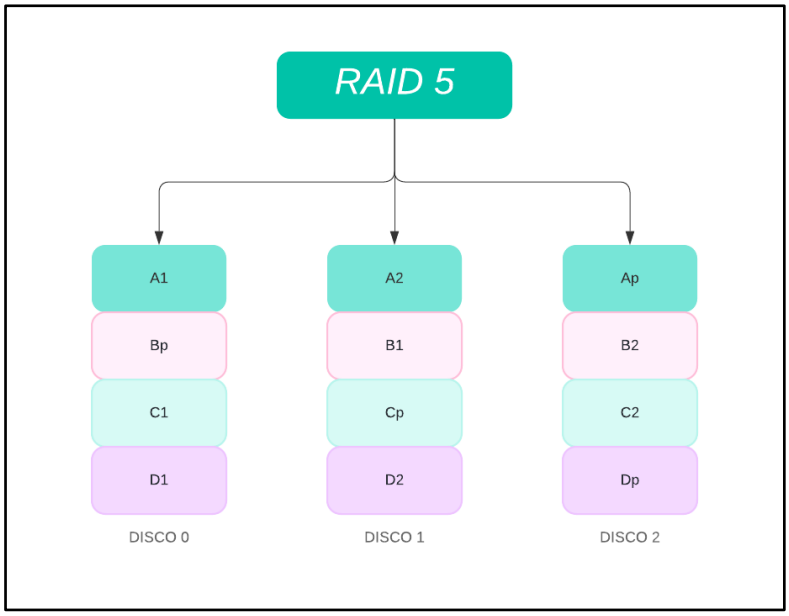
Descripción: Los datos y la información de paridad se distribuyen (striped) entre tres o más discos. La paridad permite la reconstrucción de datos en caso de fallo de un disco.

Ventajas: Ofrece un buen equilibrio entre rendimiento, capacidad de almacenamiento y redundancia. Puede tolerar el fallo de un disco sin pérdida de datos.

Desventajas: El rendimiento de escritura es menor debido a la sobrecarga de cálculo de la paridad. La reconstrucción de un disco fallido puede ser lenta.

Aplicaciones: Utilizado en sistemas donde el equilibrio entre rendimiento, capacidad y redundancia es importante, como en servidores de archivos y sistemas de almacenamiento de datos.

Figura 11. Esquema de arreglo RAID 5 Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 5 con colores por sectores.

RAID 6 (Striping con Doble Paridad)

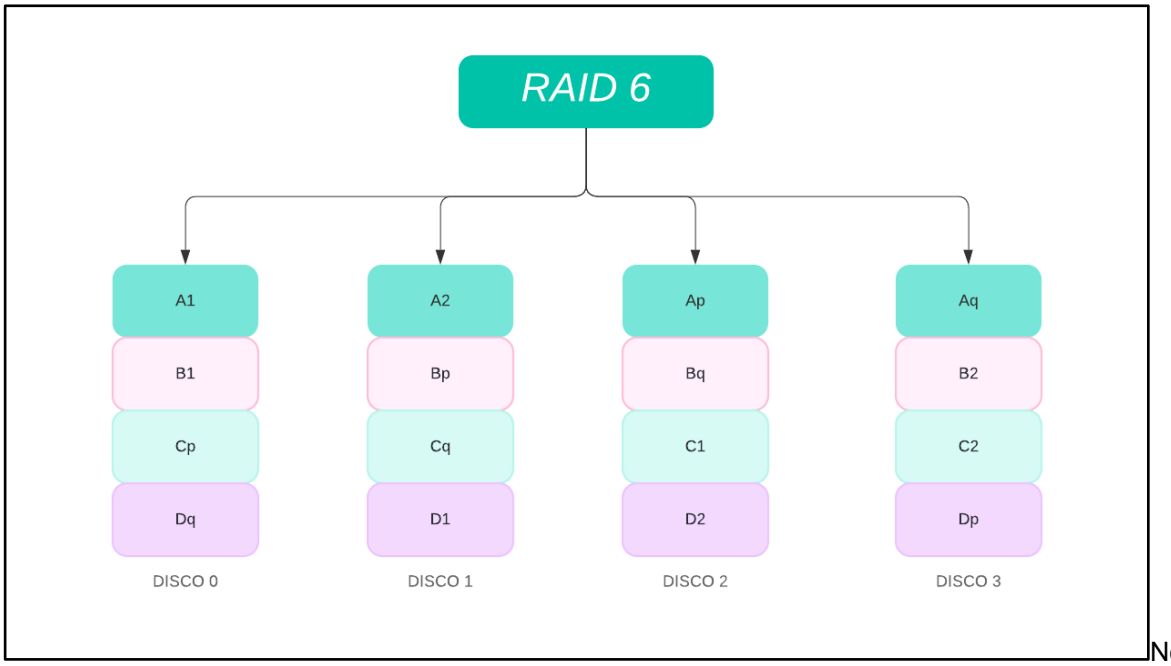
Descripción: Similar a RAID 5, pero con una segunda capa de paridad. Los datos y dos conjuntos de información de paridad se distribuyen entre cuatro o más discos.

Ventajas: Mayor tolerancia a fallos que RAID 5. Puede tolerar el fallo de dos discos simultáneamente.

Desventajas: Menor rendimiento de escritura comparado con RAID 5 debido a la sobrecarga de cálculo de la segunda paridad. La reconstrucción de discos fallidos es más lenta.

Aplicaciones: Utilizado en sistemas críticos donde la tolerancia a fallos es una prioridad, como en grandes sistemas de almacenamiento empresarial.

Figura 12. Esquema de arreglo RAID 6 Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 6 con colores por sectores.

RAID 10 (1+0) (Mirroring y Striping)

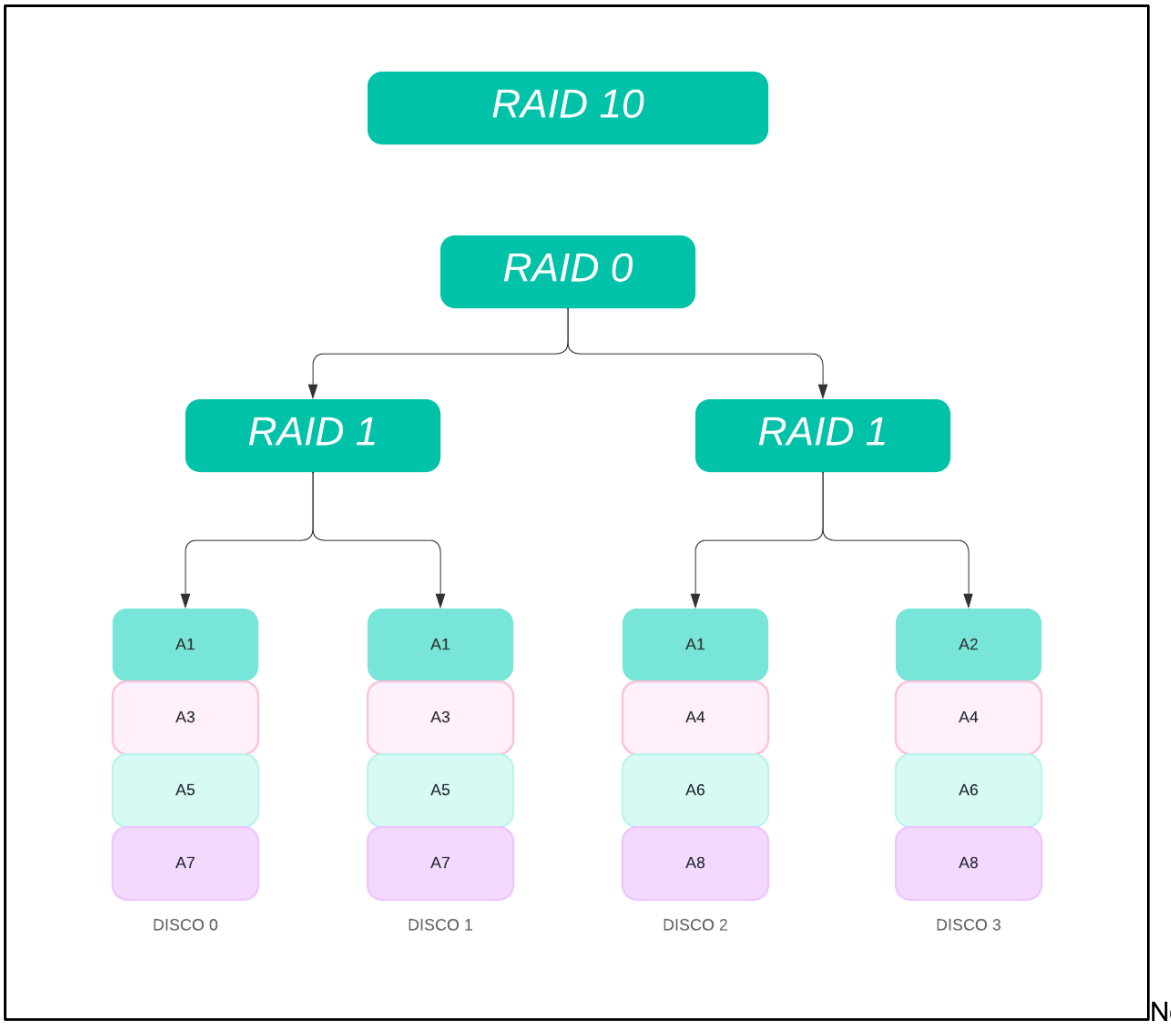
Descripción: Combina las características de RAID 1 y RAID 0. Los datos se dividen y se duplican en pares de discos.

Ventajas: Ofrece alta redundancia y rendimiento. Puede tolerar múltiples fallos de discos siempre que no afecten al mismo par de espejos.

Desventajas: Requiere al menos cuatro discos y el costo de almacenamiento es elevado debido a la duplicación de datos.

Aplicaciones: Ideal para aplicaciones que requieren alta disponibilidad y rendimiento, como bases de datos críticas y servidores de aplicaciones.

Figura 13. Esquema de arreglo RAID 10 Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 10 con colores por sectores.

RAID 50 (5+0) (Striping con Paridad y Striping)

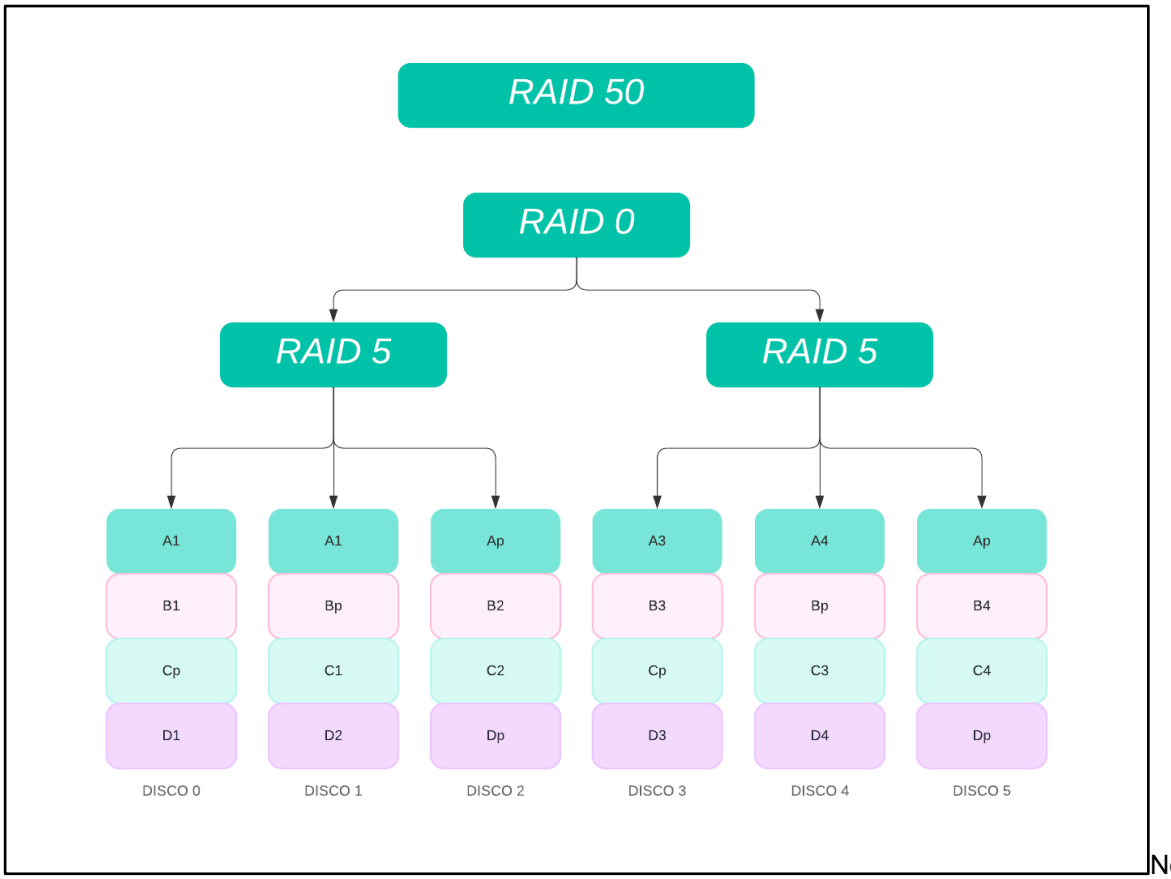
Descripción: Combina RAID 5 y RAID 0. Los datos se distribuyen con paridad en varios conjuntos RAID 5, y esos conjuntos se dividen (striped) en varios discos.

Ventajas: Combina la tolerancia a fallos de RAID 5 con el rendimiento mejorado de RAID 0.

Desventajas: La complejidad y el costo de implementación son mayores que en RAID 5 o RAID 0 solos.

Aplicaciones: Adecuado para aplicaciones que requieren alta capacidad, buen rendimiento y redundancia, como grandes bases de datos y servidores de aplicaciones.

Figura 14. Esquema de arreglo RAID 50 Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 50 con colores por sectores.

RAID 60 (6+0) (Striping con Doble Paridad y Striping)

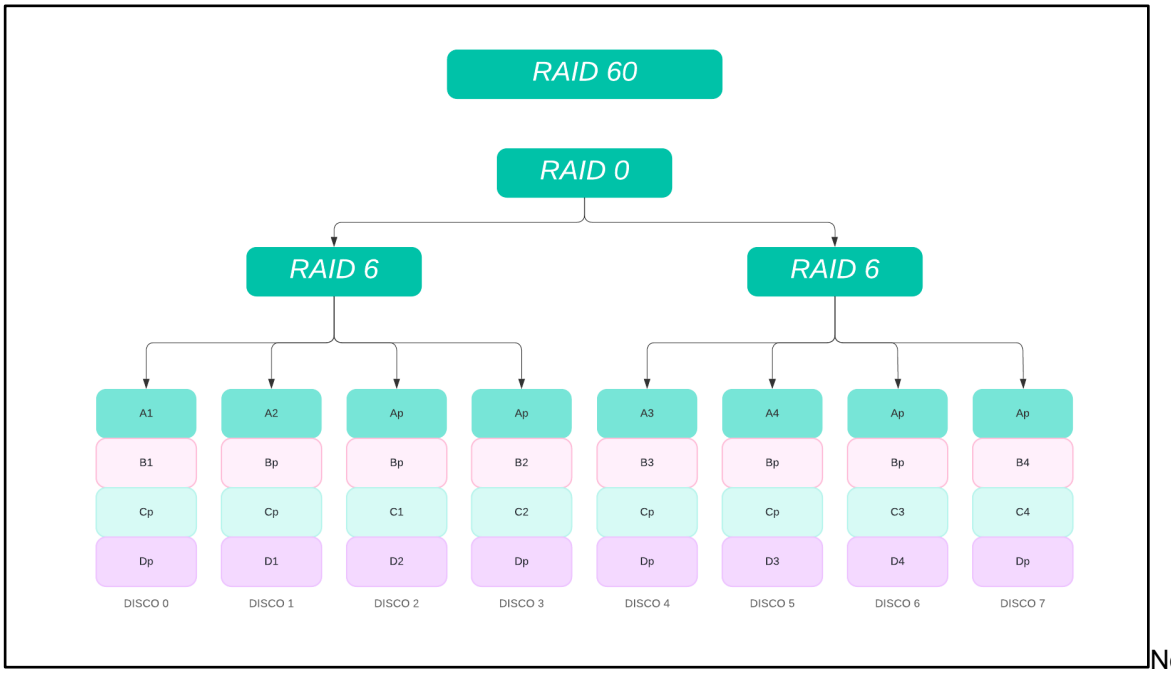
Descripción: Combina RAID 6 y RAID 0. Los datos se distribuyen con doble paridad en varios conjuntos RAID 6, y esos conjuntos se dividen (striped) en varios discos.

Ventajas: Ofrece la mayor tolerancia a fallos combinada con un rendimiento mejorado.

Desventajas: Alta complejidad y costo de implementación. La reconstrucción de discos fallidos es más lenta.

Aplicaciones: Utilizado en grandes sistemas empresariales donde la tolerancia a fallos y el rendimiento son críticos.

Figura 15. Esquema de arreglo RAID 60. Autor: Elaboración propia.



Nota. Diagrama explicativo del funcionamiento de RAID 60 con colores por sectores.

Estos son los tipos más comunes de arreglos de discos RAID, cada uno con sus ventajas y desventajas específicas, adecuándose a diferentes necesidades y aplicaciones en entornos de almacenamiento.

3.9 Implementación de NAGIOS

Paso 1: Actualización de sistema:

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

Paso 2: Instalar dependencias necesarias:

```
sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2
apache2 utils php libgd-dev
```

```
sudo apt-get install openssl libssl-dev
```

Paso 3: Descarga de paquete:

```
cd /tmp
```

```
wget -O nagioscore.tar.gz
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-
4.4.14.tar.gz
```

```
tar xzf nagioscore.tar.gz
```

Paso 4: Compilación:

```
cd /tmp/nagioscore-nagios-4.4.14/
```

```
./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

```
make all
```

Paso 5: Creación de usuarios y grupos de monitoreo:

```
make install-groups-users
```

```
usermod -a -G nagios www-data
```

Paso 6: Instalar Binarios:

```
make install
```

Paso 7: Instalar servicio o demonio:

```
make install-daemoninit
```

Paso 8: Instalar el modo comando

```
make install-commandmode
```

Paso 9: Instalar los archivos de configuración:

```
make install-config
```

Paso 10: Instalar archivos de configuración de servicio Apache

```
make install-webconf
```

```
a2enmod rewrite
```

```
a2enmod cgi
```

Paso 11: Configuración de Firewall (IP Tables):

Es necesario realizar la configuración del FW de Linux para poder aceptar tráfico proveniente del puesto 80 TCP (default de apache) y se pueda visualizar la interfaz web de Nagios Core.

```
iptables -I INPUT -p tcp --destination-port 80 -j ACCEPT
```

```
apt-get install -y iptables-persistent
```

Paso 12: Creación de cuenta de usuario (nagiosadmin)

Necesitamos crear una cuanta de usuario de apache para poder realizar login dentro de Nagios.

El siguiente comando crea la cuenta de usuario llamado nagiosadmin y en automático solicitara la contraseña de la cuenta:

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Importante: cuando sean agregados usuarios adicionales, se deberá eliminar -c del comando anterior; de lo contrario, se reemplazará al usuario nagiosadmin existente.

Paso 13: Iniciar el servidor WEB de Apache

```
systemctl restart apache2.service
```

Paso 14: Iniciar el servicio de Nagios Core

```
systemctl start nagios.service
```

Paso 15: Probar el servicio de Nagios

En este punto el servicio de Nagios está corriendo, para confirmarlo necesitamos realizar el primer inicio de sesión dentro de la interfaz Web.

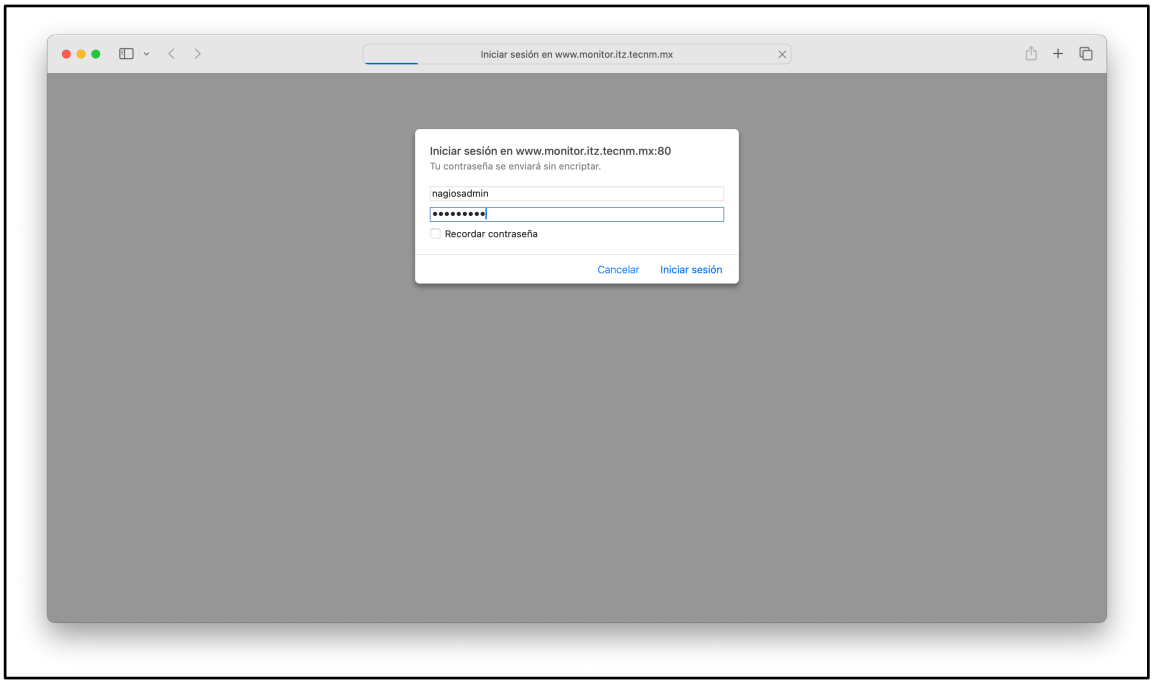
Necesitamos entrar en un navegador Web (Edge, Chrome, Firefox), apuntando a la dirección IP de nuestro servidor de Nagios Core o al FQDN creado para acceder, por ejemplo:

```
http://192.168.1.100/nagios
```

```
http://www.nagios.local/nagios
```

En este caso, el FQDN es http://www.monitor.itz.tecnm.mx/nagios/

Figura 16. Página de inicio de sesión de Nagios Core Autor: Elaboración propia.



Nota. Imagen de pantalla de log in para el sistema Nagios Core.

Necesitamos ingresar el nombre de usuario ‘nagiosadmin’ y la contraseña creados en el paso 12, una vez que podemos ingresar estamos corroborando el correcto funcionamiento del sistema.

Paso 16: Instalación de Nagios Plugins

Nagios Core necesita la instalación de complementos para su correcto funcionamiento, para este caso instalaremos la versión 2.4.6.

Necesitamos asegurarnos de que el paquete de monitores de SNMP está instalado con el siguiente comando:

```
apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev
wget bc gawk dc build-essential snmp libnet-snmp-perl gettext
```

Paso 17: Descargamos el paquete de complementos

```
cd /tmp
```

```
wget --no-check-certificate -O nagios-plugins.tar.gz
https://github.com/nagios-plugins/nagios-plugins/archive/release-
2.4.6.tar.gz
```

```
tar zxf nagios-plugins.tar.gz
```

Paso 18: Compilar e instalar

```
cd /tmp/nagios-plugins-release-2.4.6/
```

```
./tools/setup
```

```
./configure
```

```
make
```

```
make install
```

Paso 19: Reinicio de servicios/demonios

```
systemctl start nagios.service
```

```
systemctl stop nagios.service
```

```
systemctl restart nagios.service
```

```
systemctl status nagios.service
```

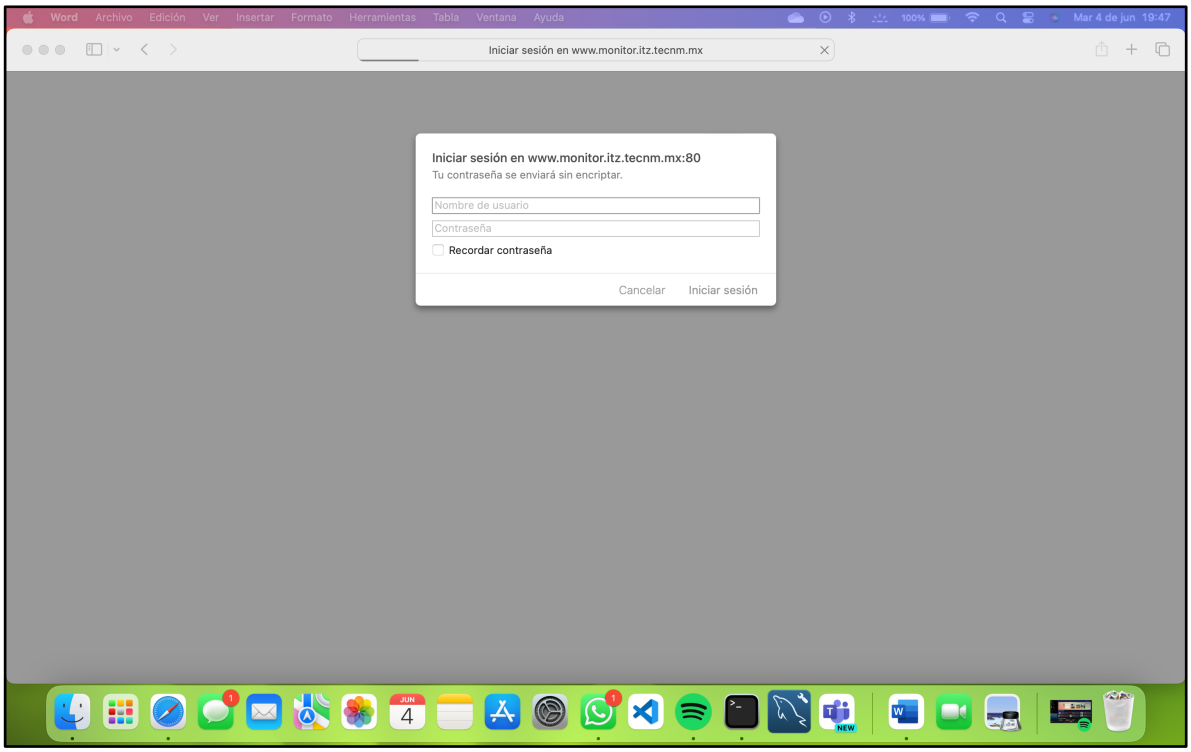
con lo anterior confirmamos el correcto funcionamiento e instalación de software Nagios Core dentro de la Raspberry PI con el sistema de Raspbian OS. (Nagios Core, 2024).

3.10 Configuración de prototipo de monitoreo

Se podrá acceder desde la red local apuntando un registro de DNS a la IP otorgada al servidor donde estará alojada nuestra aplicación WEB, como se muestra a continuación:

Dentro del navegador de uso cotidiano ingresaremos al siguiente enlace: `http://www.monitor.itz.tecnm.mx/nagios`

Figura 17. Dashboard de inicio de sesión de Nagios Core apuntando por el registro de DNS (Ver Anexo I) Autor: Elaboración propia.

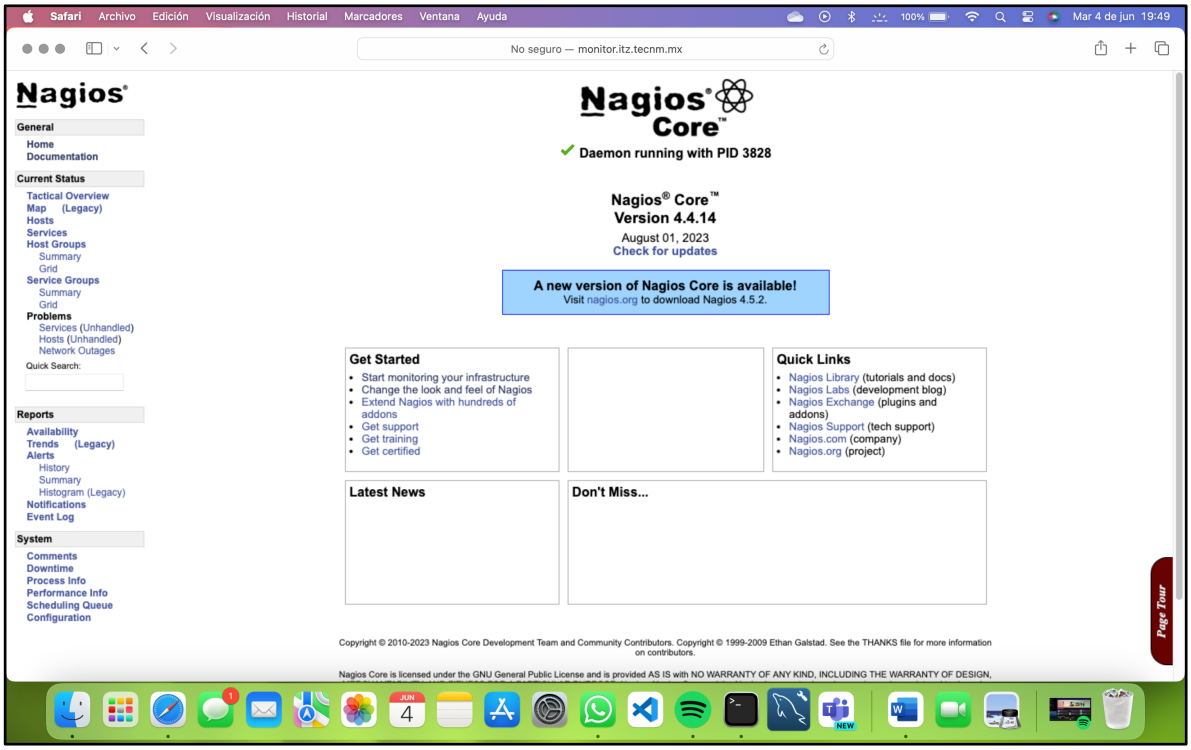


Nota. Log in para el sistema Nagios Core.

Dentro de la aplicación es posible tener un menú del lado izquierdo para obtención de reportes y consultas a los dispositivos supervisados por la herramienta.

Imagen donde se muestra la versión y pantalla inicial de la aplicación Nagios Core

Figura 18. Pantalla de bienvenida Nagios Core Autor: Elaboración propia.



Nota. Imagen de acceso directo a características de la herramienta.

Pantalla de alertas recientes

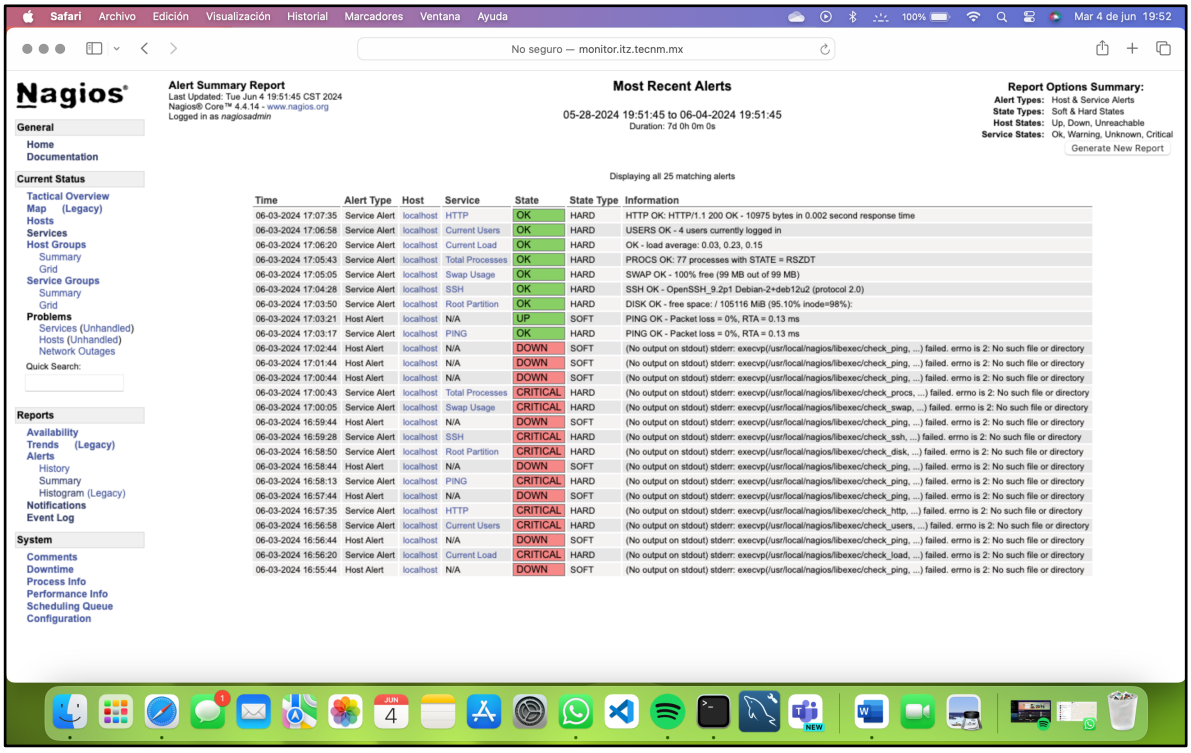
Se muestran los eventos generados de los hosts en nuestro monitoreo con el esquema de colores en semáforo

Tabla 2. Semáforo de alertas de monitoreo. Autor: Elaboración propia.

Rojo	DOWN - CRITICAL
Amarillo	WARNING
Verde	OK - UP
Naranja	UNKNOWN

Nota. Tabla de colores en modo semáforo.

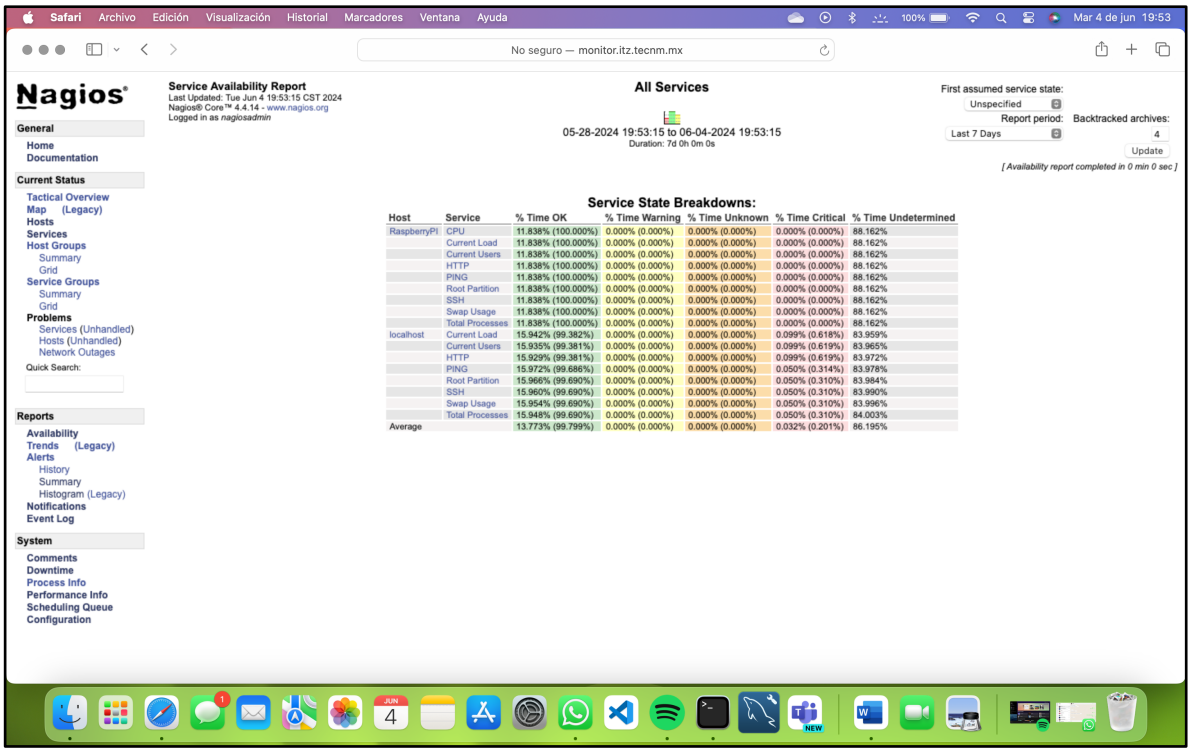
Figura 19. Pantalla de bienvenida Nagios Core. Autor: Elaboración propia.



Nota. Imagen de acceso directo a características de la herramienta.

Pantalla de porcentajes de disponibilidad de dispositivos monitoreados por servicio, se muestran en forma de lista con base al semáforo de colores.

Figura 20. Pantalla de porcentajes de disponibilidad. Autor: Elaboración propia.

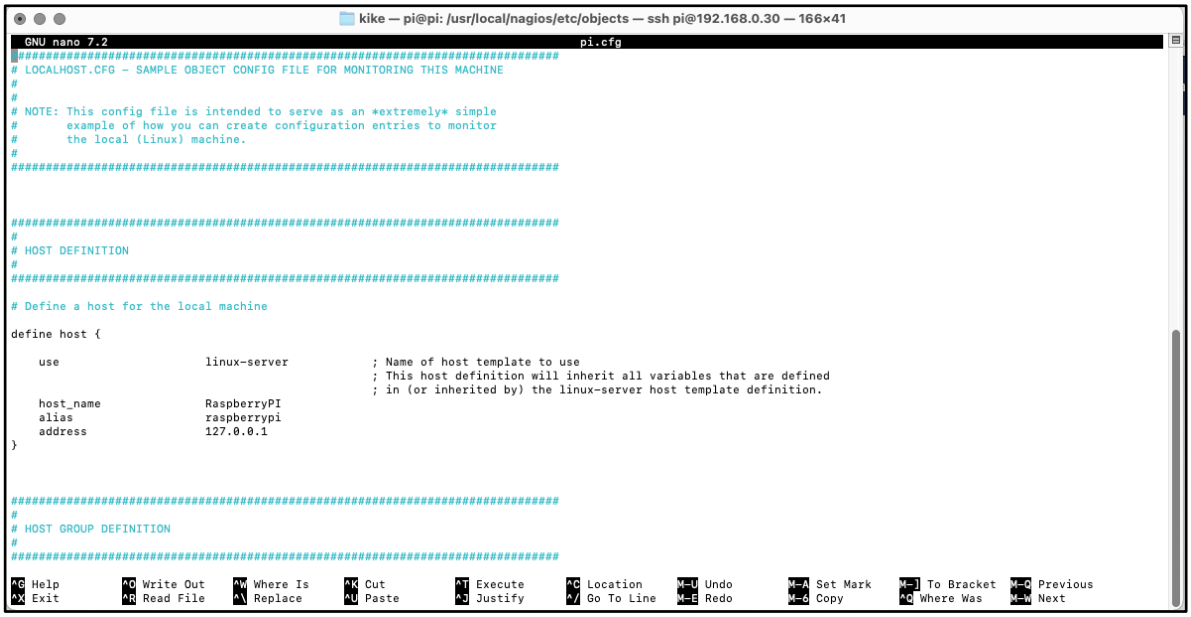


Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
RaspberryPI	CPU	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	Current Load	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	Current Users	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	HTTP	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	PING	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	Root Partition	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	SSH	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	Swap Usage	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
	Total Processes	11.838% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	88.162%
localhost	Current Load	15.942% (99.382%)	0.000% (0.000%)	0.000% (0.000%)	0.099% (0.618%)	83.959%
	Current Users	15.935% (99.381%)	0.000% (0.000%)	0.000% (0.000%)	0.099% (0.619%)	83.965%
	HTTP	15.929% (99.381%)	0.000% (0.000%)	0.000% (0.000%)	0.099% (0.619%)	83.972%
	PING	15.972% (99.686%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.314%)	83.978%
	Root Partition	15.966% (99.690%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.310%)	83.984%
	SSH	15.960% (99.690%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.310%)	83.990%
	Swap Usage	15.954% (99.690%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.310%)	83.996%
	Total Processes	15.948% (99.690%)	0.000% (0.000%)	0.000% (0.000%)	0.050% (0.310%)	84.003%
Average		13.773% (99.799%)	0.000% (0.000%)	0.000% (0.000%)	0.032% (0.201%)	86.195%

Nota. Imagen de servidores monitoreados con porcentajes de disponibilidad.

Alta de nuevo servicio, se tiene que realizar mediante CLI en la ruta `/usr/local/nagios/etc/objects`

Figura 21. SSH – Edición de archivo de servicios. Autor: Elaboración propia.

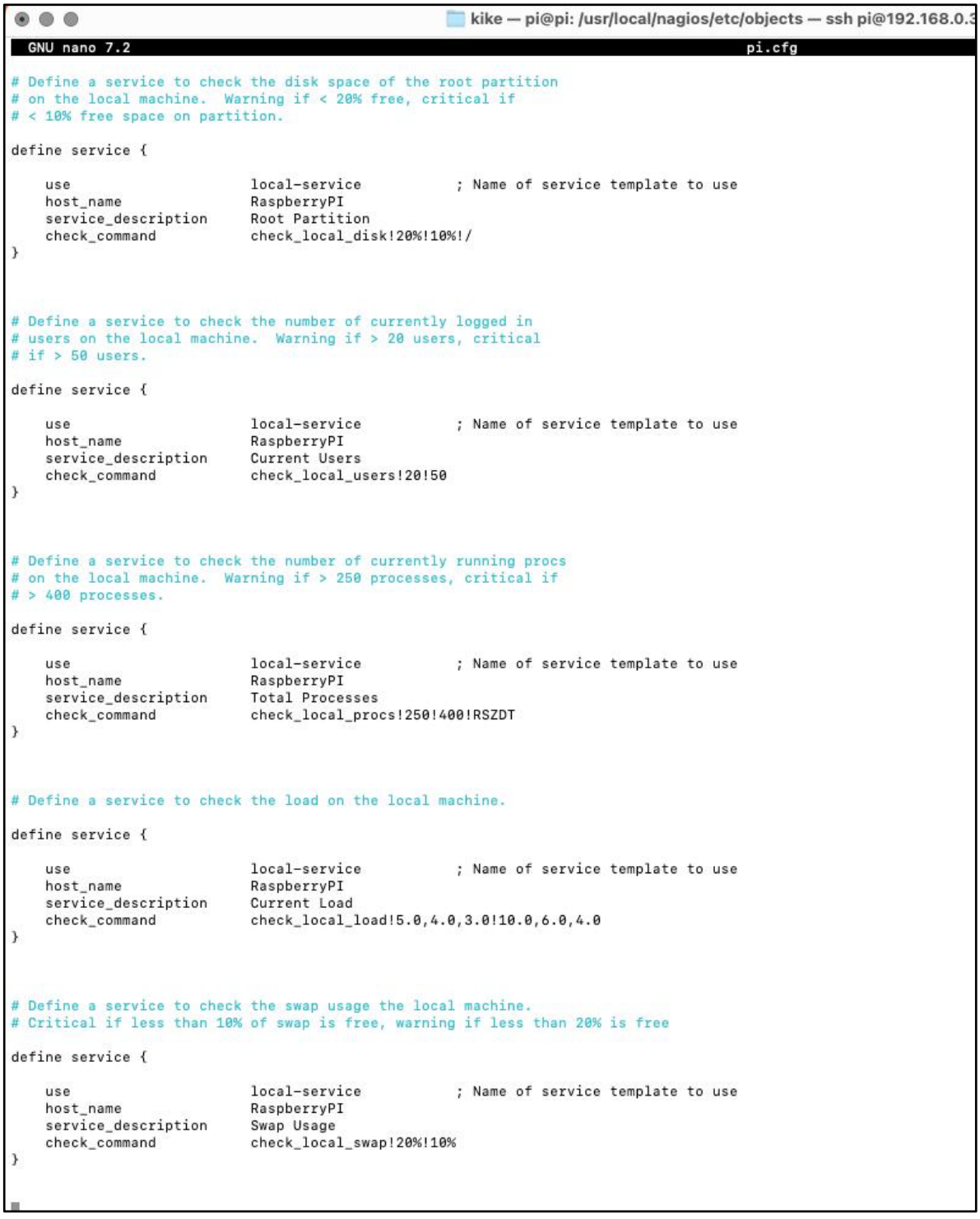


Nota. Definición de servidores a monitorear con tipo de Sistema operativo, dirección IP del dispositivo y grupos a los que pertenece.

Pantalla de nuevos servicios a dar de alta en nuestro host monitoreado, desde CLI entrando al Path: `/usr/local/nagios/etc/objects.`

se edita el archivo objetivo de la configuración del dispositivo objetivo este caso pi.cfg

Figura 22. SSH – Edición del archivo pi.cfg. Autor: Elaboración propia.

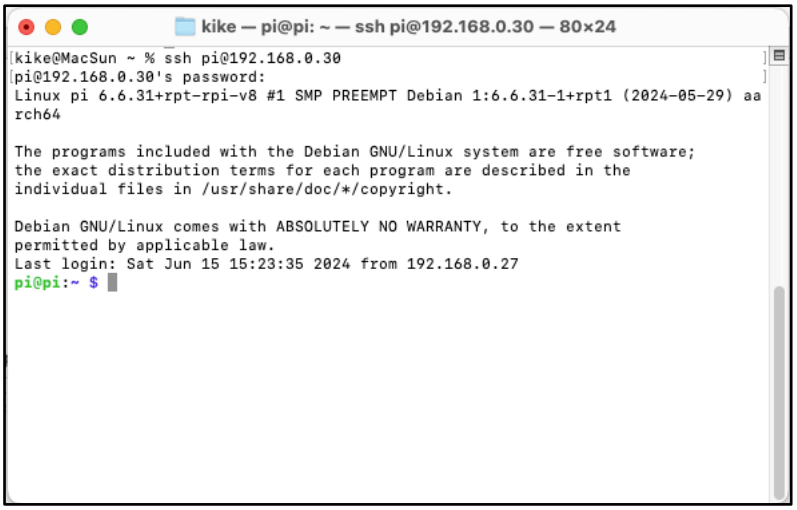


Nota. Definición de servicios a monitorear con comandos a ejecutarse. Elaboración propia.

Acceso por SSH:

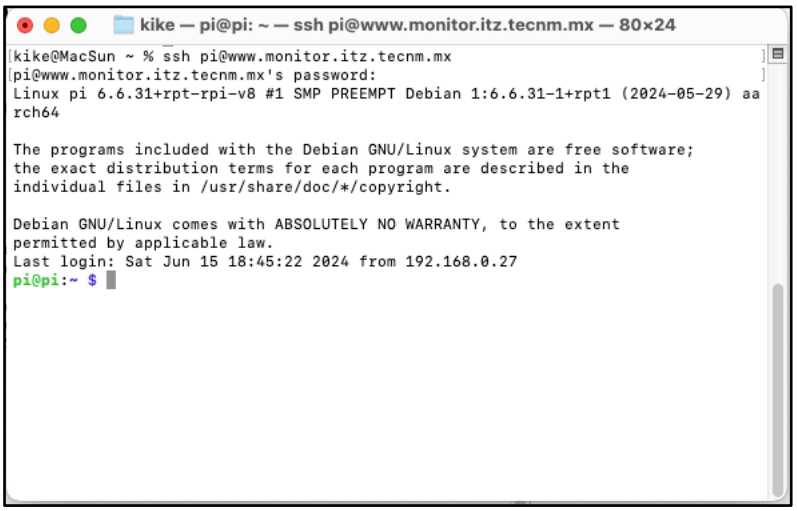
Se debe abrir un terminal apuntando a la dirección IP de nuestro servidor de monitoreo o al nombre registrado en nuestro DNS local para poder acceder por el puerto SSH 22.

Figura 23. Acceso por SSH mediante IP (Revisar Anexo I). Autor: Elaboración propia.



Nota. Log in por puerto 22 SSH por IP.

Figura 24. Acceso por SSH mediante registro de DNS (Revisar anexo I). Autor: Elaboración propia.



Nota. Log in por puerto 22 SSH por registro de DNS.

3.11 Implementación de Syslog

Paso 1: Verificar que los paquetes de la Raspberry PI están actualizados:

```
sudo apt-get update
```

Paso 2: instalar el servicio de syslog:

```
sudo apt-get install syslog-ng
```

Paso 3: Una vez que el servicio de syslog está instalado, nos movemos a /etc/syslog-ng, con el siguiente comando:

```
cd /etc/syslog-ng
```

Paso 4: Se recomienda realizar una copia de seguridad al archivo de configuración de syslog, asegurando en caso de algún fallo poder recuperar la configuración sin ningún contratiempo, proceso con el siguiente comando:

```
sudo cp syslog-ng.conf syslog-ng_original_conf
```

Paso 5: Abrir el archive de configuración de syslog en modo edición:

```
sudo nano syslog-ng.conf
```

Paso 6: el archivo de configuración de syslog de inicio parece un poco complejo de comprender, el archivo de syslog se compone de 4 secciones:

- sources
- destinations
- filters
- log paths

Importante: el carácter especial # es utilizado al principio de cada línea para poder omitir (comentar) la ejecución de una línea de código.

Paso 7: Se realiza la configuración de orígenes para poder aceptar el tráfico proveniente desde cualquier punto de la red por el puerto 514 UDP.

Sources

```
source s_net { udp(ip(0.0.0.0) port(514)); };
```

Paso 8: En el apartado de destinos, se le indica al sistema enviar todos los eventos relacionados del objeto creado d_Raspberry al archivo pi.log

Destinations

```
destination d_Raspberry { file("/var/log/pi.log"); };
```

Paso 9: aquí indicamos dentro de la configuración que los eventos provenientes del source s_net creado en el punto 8 se envíen al objeto d_Raspberry creado en el punto anterior.

Log Path

```
log { source(s_net); destination(d_Raspberry); };
```

Paso 10: Reinicio del demonio syslog con el siguiente comando:

```
sudo service syslog-ng restart
```

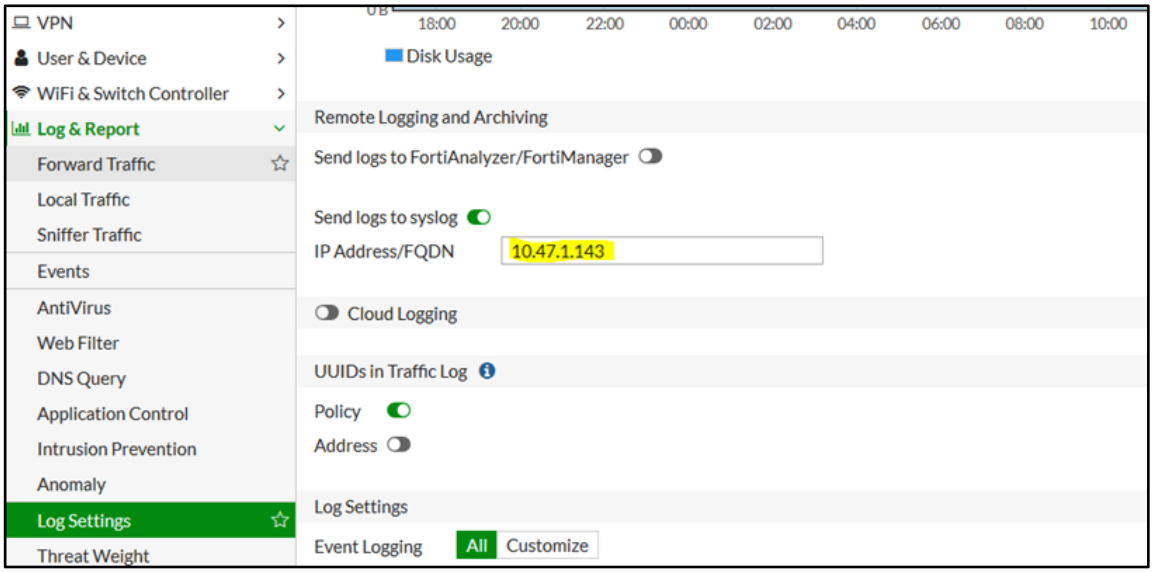
Paso 11: dentro de nuestro equipo objetivo de envió de eventos de syslog únicamente tenemos que apuntar a la IP del Syslog Server (Raspberry PI) para concluir la configuración.

Ejemplo de cómo realizarla en equipo Fortinet:

- Movernos a la parte de Log & Report > Log Setting.
- Click en el checkbox de send logs to syslog
- Agregar la IP de nuestro syslog (Raspberry PI)
- Completar la configuración

- Guardar la configuración para finalizar

Figura 25. Parámetros de configuración en Fortinet para syslog events. Tomada de (Fortinet, s.f.).



Nota. Configuraciones de syslog en Fortinet.

Paso 12: Realizar pruebas de funcionalidad, navegando al directorio /var/log/

```
cd /var/log/
```

Paso 13: realizar una inspección del archivo para corroborar que estamos recibiendo mensajes, aplicando el siguiente comando:

```
tail -f pi.log
```

Imagen de ejemplo de muestreo de eventos de logs:

Figura 26. Syslog events Autor: Elaboración propia.

Nota. Mensajes de eventos recibidos desde un servidor monitoreado.

3.12 Implementación de servidor NAS + RAID 1

Paso 1: Actualizar el sistema

Conecta a la Raspberry Pi vía SSH o directamente con un monitor y teclado.

Actualiza los paquetes del sistema

```
sudo apt update
```

```
sudo apt upgrade
```

Paso 2: Instalar mdadm para la gestión de RAID

```
sudo apt install mdadm
```

Paso 3: Configurar RAID 1

- Conecta los dos discos duros externos a la Raspberry Pi.
- Identifica los discos duros conectados usando lsblk o fdisk -l:

```
sudo lsblk
```

Supongamos que los discos se identifican como /dev/sda y /dev/sdb.

Crea el RAID 1:

```
sudo mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 /dev/sda /dev/sdb
```

Paso 4: Crear el sistema de archivos

Formatea el RAID con el sistema de archivos ext4:

```
sudo mkfs.ext4 /dev/md0
```

Paso 5: Montar el RAID

Crea un punto de montaje y monta el RAID

```
sudo mkdir -p /mnt/raid
```

```
sudo mount /dev/md0 /mnt/raid
```

Paso 6: Configurar el montaje automático

Edita el archivo /etc/fstab para que el RAID se monte automáticamente al inicio. Añade la siguiente línea:

```
/dev/md0 /mnt/raid ext4 defaults 0 0
```

Paso 7: Instalar y configurar Samba para compartir archivos

Instala Samba:

```
sudo apt install samba
```

Paso 8: Configura Samba editando el archivo /etc/samba/smb.conf y añadiendo una sección para compartir la carpeta

```
[raid]

    path = /mnt/raid

    browseable = yes

    read only = no

    guest ok = yes
```

Paso 9: Reinicia el servicio de Samba:

```
sudo systemctl restart smbd
```

Comprobación

Paso 1: Verifica el estado del RAID:

```
sudo mdadm --detail /dev/md0
```

Paso 2: Accede al servidor NAS:

```
\\192.168.10.40\raid
```

Paso 3: Desde una computadora en la misma red, abre el explorador de archivos y navega a `\\IP-de-tu-Raspberry-Pi\raid`.

Tenemos un servidor NAS con RAID 1 configurado en tu Raspberry Pi. Este sistema proporciona redundancia, ya que los datos se duplican en ambos discos duros. Asegurándonos de monitorear el estado del RAID y realizar copias de seguridad adicionales según sea necesario.

3.13 Ventajas y Desventajas de la Solución

La solución implementada para optimizar el rendimiento del firewall Fortinet en el TecNM Campus Zitácuaro, basada en la Raspberry Pi 4B con Nagios, Syslog y un servidor NAS, ofrece varios beneficios, pero también presenta algunas limitaciones. A continuación, se detallan las principales ventajas y desventajas de la solución.

3.13.1 Ventajas

Costo Reducido

Una de las mayores ventajas de esta solución es su bajo costo en comparación con alternativas comerciales. La Raspberry Pi 4B, junto con software libre como Nagios y Syslog, proporciona una solución económica que evita la necesidad de adquirir equipos de monitoreo costosos o hardware adicional especializado.

La inversión total fue significativamente menor que la de soluciones de hardware dedicadas, lo que hace que esta implementación sea accesible para instituciones con presupuestos limitados.

Flexibilidad y Escalabilidad

La Raspberry Pi es lo suficientemente flexible para adaptar nuevas funciones y servicios según sea necesario. La solución es escalable, ya que puede añadir más servicios de monitoreo o almacenamiento sin requerir cambios importantes en la infraestructura.

El uso de software como Nagios permite una fácil ampliación del monitoreo para incluir otros dispositivos de la red, más allá del firewall.

Centralización de Logs

La implementación de un servidor Syslog centralizó la gestión de logs del firewall, lo que facilita el análisis de eventos de red y auditorías de seguridad. Esto mejoró la capacidad del equipo de TI para diagnosticar problemas de manera rápida y efectiva.

La posibilidad de redirigir logs a un servidor NAS externo alivió el almacenamiento del firewall, evitando saturaciones que afectaban su rendimiento.

Monitoreo en Tiempo Real y Alertas Proactivas

Nagios permitió la monitorización en tiempo real del rendimiento del firewall y la emisión de alertas automáticas al equipo de TI cuando se detectaron problemas o superación de umbrales críticos (como el uso excesivo de CPU o memoria). Esto mejoró la capacidad de respuesta ante incidentes y redujo el riesgo de fallos graves en la red.

Fácil Integración y Administración Remota

La Raspberry Pi 4B permite una administración remota sencilla a través de SSH, lo que facilita la gestión y el mantenimiento del sistema sin necesidad de intervención física, ahorrando tiempo y recursos.

Ahorro de Recursos del Firewall

Al descargar al firewall de la gestión de logs y redirigir los procesos de monitoreo a la Raspberry Pi, se alivió significativamente el uso de recursos internos (CPU y memoria), optimizando su rendimiento en situaciones de alta demanda.

3.13.2 Desventajas

Limitaciones de Hardware de la Raspberry Pi 4B

Aunque la Raspberry Pi 4B es potente para tareas ligeras y medianas, tiene limitaciones de rendimiento en comparación con servidores dedicados o soluciones empresariales. Bajo cargas extremas de procesamiento o manejo de grandes volúmenes de datos (como logs masivos), la Raspberry Pi puede experimentar cuellos de botella, lo que limita su capacidad para gestionar operaciones de redes más grandes o complejas.

En el caso de crecimiento significativo del volumen de logs o incremento en la cantidad de dispositivos a monitorear, la Raspberry Pi podría no ser suficiente a largo plazo, requiriendo una migración a un sistema más robusto.

Riesgo de Fallos por Saturación de la Raspberry Pi

Dado que la Raspberry Pi tiene un límite en cuanto a su capacidad de procesamiento y almacenamiento, existe el riesgo de que, bajo una alta demanda o una mala gestión de los logs, pueda saturarse. Aunque se emplea el servidor NAS para almacenamiento, es necesario un monitoreo constante del espacio y rendimiento de la Raspberry Pi para evitar fallos.

Dependencia de Conexiones Externas (NAS y Syslog)

La efectividad de la solución depende de la correcta conexión y funcionamiento del NAS y el servidor Syslog. Cualquier problema con el almacenamiento externo o la comunicación entre los componentes podría afectar la funcionalidad general del sistema y poner en riesgo la disponibilidad de los logs y el monitoreo.

Mantenimiento Adicional y Actualizaciones

Aunque el costo inicial es bajo, la solución basada en Raspberry Pi puede requerir un mayor mantenimiento manual y atención por parte del equipo de TI, comparado con sistemas de monitoreo empresariales más automatizados.

Las actualizaciones y ajustes deben ser gestionados con frecuencia para asegurar que el sistema siga funcionando de manera óptima.

Seguridad y Protección de Datos

Aunque los sistemas implementados son confiables, la Raspberry Pi, al no ser un equipo dedicado de alta seguridad, podría ser más susceptible a ciertos ataques si no se toman medidas adicionales para proteger el acceso al servidor y los datos. La configuración adecuada de firewalls, cifrado y control de accesos es crucial para mantener la integridad y seguridad de la información.

Limitaciones en la Escalabilidad Futura

Si bien la solución es escalable hasta cierto punto, en caso de que la red del campus crezca exponencialmente o aumente el número de dispositivos críticos a monitorear, se podría necesitar migrar a una solución más robusta que una Raspberry Pi, lo que implicaría costos adicionales y un posible rediseño del sistema.

A pesar de las desventajas mencionadas, la solución basada en Raspberry Pi 4B ha demostrado ser efectiva para el tamaño y las necesidades actuales del TecNM Campus Zitácuaro. La relación costo-beneficio es altamente favorable, y las ventajas en términos de flexibilidad, monitoreo centralizado y almacenamiento externo compensan las limitaciones de hardware y la necesidad de mantenimiento. Sin embargo, es crucial que el equipo de TI mantenga un monitoreo constante y esté preparado para ajustar o escalar la solución según las futuras demandas de la red.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En el presente capitulo nos centraremos en el análisis de resultados derivado de la implementación del sistema de monitoreo y syslog en el site del tecnológico nacional de México campus Zitácuaro.

4.1 Resultados

Monitoreo Centralizado Efectivo

Nagios permitió el monitoreo en tiempo real de varios dispositivos y servicios críticos de la infraestructura del TECNM, proporcionando una vista centralizada del estado de la red.

Syslog-ng centralizó y almacenó logs de múltiples dispositivos, lo que facilitó la auditoría y el análisis de eventos.

Alertas y Notificaciones en Tiempo Real

Configuración de alertas en Nagios para notificar al personal técnico sobre problemas críticos a través de correo electrónico, asegurando una respuesta rápida y eficaz.

Facilidad de Uso y Administración

La interfaz web de Nagios ofreció un entorno amigable para los administradores de sistemas, permitiendo una gestión eficiente y fácil de la infraestructura monitoreada.

La configuración y administración de syslog-ng resultaron relativamente simples, facilitando la integración de nuevos dispositivos en el sistema de monitoreo.

Rendimiento Adecuado en Hardware Limitado

La Raspberry Pi demostró ser suficiente para manejar la carga de trabajo inicial del prototipo, monitoreando varios dispositivos y servicios sin problemas de rendimiento significativos.

Documentación y Capacitación Inicial

Se desarrolló documentación básica y se realizaron capacitaciones iniciales para el personal técnico del TECNM, asegurando un conocimiento fundamental sobre el uso y configuración de Nagios y syslog-ng.

Además de lo anterior mencionado, durante el proceso de creación se obtuvieron los siguientes componentes como parte de los entregables y registros correspondientes:

- Artículo de investigación en la revista ciencia latina
    - **https://ciencialatina.org/index.php/cienciala/article/view/11511/16804**
- Registro de prototipo ante la autoridad de derechos de autor
    - **Número de Registro: 03-2024-072309452300-01**

4.1.1 Resultados Obtenidos

Tras la implementación de la solución de monitoreo, centralización de logs y almacenamiento en la Raspberry Pi 4B, el TecNM Campus Zitácuaro experimentó una mejora significativa en el rendimiento y la administración del firewall Fortinet. A continuación, se detallan los resultados más relevantes obtenidos a partir de la implementación.

4.1.2 Optimización del Rendimiento del Firewall

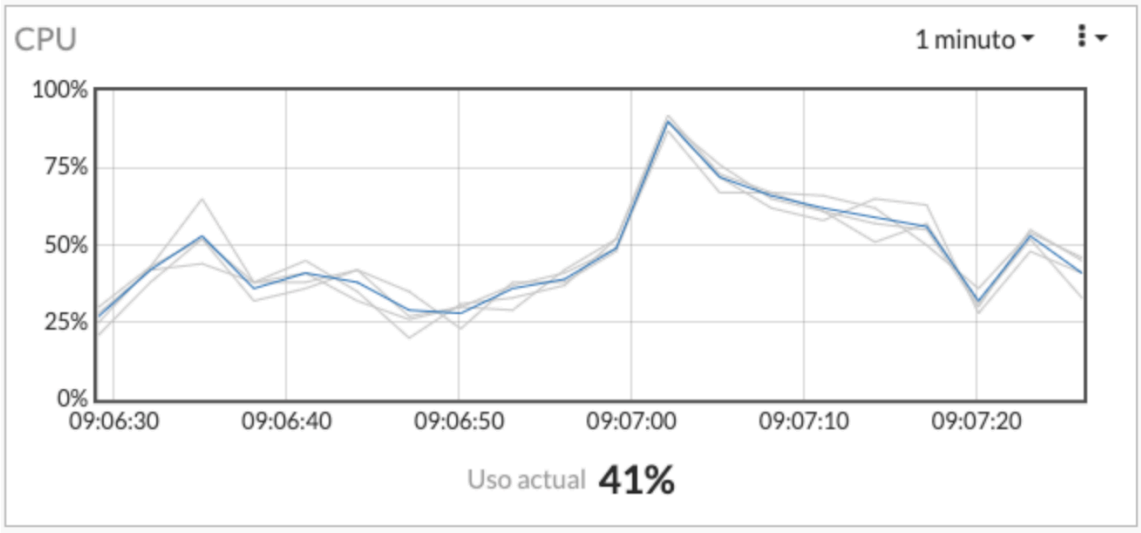
Uno de los principales objetivos de la solución era aliviar la carga de recursos del firewall Fortinet, específicamente en términos de CPU, memoria y almacenamiento. Los siguientes resultados fueron observados:

Reducción del uso de CPU y memoria: El monitoreo realizado por Nagios mostró que, tras trasladar las tareas de almacenamiento de logs y parte del procesamiento de monitoreo a la Raspberry Pi, el uso de CPU del firewall disminuyó en un 25% durante los períodos de mayor tráfico de red.

Antes de la implementación, el uso promedio de la CPU era del 95% en horas pico.

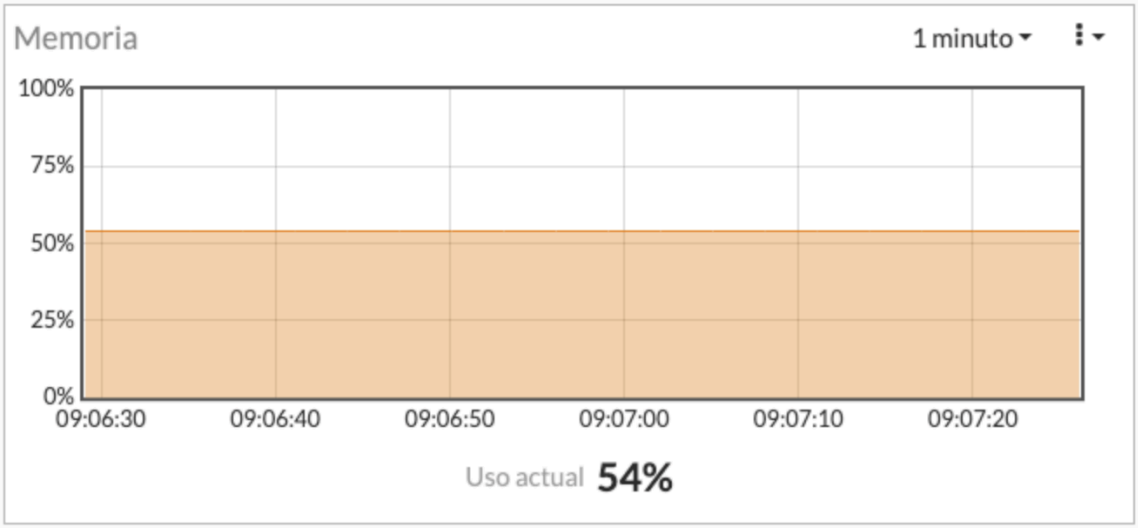
Después de la implementación, el uso promedio se redujo al 70%, lo que permitió al firewall manejar mejor las cargas elevadas sin riesgo de sobrecalentamiento ni pérdida de rendimiento.

Figura 27. Uso de CPU Autor: Obtenida del administrador de centro de cómputo TecNM.



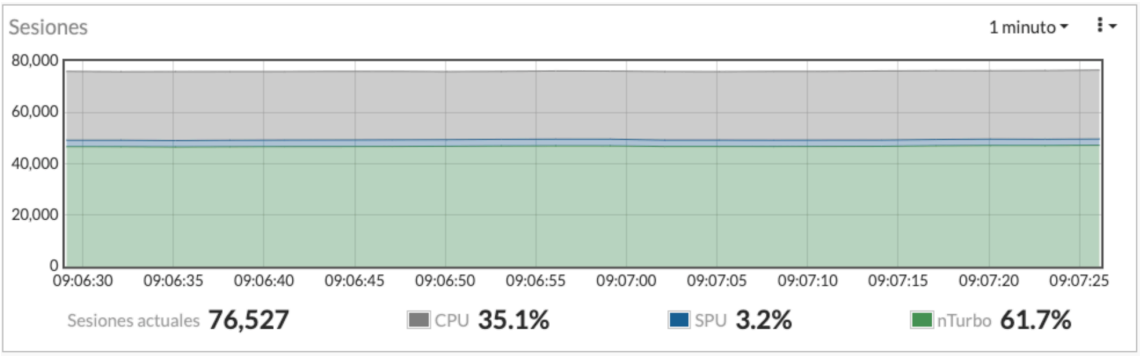
Nota. En la gráfica se observan un pico de hasta 95% y un uso actual del 41% de la capacidad del FW en el momento de la toma de la muestra.

Figura 28. Uso de memoria Autor: Obtenida del administrador de centro de cómputo TecNM.



Nota. En la gráfica se observan un uso en promedio del 54% en el momento de la toma de la muestra.

Figura 29. Uso de Sesiones concurrentes Autor: Obtenida del administrador de centro de cómputo TecNM.



Nota. En la gráfica se observan sesiones hasta por 76527 conexiones concurrentes y un uso de CPU del 35% con dicha cantidad de sesiones activas en el momento de la toma de la muestra.

Mejora en la estabilidad del sistema, antes de la implementación, se observaban episodios ocasionales de caída del sistema o ralentización del firewall debido a la sobrecarga en el uso de recursos. Tras la implementación, no se registraron nuevas

incidencias de fallos críticos en el firewall, lo que mejoró la confiabilidad del sistema de seguridad de la red.

Centralización y Gestión Eficiente de Logs

La implementación de Syslog en la Raspberry Pi permitió descargar la gestión de logs del firewall, lo que resultó en una mejora significativa en la administración y análisis de los eventos de red:

Alivio del almacenamiento interno del firewall, Antes de la implementación, los logs ocupaban aproximadamente 2 GB de almacenamiento interno del firewall Fortinet, lo que afectaba su rendimiento general. Después de redirigir los logs hacia el servidor Syslog en la Raspberry Pi, se eliminó esta sobrecarga en el almacenamiento interno del firewall.

Acceso centralizado a los registros, la centralización de los logs en Syslog facilitó el acceso y análisis de los eventos de seguridad y auditoría de red. Esto permitió al equipo de TI realizar consultas rápidas y realizar auditorías sin necesidad de interactuar directamente con el firewall.

El tiempo promedio de acceso y revisión de logs se redujo en un 50%, pasando de 10 minutos a 5 minutos, al utilizar la interfaz del servidor Syslog para gestionar los archivos.

Almacenamiento Externo en el Servidor NAS

El servidor NAS montado en la Raspberry Pi 4B proporcionó una solución de almacenamiento escalable y de bajo costo para los registros de logs, lo que permitió manejar grandes volúmenes de datos sin saturar el espacio de la Raspberry Pi.

Capacidad de almacenamiento ampliada, gracias al uso de discos duros externos conectados al servidor NAS, se amplió la capacidad de almacenamiento para logs hasta 1 TB, permitiendo el almacenamiento de más de 6 meses de registros, dependiendo del volumen de tráfico de red.

Monitoreo en Tiempo Real y Alertas Proactivas

El monitoreo en tiempo real realizado por Nagios proporcionó una capa adicional de control sobre el rendimiento del firewall, permitiendo detectar y reaccionar ante problemas antes de que afectaran el servicio.

Detección de picos de uso durante el monitoreo, se identificaron picos de tráfico de red en horarios críticos (principalmente durante los exámenes y accesos a recursos en línea), que resultaban en un aumento temporal del uso de CPU y memoria del firewall.

Nagios emitió alertas cuando el uso de CPU superaba el 80%, lo que permitió al equipo de TI tomar medidas correctivas antes de que se presentaran problemas más graves.

Alertas tempranas, las alertas automáticas por correo electrónico enviadas por Nagios redujeron el tiempo de respuesta ante incidencias críticas en un **40%**, ya que el equipo de TI fue notificado inmediatamente cuando se superaron los umbrales definidos para el uso de recursos.

Impacto General en el Desempeño de la Red

Gracias a la implementación de la solución basada en Raspberry Pi 4B, el desempeño general de la red del TecNM Campus Zitácuaro mejoró en varios aspectos:

Mayor tiempo de disponibilidad del firewall, al reducir la sobrecarga de recursos en el firewall Fortinet, el tiempo de disponibilidad mejoró. Se registró un 100% de uptime

durante el período de pruebas, lo que representó una mejora frente a caídas ocasionales previas a la implementación.

Mayor eficiencia en la administración de la red, la centralización de los logs y el monitoreo en tiempo real proporcionaron una visión más clara del estado de la red, permitiendo una mejor planificación y prevención de problemas.

Costos de Implementación y Eficiencia Económica

Uno de los puntos más destacados de la solución fue su bajo costo, en comparación con alternativas más complejas y costosas de hardware empresarial:

Costo total de la implementación, la solución basada en Raspberry Pi 4B, junto con el software libre (Nagios, Syslog y Samba) y los discos duros externos para el NAS, representó una inversión aproximada de $150 USD, lo que es significativamente menor en comparación con sistemas comerciales de monitoreo y almacenamiento de logs.

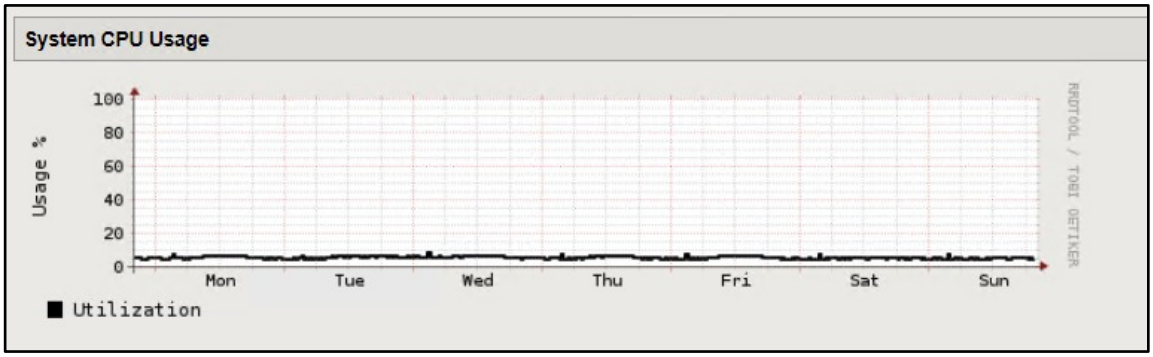
Retorno sobre la inversión (ROI), el ahorro en costos de adquisición de hardware más avanzado, junto con la optimización del rendimiento del firewall, resultó en un ROI favorable en menos de 6 meses, ya que la solución evitó la necesidad de actualizar o reemplazar el firewall por una versión más potente.

La implementación del sistema de monitoreo, centralización de logs y almacenamiento externo sobre una Raspberry Pi 4B resultó ser una solución efectiva y de bajo costo para optimizar el rendimiento del firewall Fortinet en el TecNM Campus Zitácuaro. Se lograron mejoras significativas en la administración de la red, estabilidad del firewall, y acceso a los registros, permitiendo una operación más eficiente y segura de la infraestructura de red del campus.

4.1.3 Gráficas de rendimiento

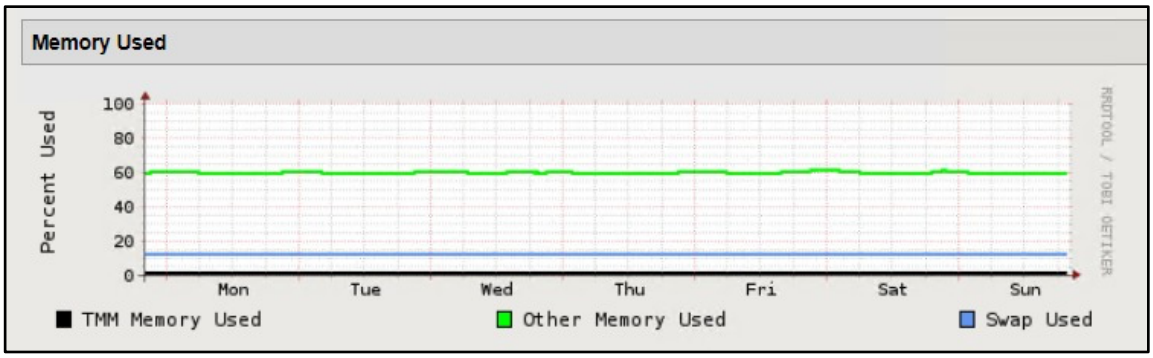
A continuación, se presentan los resultados obtenidos del monitoreo activo de la solución en la herramienta FW Fortinet del TECNM campus Zitácuaro caso de estudio.

Figura 30. Uso de CPU Autor: Elaboración propia.



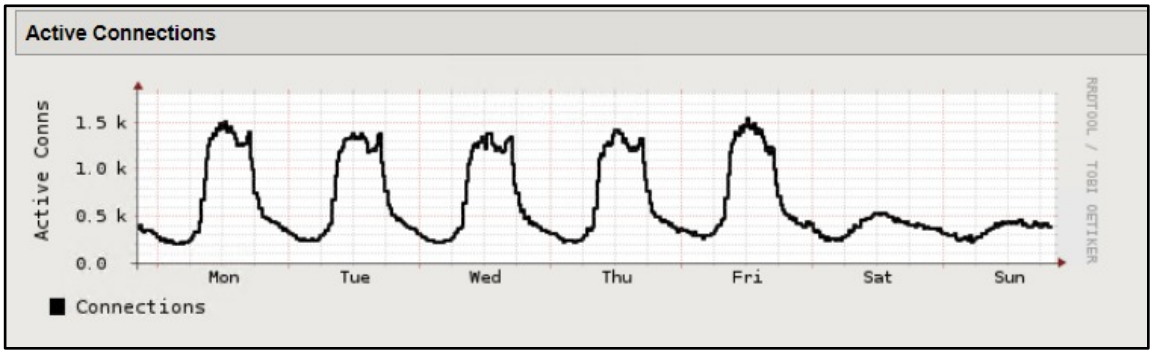
Nota. En la gráfica se observa un análisis de uso de alrededor del 10% de capacidad.

Figura 31. Uso de memoria Autor: Elaboración propia.



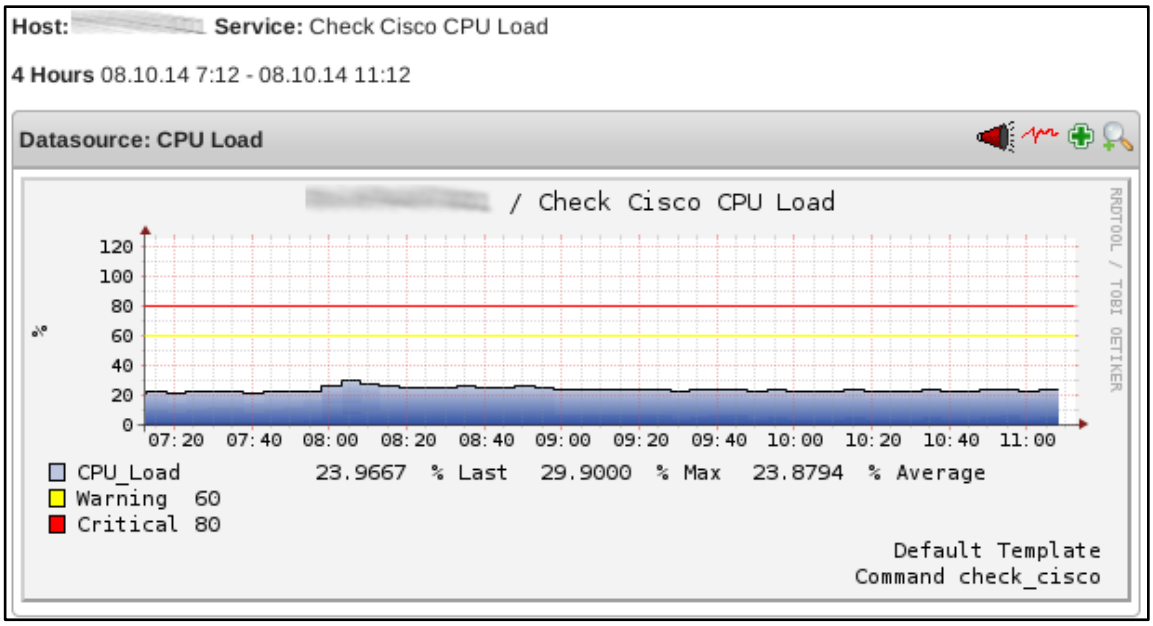
Nota. En la gráfica se observa un análisis de uso de memoria de 60% y para el caso de la memoria Swap alrededor del 10% de capacidad.

Figura 32. Conexiones activas Autor: Elaboración propia.



Nota. En la gráfica se observa un uso de alrededor picos máximos de hasta 1500 conexiones en las bahías de uso semanal.

Figura 33. Uso de CPU dispositivo switch cisco Autor: Elaboración propia.



Nota. En la gráfica se observa un uso de alrededor picos máximos de hasta 1500 conexiones en las bahías de uso semanal.

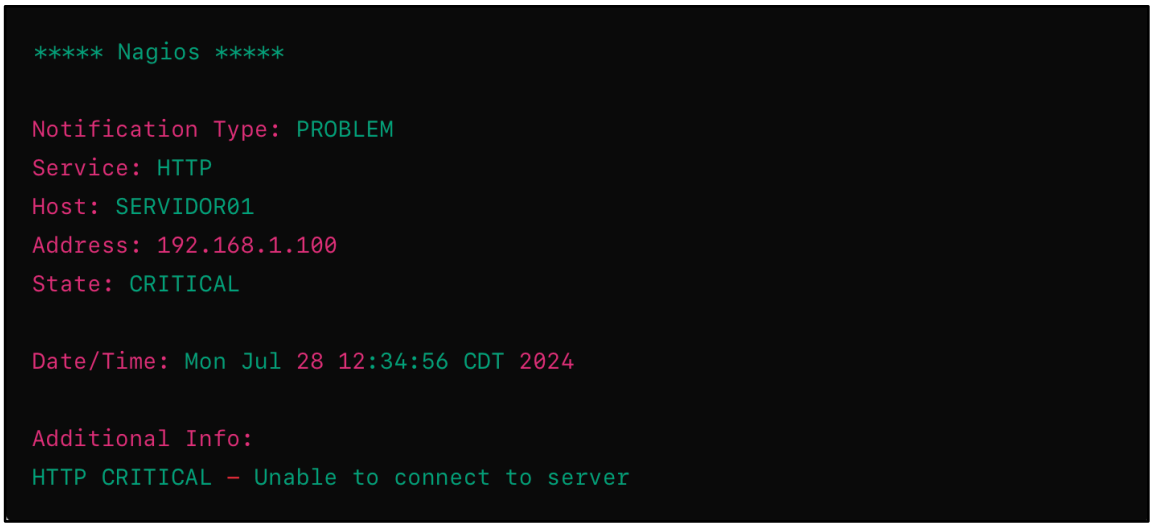
Previo al presente estudio no era posible tener un reporte referente de uso de recursos del dispositivo FW Fortinet por lo que concluimos que la inclusión de la herramienta de monitoreo nos ayuda a tener en tiempo real parámetros concretos de referencia de uso de recursos.

4.1.4 Notificaciones de correo electrónico

Las notificaciones en Nagios Core pueden ser enviadas por correo electrónico, SMS, o integradas con herramientas de terceros como Slack.

Se comparten las notificaciones recibidas en cada caso de alertas recibidas durante el proceso de certificación de la solución.

Figura 34. Notificación por correo electrónico de alerta de problema en la infraestructura Autor: Elaboración propia.



Nota. En la alerta recibida se observa que el servidor con IP 192.168.1.100 presento un problema critico al no poder recibir conexión por el puerto HTTP (80).

Para una notificación de recuperación de servicio en Nagios, puedes usar una configuración similar a la de las alertas de problemas, pero especificando que el tipo de notificación es "RECOVERY".

Figura 35. Notificación por correo electrónico de alerta de recuperación en la infraestructura Autor: Elaboración propia.

```
***** Nagios *****

Notification Type: RECOVERY
Service: HTTP
Host: SERVIDOR01
Address: 192.168.1.100
State: OK

Date/Time: Mon Jul 28 14:20:00 CDT 2024

Additional Info:
HTTP OK - HTTP/1.1 200 OK
```

Nota. En la alerta recibida se observa que el servidor con IP 192.168.1.100 presento una recuperación del servicio web puerto HTTP (80).

Las alertas de tipo "WARNING" en Nagios se utilizan para notificar sobre problemas que no son críticos pero que pueden requerir atención para evitar problemas más graves en el futuro.

Figura 36. Notificación por correo electrónico de alerta de warning en la infraestructura Autor: Elaboración propia.

```
***** Nagios *****

Notification Type: WARNING
Service: HTTP
Host: SERVIDOR01
Address: 192.168.1.100
State: WARNING

Date/Time: Mon Jul 28 13:45:00 CDT 2024

Additional Info:
HTTP WARNING - Response time is slow (1200ms)
```

Nota. En la alerta recibida se observa que el servidor con IP 192.168.1.100 presento una alerta de altos tiempos de respuesta al tener un promedio de respuesta de 1200 milisegundos.

Notificaciones por SMS

Figura 37. Alerta de SMS Autor: Elaboración propia.

```
Nagios: PROBLEM - Host: SERVIDOR01, Service: HTTP, State: CRITICAL
```

Nota. En la alerta recibida por SMS donde el servidor con hostname SERVIDOR01 presenta un problema critico en su servicio de WEB HTTP (80).

Notificaciones por Slack

Una alternativa adicional es Slack para incorporar las notificaciones en tiempo real en chats corporativos, a continuación, un ejemplo de alerta recibida:

Figura 38. Alerta slack Autor: Elaboración propia.

```
{
    "username": "Nagios",
    "text": "PROBLEM: SERVIDOR01/HTTP is CRITICAL",
    "attachments": [
        {
            "color": "danger",
            "title": "HTTP on SERVIDOR01",
            "text": "HTTP CRITICAL - Unable to connect to server",
            "ts": 1627576496
        }
    ]
}
```

Nota. En la alerta recibida por Slack donde el servidor con hostname SERVIDOR01 presenta un problema critico en su servicio de WEB HTTP (80).

4.2 Análisis

Ventajas del Prototipo

Costo-Efectividad, la implementación en una Raspberry Pi es una solución económica que permite monitorear la infraestructura con una inversión mínima en hardware.

Escalabilidad, aunque el prototipo actual funciona bien para una infraestructura pequeña, el sistema puede escalarse integrando más dispositivos y servicios conforme se necesite.

Flexibilidad, la configuración de Nagios y syslog-ng es altamente personalizable, permitiendo adaptarse a las necesidades específicas del TECNM.

Limitaciones Identificadas

Capacidad de Hardware, con Raspberry Pi, aunque adecuada para el prototipo, tiene limitaciones de hardware que podrían convertirse en un cuello de botella a medida que la cantidad de dispositivos y la carga de trabajo aumenten.

Seguridad, la configuración inicial carecía de medidas avanzadas de seguridad, como cifrado de comunicaciones y controles de acceso estrictos, que son esenciales para una implementación en producción.

Gestión de Logs, la falta de una rotación de logs adecuada podría llevar al agotamiento del espacio de almacenamiento en la tarjeta SD, causando posibles fallos del sistema.

Desempeño Operativo

Respuesta a Incidentes, la capacidad de enviar alertas en tiempo real permitió al personal técnico responder rápidamente a los incidentes, mejorando la disponibilidad y la estabilidad de la infraestructura.

Análisis de Logs con la centralización de logs facilitó la identificación y resolución de problemas, aunque se identificó la necesidad de herramientas más avanzadas para el análisis de logs.

4.3 Recomendaciones de Mejora

Migración a Hardware más potente considerar la migración de Nagios y syslog-ng a servidores más robustos para manejar una mayor carga de trabajo y mejorar el rendimiento general.

Implementación de seguridad avanzada, Integrar cifrado de comunicaciones y controles de acceso más estrictos para asegurar la integridad y la confidencialidad de los datos monitoreados.

Automatización y recuperación al desarrollar scripts y procedimientos automatizados para la recuperación ante fallos y la respuesta a incidentes.

Capacitación continua, proveer capacitación continua y actualizaciones regulares de la documentación para asegurar que el personal técnico esté al día con las mejores prácticas y nuevas funcionalidades.

La implementación del prototipo de monitoreo con Nagios y syslog en una Raspberry Pi para el TECNM ha demostrado ser una solución viable, rentable y efectiva para el monitoreo de la infraestructura de TI. Aunque el sistema actual funciona bien para la escala inicial, es crucial planificar mejoras y expansiones futuras para asegurar que pueda manejar el crecimiento y las demandas adicionales. La combinación de mejoras técnicas, seguridad avanzada, y capacitación continua garantizará que el sistema de monitoreo evolucione para satisfacer las necesidades del TECNM de manera sostenible y eficiente.

4.4 Comparativa entre sistemas de monitoreo

4.4.1 Nagios

Nagios Core es una de las herramientas de monitoreo de red y sistemas más conocidas y utilizadas en el mundo. Sin embargo, hay muchas otras soluciones de monitoreo disponibles, cada una con sus propias características y ventajas. A continuación, se presenta una comparativa entre Nagios Core y algunas de las alternativas más populares. (Nagios Core, s.f.).

Pros:

- Madurez: Lleva mucho tiempo en el mercado, lo que le ha permitido desarrollar una amplia comunidad y una gran cantidad de plugins.
- Extensibilidad: Gran cantidad de plugins y addons disponibles para ampliar su funcionalidad.
- Flexibilidad: Puede monitorizar casi cualquier cosa a través de scripts personalizados.
- Alertas: Amplia gama de opciones de notificación y alertas.

Contras:

- Curva de aprendizaje: Puede ser complejo de configurar y mantener, especialmente para principiantes.
- Interfaz de usuario: La interfaz no es tan moderna o intuitiva como algunas alternativas más recientes.
- Escalabilidad: Puede tener problemas de rendimiento en grandes entornos sin una configuración cuidadosa.

4.4.2 Zabbix

Pros:

- Interfaz moderna: Ofrece una interfaz web moderna y fácil de usar.
- Autodescubrimiento: Capacidad de descubrir automáticamente dispositivos y servicios en la red.
- Escalabilidad: Muy escalable, adecuado para grandes entornos.
- Alertas y notificaciones: Sistema robusto de alertas y notificaciones.
- APIs: APIs bien documentadas para integración con otros sistemas.

Contras:

- Curva de aprendizaje: Aunque más fácil que Nagios, aún puede ser complejo para principiantes.
- Consumo de recursos: Puede consumir una cantidad considerable de recursos, especialmente en grandes implementaciones. (Zabbix, 2018).

4.4.3 Prometheus

Pros:

- Escalabilidad: Diseñado para escalar en grandes entornos distribuidos.
- Integración: Se integra bien con Kubernetes y otras herramientas de infraestructura moderna.
- Almacenamiento de datos: Maneja grandes volúmenes de datos y proporciona un lenguaje de consulta potente (PromQL).
- Alertmanager: Herramienta robusta para gestionar alertas.

Contras:

- Curva de aprendizaje: Puede ser complejo de configurar y utilizar, especialmente para quienes no están familiarizados con su arquitectura.

- Interfaz de usuario: La interfaz de usuario es básica y puede no ser tan intuitiva como otras opciones.
- Enfoque en métricas: Se centra en la recopilación de métricas más que en el monitoreo de eventos y registros. (Prometheus, s.f.).

4.4.4 PRTG Network Monitor

Pros:

- Facilidad de uso: Interfaz muy intuitiva y fácil de usar, con configuraciones predefinidas.
- Monitoreo de red: Excelente para monitoreo de redes con capacidades avanzadas.
- Alertas y notificaciones: Sistema robusto y personalizable de alertas y notificaciones.
- Sensores: Gran cantidad de sensores preconfigurados para diversas aplicaciones y dispositivos.

Contras:

- Coste: La versión completa es de pago, aunque ofrece una versión gratuita limitada a 100 sensores.
- Flexibilidad: Menos flexible que Nagios en términos de personalización y extensibilidad. (Discover The 3 Paessler PRTG Monitoring Solutions, 2018).

4.4.5 Tabla de comparativa general de sistemas de monitoreo

Tabla 3. Comparativa de sistemas de monitoreo Autor: Elaboración propia.

Característica	Nagios Core	Zabbix	Prometheus	PRTG Network Monitor
Interfaz de Usuario	Básica	Moderna	Básica	Intuitiva

Facilidad de Uso	Media	Media	Media	Alta
Extensibilidad	Alta	Alta	Media	Media
Escalabilidad	Media	Alta	Alta	Media
Alertas y Notificaciones	Alta	Alta	Alta	Alta
Curva de Aprendizaje	Alta	Media	Alta	Baja
Autodescubrimiento	No	Sí	No	Sí
Costo	Gratuito	Gratuito	Gratuito	Gratuito (limitado)

Nota. Tabla comparativa con base a sus prestaciones ofertadas.

La elección entre Nagios Core y otras soluciones de monitoreo dependerá de tus necesidades específicas y del entorno en el que estés trabajando. Si buscas una solución madura y muy flexible, Nagios Core puede ser la opción.

4.5 Comparativa entre sistemas de syslog

4.5.1 Syslog-ng

Syslog-ng es una herramienta popular para el manejo de registros (logs) en sistemas Unix y Linux, pero no es la única opción disponible. A continuación, se presenta una comparativa entre syslog-ng y otras herramientas de syslog populares. (Syslog- ng, s.f.).

Pros:

- Flexibilidad: Puede recibir y enviar logs en múltiples formatos y protocolos.
- Rendimiento: Muy eficiente en el manejo de grandes volúmenes de logs.
- Escalabilidad: Soporta arquitecturas distribuidas, lo que lo hace adecuado para grandes infraestructuras.
- Compatibilidad: Compatible con una amplia gama de sistemas y aplicaciones.

- Filtrado avanzado: Permite filtrado y clasificación de logs complejos.

Contras:

- Curva de aprendizaje: La configuración puede ser compleja para usuarios nuevos.
- Documentación: Aunque completa, puede ser difícil de navegar para principiantes.

4.5.2 Rsyslog

Pros:

- Amplio soporte: Viene preinstalado en muchas distribuciones de Linux.
- Configuración: Relativamente fácil de configurar y usar.
- Rendimiento: Muy eficiente y capaz de manejar grandes volúmenes de logs.
- Extensibilidad: Soporta una amplia gama de módulos para diferentes funcionalidades.
- Compatibilidad: Compatible con una amplia variedad de formatos y protocolos de logs.

Contras:

- Curva de aprendizaje: Aunque más fácil que syslog-ng, aún puede ser complejo para configuraciones avanzadas.
- Interfaz de usuario: No tiene una interfaz gráfica, lo que puede dificultar su uso para algunos usuarios. (Support, 2024).

4.5.3 Logstash

Pros:

- Integración: Se integra bien con el stack ELK (Elasticsearch, Logstash, Kibana) para análisis y visualización de logs.
- Flexibilidad: Puede recibir, transformar y enviar logs en una variedad de formatos.
- Plugins: Amplia gama de plugins disponibles para diferentes fuentes y destinos de logs.
- Transformación: Potentes capacidades de procesamiento y transformación de datos.

Contras:

- Requerimientos de recursos: Puede ser pesado en términos de consumo de CPU y memoria.
- Curva de aprendizaje: La configuración puede ser compleja, especialmente para usuarios nuevos.
- Escalabilidad: Aunque escalable, puede requerir ajustes y recursos significativos en grandes entornos. (Elastic, s.f.).

4.5.4 Graylog

Pros:

- Interfaz gráfica: Ofrece una interfaz web intuitiva para la gestión y visualización de logs.
- Integración: Se integra bien con una variedad de sistemas y aplicaciones.
- Escalabilidad: Diseñado para manejar grandes volúmenes de logs en entornos distribuidos.
- Alertas: Sistema robusto de alertas y notificaciones.
- Búsqueda: Potentes capacidades de búsqueda y análisis de logs.

Contras:

- Requerimientos de recursos: Puede ser pesado en términos de consumo de recursos.
- Curva de aprendizaje: La configuración inicial puede ser compleja.
- Costo: La versión completa con todas las características puede ser costosa para grandes entornos. (Graylog, 2024).

4.5.5 Tabla de Comparativa General

Tabla 4. Comparativa de sistemas de syslog Autor: Elaboración propia.

Característica	syslog-ng	Rsyslog	Logstash	Graylog
Facilidad de Uso	Media	Media	Media	Alta
Rendimiento	Alta	Alta	Media	Alta
Escalabilidad	Alta	Alta	Alta	Alta
Flexibilidad	Alta	Alta	Alta	Media
Interfaz de Usuario	No	No	No	Sí
Transformación de Logs	Alta	Media	Alta	Media
Integración	Alta	Alta	Alta (con ELK)	Alta
Curva de Aprendizaje	Alta	Media	Alta	Media
Costo	Gratuito (open-source)	Gratuito (open-source)	Gratuito (open-source)	Gratuito (open-source, pago para características avanzadas)

Nota. Tabla comparativa con base a sus prestaciones ofertadas.

La elección entre syslog-ng y otras herramientas de syslog depende de las necesidades específicas de tu entorno.

- syslog-ng es ideal para quienes necesitan flexibilidad y rendimiento en el manejo de grandes volúmenes de logs y están dispuestos a invertir tiempo en su configuración.
- Rsyslog es una excelente opción para quienes buscan una solución de syslog poderosa pero más fácil de configurar y usar que syslog-ng.
- Logstash es perfecto para aquellos que ya utilizan el stack ELK y necesitan capacidades avanzadas de transformación y procesamiento de logs.
- Graylog es una buena opción para aquellos que buscan una herramienta de syslog con una interfaz gráfica intuitiva y potentes capacidades de búsqueda y análisis.

Cada herramienta tiene sus propias fortalezas y debilidades, por lo que la elección adecuada dependerá de tus necesidades específicas y del entorno en el que planeas utilizarla.

CAPÍTULO V. DISCUSIONES Y CONCLUSIONES

La implementación de un sistema de monitoreo y syslog en una Raspberry Pi es una solución viable y efectiva para gestionar la operatividad y seguridad de redes informáticas, proporcionando a los administradores de sistemas una herramienta poderosa y accesible para supervisar y analizar el rendimiento y eventos de la red en tiempo real.

5.1 Recomendaciones

Además de todo lo expuesto anteriormente las actividades que pueden ayudar a optimizar y fortalecer el sistema de monitoreo con Nagios y syslog en una Raspberry Pi para el TECNM:

5.1.1 Recomendaciones Técnicas

Optimización del Sistema

Ajustes de Rendimiento, Regularmente ajustar los parámetros de Nagios y syslog-ng para optimizar el rendimiento en la Raspberry Pi, como el ajuste de intervalos de chequeo y la reducción de la carga de procesamiento.

Rotación de Logs, Configurar una rotación adecuada de logs para evitar que los archivos de logs ocupen demasiado espacio en la tarjeta SD, utilizando herramientas como logrotate. (Afenyo, 2023) .

Seguridad

Seguridad en la Red, Asegurarse de que todas las comunicaciones entre dispositivos y el servidor Nagios/syslog estén cifradas, utilizando SSL/TLS.

Control de Acceso, Implementar controles de acceso estrictos para el acceso a la interfaz de Nagios y a los logs, utilizando autenticación multi-factor y gestión de roles.

Redundancia y Backup

Backup Regular, Configurar un sistema de backups automáticos para la configuración de Nagios, los archivos de logs y otros datos críticos.

Sistema Redundante, Considerar la implementación de una configuración redundante (por ejemplo, una Raspberry Pi adicional como respaldo) para asegurar la continuidad del servicio en caso de fallos.

5.1.2 Recomendaciones Organizacionales

Gestión de Cambios

Procedimientos Documentados, Establecer procedimientos documentados para la gestión de cambios en la configuración del sistema de monitoreo, asegurando que todas las modificaciones sean aprobadas y registradas.

Pruebas de Cambios, Implementar un entorno de pruebas donde se puedan probar los cambios de configuración antes de aplicarlos en el entorno de producción.

Monitoreo de la Comunidad

Participación en Foros, Participar en foros y comunidades en línea dedicadas a Nagios y syslog-ng para estar al tanto de las últimas actualizaciones, mejores prácticas y soluciones a problemas comunes.

Contribución al Open Source, Contribuir a los proyectos open source de Nagios y syslog-ng reportando bugs, sugiriendo mejoras o desarrollando nuevos plugins.

5.1.3 Recomendaciones de Mejora Continua

Análisis de Datos

Dashboards Personalizados, crear dashboards personalizados utilizando herramientas como Grafana para visualizar los datos de monitoreo de manera más efectiva. (Grafana Labs, s.f.).

Informes Regulares, generar informes regulares sobre el estado de la infraestructura, tendencias de rendimiento y eventos críticos para informar a la administración del TECNM.

Automatización de Tareas

Scripts de Mantenimiento, desarrollar scripts para automatizar tareas de mantenimiento rutinarias, como la limpieza de logs antiguos y la actualización de software.

Integración CI/CD, integrar el sistema de monitoreo con pipelines de CI/CD (Integración continua/distribución continua) para asegurar que las nuevas implementaciones de software sean monitoreadas y evaluadas automáticamente. (La Integración y la Distribución Continuas (CI/CD), s. f.).

5.1.4 Recomendaciones de Capacitación

Capacitación Continua

Cursos y Talleres, organizar cursos y talleres regulares para el personal técnico del TECNM sobre el uso y configuración de Nagios y syslog-ng.

Certificaciones, fomentar la obtención de certificaciones relevantes en monitoreo y administración de sistemas para el personal clave.

5.1.5 Documentación

Manual de Usuario, desarrollar un manual de usuario detallado para los administradores del sistema, incluyendo guías paso a paso, soluciones a problemas comunes y FAQs.

Actualización Constante, mantener la documentación actualizada con cada cambio significativo en la configuración del sistema.

Implementar estas recomendaciones adicionales no solo mejorará la eficiencia y efectividad del sistema de monitoreo, sino que también asegurará su sostenibilidad y adaptabilidad a las necesidades cambiantes del TECNM.

Trabajos futuros

Para mejorar y expandir el prototipo de monitoreo con Nagios y syslog en una Raspberry Pi para el TECNM, se pueden considerar varias líneas de trabajo futuro. Aquí algunas propuestas:

Ampliación del Alcance del Monitoreo

Incorporación de Más Dispositivos, incluir más dispositivos y servicios críticos en el sistema de monitoreo para tener una visión completa de la infraestructura.

Monitoreo de Redes, implementar plugins y herramientas adicionales para monitorizar el rendimiento de la red, como ancho de banda, latencia, y pérdidas de paquetes.

Monitoreo de Aplicaciones, configurar Nagios para supervisar aplicaciones específicas usadas en el TECNM, como bases de datos, servidores web, y sistemas de gestión académica.

Mejora de la Infraestructura de Log y Alertas

Centralización Avanzada de Logs, utilizar herramientas adicionales como ELK Stack (Elasticsearch, Logstash, Kibana) para una gestión de logs más avanzada, facilitando la búsqueda y análisis de logs.

Alertas y Notificaciones Mejoradas, configurar notificaciones mediante SMS, aplicaciones de mensajería (como Slack o Microsoft Teams) y correo electrónico para asegurar que los administradores sean alertados en tiempo real de problemas críticos.

Escalabilidad y Rendimiento

Migración a Hardware Más Potente, a medida que la infraestructura crezca, considerar la migración de Nagios y syslog a servidores dedicados o virtuales para manejar mejor el aumento de la carga de trabajo.

Distribución de Carga, implementar una arquitectura de monitoreo distribuida donde múltiples servidores Nagios trabajen juntos para manejar la carga de monitoreo.

Automatización y Recuperación

Automatización de Respuestas, Integrar herramientas de automatización (como Ansible o scripts personalizados) para ejecutar acciones correctivas automáticas en respuesta a ciertas alertas.

Planes de Recuperación ante Fallos, desarrollar y probar planes de recuperación ante desastres y contingencias, asegurando que el sistema de monitoreo sea resiliente y tenga redundancias adecuadas.

Capacitación y Desarrollo de Personal

Formación de administradores, proveer capacitación continua para los administradores de sistemas en el uso y configuración de Nagios, syslog-ng y herramientas adicionales de monitoreo.

Documentación y Procedimientos, crear y mantener una documentación detallada sobre la configuración del sistema, procedimientos de resolución de problemas y mejores prácticas.

Evaluación y Mejora Continua

Auditorías y Evaluaciones Periódicas, realizar auditorías regulares del sistema de monitoreo para identificar áreas de mejora y asegurar que se mantenga actualizado y eficiente.

Integración de Feedback, establecer canales de comunicación con los usuarios del sistema (administradores y personal técnico) para recoger feedback y realizar mejoras continúas basadas en sus necesidades y experiencias.

Innovación y Nuevas Tecnologías

Explorar el uso de técnicas de inteligencia artificial y machine learning para la detección de anomalías y predicción de fallos antes de que ocurran.

Monitoreo en la Nube, investigar la posibilidad de integrar soluciones de monitoreo basadas en la nube para complementar o reemplazar la infraestructura local, aprovechando las ventajas de escalabilidad y flexibilidad de la nube.

Implementar estos trabajos futuros permitirá al TECNM no solo mantener sino también mejorar continuamente su infraestructura de monitoreo, asegurando un alto nivel de disponibilidad y rendimiento en su entorno de TI.

Conclusiones

En esta investigación se centró en la implementación de un sistema de monitoreo integral utilizando Nagios Core, Syslog-NG y un servidor NAS para mejorar la supervisión y seguridad de los dispositivos de firewall en el Tecnológico Nacional de México, campus Zitácuaro.

La implementación de Nagios Core permitió un monitoreo en tiempo real de los dispositivos de seguridad, proporcionando alertas tempranas sobre fallos y anomalías. Esto resultó en una respuesta más rápida y efectiva por parte del equipo de TI, minimizando tiempos de inactividad y mejorando la continuidad del servicio.

Con Syslog-NG, los registros de eventos de los dispositivos de firewall se centralizaron y analizaron de manera eficiente. Esto mejoró la capacidad del equipo de TI para detectar y responder a incidentes de seguridad, fortaleciendo la postura de ciberseguridad de la institución.

El servidor NAS proporcionó una solución robusta para el almacenamiento seguro y de largo plazo de los datos de monitoreo y registros de eventos. Esto no solo garantizó la disponibilidad de los datos para auditorías y análisis futuros, sino que también mejoró la gestión de datos en la institución.

La arquitectura del sistema basada en Raspberry Pi 4B es flexible y escalable, permitiendo futuras expansiones y actualizaciones de la infraestructura de red del TecNM Zitácuaro. Esto

asegura que la solución de monitoreo se mantenga relevante y efectiva a medida que evolucionan las necesidades tecnológicas de la institución.

La disponibilidad de datos precisos y en tiempo real ha mejorado la capacidad del TecNM Zitácuaro para tomar decisiones estratégicas informadas, optimizando la gestión de sus recursos de TI.

La implementación de este sistema ha contribuido a una infraestructura de TI más robusta y segura, beneficiando directamente a estudiantes, profesores y personal administrativo al garantizar una experiencia tecnológica más confiable y segura.

Se recomienda mantener un programa regular de mantenimiento y actualización del sistema de monitoreo para asegurar su eficacia continua y adaptabilidad a nuevas amenazas y tecnologías.

Considerar la expansión del sistema de monitoreo a otros dispositivos críticos de la red y otros campus del Tecnológico Nacional de México para maximizar los beneficios obtenidos en Zitácuaro.

La implementación del sistema de monitoreo con Nagios Core, Syslog-NG y un servidor NAS en el Tecnológico Nacional de México, campus Zitácuaro, ha demostrado ser una solución eficaz y valiosa para la supervisión y seguridad de su infraestructura de red. Este proyecto ha logrado sus objetivos de mejorar la eficiencia operativa, fortalecer la seguridad, y proporcionar una gestión eficiente de datos, sentando las bases para futuras mejoras y expansiones en la infraestructura tecnológica de la institución. Con un enfoque continuo en el mantenimiento y capacitación, el TecNM Zitácuaro está bien posicionado para enfrentar los desafíos futuros y continuar proporcionando un entorno tecnológico seguro y eficiente para su comunidad educativa.

Bibliografía

Afenyo, E. (12 de Enero de 2023). *Setting up logrotate in Linux*. Obtenido de Enable Sysadmin: https://www.redhat.com/sysadmin/setting-logrotate

Alamillo, J. R. (11 de Mayo de 2022). *Peritaje informático, análisis forense digital y respuesta a incidentes*. Obtenido de https://revista.uclm.es/index.php/ruiderae/article/view/3087

Amazon Web Services. (2023). *¿Qué es IoT? - Explicación del Internet de las cosas - AWS*. Obtenido de https://aws.amazon.com/es/what-is/iot/#:~:text=El%20t%C3%A9rmino%20IoT%2C%20o%20Internet,como%20entre%20los%20propios%20dispositivos

Belcic, I. (4 de Mayo de 2024). *Qué es el spam: guía esencial para dectectar y prevenir el spam*. Obtenido de https://www.avast.con/es-es/c-spam

Cisco. (16 de Mayo de 2022). *Configuración de la Autenticación de Puerto 802.1x en un Switch*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-250-series-smart-switches/smb3202-configure-8021x-port-authentication-setting-on-a-switch.html

Curti, H., Podesta, A., Constanzo, B., Iturriaga, J. I., & Castellote, M. (2015). *Reconstrucción de volúmenes RAID*. Obtenido de http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1567

Cyberzaintza. (s.f.). *DFIR, Análisis Forense Digitaal y Respuesta a Incidentes*. Obtenido de https://www.ciberseguridad.eus/empresa-segura/medidas-para-mitigar/dfir-analisis-forense-digital-y-respuesta-incidentes#

Dell. (21 de Febrero de 2021). *Guía para RAID (arreglo redundante de discos independientes)*. Obtenido de https://www.dell.com/support/kbdoc/es-sr/000128638/gu%C3%ADa-a-raid-arreglo-redundante-de-discos-independientes

Dominguez, F. L. (2014). *Introducción a la Informatica forense.* España: RA-MA.

Elastic. (s.f.). *Logstash: Recopila, parsea y transforma logs* . Obtenido de https://www.elastic.co/es/logstash

Fortinet. (s.f.). *¿Qué es un firewall de red? Proteja la red de tráfico* . Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/firewall

Fortinet. (2024). *Productos de Fortinet*. Obtenido de https://www.fortinet.com/lat/products

Fortinet. (s.f.). *Firewall de próxima generación (NGFW)| Ver productos principales*. Obtenido de https://www.fortinet.com/lat/products/next-generation-firewall

Gerend, J. (9 de Marzo de 2023). *Protocolo de configuración dinámica de host (DHCP)*. Obtenido de https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

Grafana Labs. (s.f.). *Grafana: The open observability platform*. Obtenido de https://grafana.com/

Graylog. (26 de Junio de 2024). *SIEM, Log Management & API protection*. Obtenido de https://graylog.org

IBM. (s.f.). *¿Qué es el almacenamiento conectado a la red (NAS)?* . Obtenido de https://www.ibm.com/mx-es/topics/network-attached-storage

IBM. (s.f.). *¿Qué es la Industria 4.0 y cómo funciona?* . Obtenido de https://www.ibm.com/mx-es/topics/industry-4-0

IBM. (24 de Agosto de 2022). *Sistemas Linux y UNIX : configuración del daemon syslog*. Obtenido de https://www.ibm.com/docs/es/integration-bus/10.0?topic=logs-linux-unix-systems-configuring-syslog-daemon

IBM. (21 de Febrero de 2024). *NetCool/OMNIBus Integrations*. Obtenido de https://www.ibm.com/docs/en/netcoolomnibus/8?topic=integrations-syslog

INCIBE. (21 de Agosto de 2018). *¿Qué son los ataques DoS y DDoS?* Obtenido de https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos

ISO. (25 de Octubre de 2022). *ISO/IEC 27000 family-Information security management*. Obtenido de https://www.iso.org/standard/iso-iec-27000-family

Jnguyen. (5 de Junio de 2023). *Ransomware Attack- What is it and How Does it Work?* Obtenido de Check Point Software: https://www.checkpoint.com/es/cyber-hub/threat-prevention/ransomware/

Kodi. (s.f.). *Open source home theater software*. Obtenido de https://kodi.tv/

McAfee. (15 de Mayo de 2020). *¿Qué es el malware?* Obtenido de https://www.mcafee.com/es-mx/antivirus/malware.html

Microsoft. (s.f.). *¿Qué es el phishing? | Seguridad de Microsoft*. Obtenido de https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing

Microsoft. (s.f.). *¿Qué es SIEM? | Seguridad de Microsoft*. Obtenido de https://www.microsoft.com/es-mx/security/business/security-101/what-is-siem

Microsoft. (8 de Mayo de 2024). *Inyección de código SQL* . Obtenido de https://learn.microsoft.com/es-es/sql/relational-databases/security/sql-injection?view=sql-server-ver16

Microsoft Learn. (6 de Julio de 2023). *Recopilación de orígenes de datos de Syslog con el agente de Log Analytics*. Obtenido de https://learn.microsoft.com/es-es/azure/azure-monitor/agents/data-sources-syslog

Nagios Core. (6 de Marzo de 2024). *Installing Nagios Core from source*. Obtenido de https://support.nagios.com/kb/article/nagios-core-installing-nagios-core-from-source-96.html#Raspbian

Nagios Core. (s.f.). *Nagios Open Sourse*. Obtenido de https://www.nagios.org/projects/nagios-core/

Prometheus. (s.f.). *Prometheus - Monitoring system & time series database*. Obtenido de https://prometheus.io/

Raspberry Pi. (26 de Abril de 2022). *¿Que es Rasberry Pi?* Obtenido de https://raspberrypi.cl/que-es-raspberry/

Raspberry Pi. (1 de Julio de 2024). *Raspberry Pi 4 Modelo B / 8GB RAM* . Obtenido de https://raspberrypi.cl/producto/raspberry-pi-4-modelo-b-8gb-ram/

RedHat. (29 de Abril de 2022). *Las amenazas internas*. Obtenido de RedHat.com: https://www.redhat.com/es/topics/security/what-are-insider-threats

RedHat. (31 de Julio de 2023). *¿Qué es Linux?* . Obtenido de https://www.redhat.com/es/topics/linux

Santillán, L. F. (s.f.). *Sistema de Gestión y Capacitación*. Obtenido de https://www.educacioncontinua-abm.com.mx/sistema_lms/

Support, A. (26 de Junio de 2024). *rsyslog on AWS – Update an existing CloudFormation stack*. Obtenido de https://www.rsyslog.com/

Syslog- ng. (s.f.). *syslog-ng - Log Management Solutions*. Obtenido de https://www.syslog-ng.com/

TP- Link. (s.f.). *Switch para sobremesa con 8 puertos a 10/100/1000 Mbps*. Obtenido de https://www.tp-link.com/es/business-networking/unmanaged-switch/tl-sg108/

Zabbix. (23 de Julio de 2018). *The Enterprise-Class open source network monitoring Solution*. Obtenido de https://www.zabbix.com/

Anexo I

Nombre de dominio

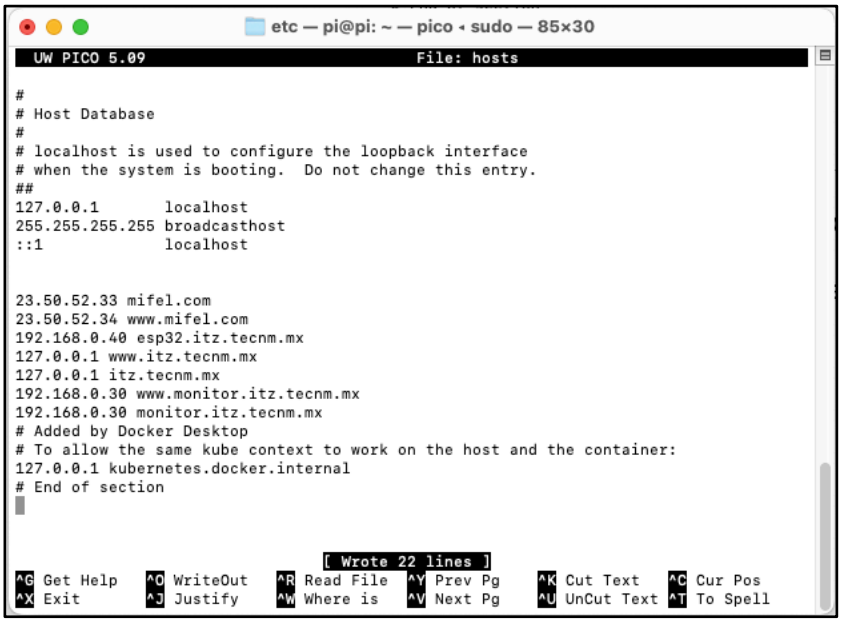
Ajuste de DNS local en máquina para resolución de nombres:

Tenemos que navegar hasta el siguiente directorio para el caso de Mac OS:

```
cd /private/etc/hosts
```

```
sudo nano hosts
```

Figura 39. Acceso a archivo de hosts en modo edición. Autor: Elaboración propia.



Nota. Archivo editado de hosts locales de resolución de DNS.

Se tiene que configurar de la siguiente manera para poder definir los registros:

```
IP_Address dominio.com
```

```
IP_Address www.dominio.com
```

Nuestros registros serían los siguientes:

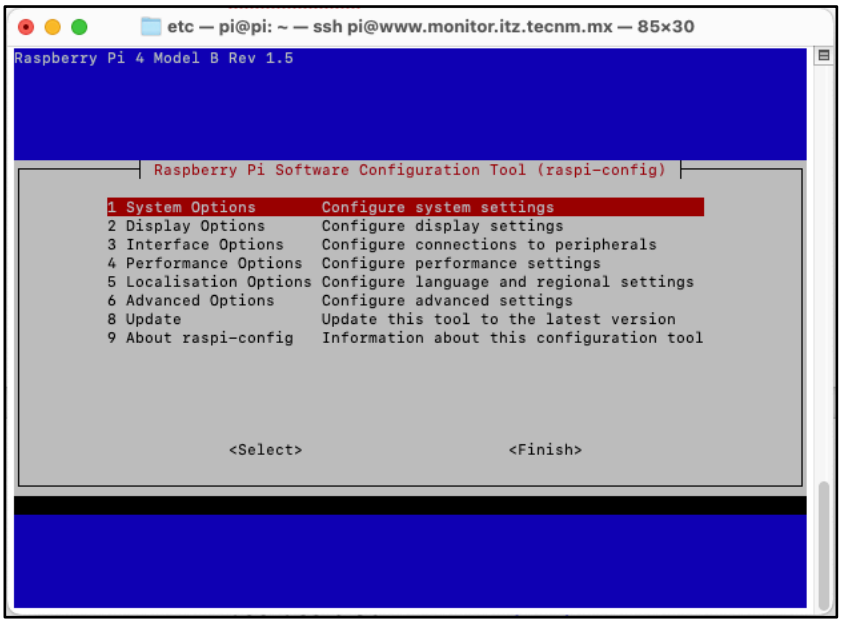
192.168.0.30 monitor.itz.tecnm.mx

192.168.0.30 www.monitor.itz.tecnm.mx

Activar VNC en Raspberry PI

Se ejecutan los comandos sudo raspi-config

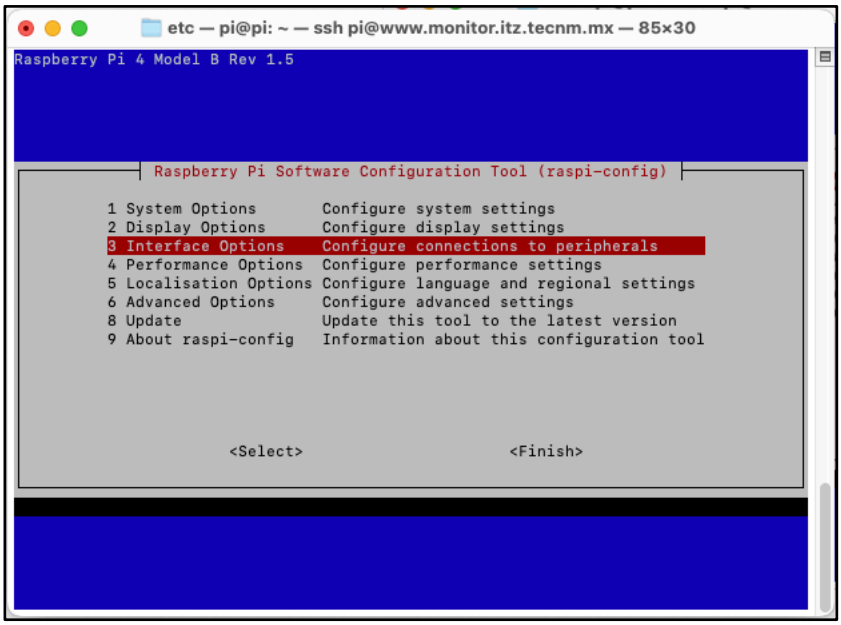
Figura 40. Raspberry PI en modo edición de servicios. Autor: Elaboración propia.



Nota. Menú de comando raspi-config.

Seleccionamos la opción 3 – Opciones de interfaz

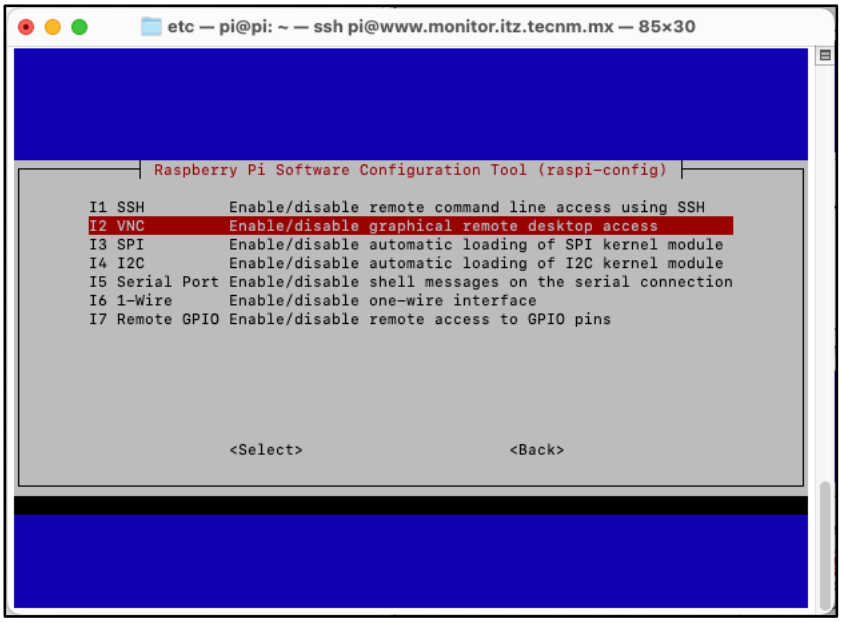
Figura 41. Raspberry PI opciones de interfaz. Autor: Elaboración propia.



Nota. Selección de opciones de interfaz.

Navegamos a la opción I2 VNC

Figura 42. Raspberry PI servicio de VNC. Autor: Elaboración propia.



Nota. Selección de opciones VNC.

Finalmente seleccionamos habilitar el acceso por VNC

Figura 43. Raspberry PI confirmación de activación de servicio VNC. Autor: Elaboración propia.

Nota. Confirmación de activación de servicio VNC.

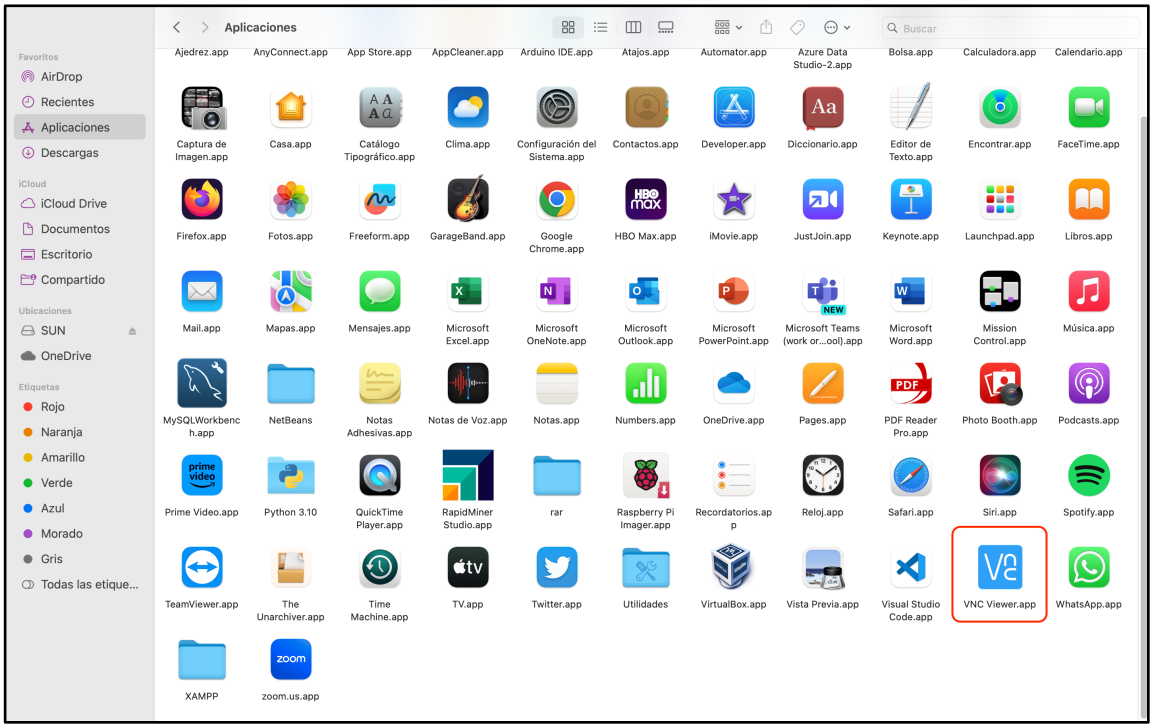
Pantalla de confirmación

Figura 44. Raspberry PI servicio activo VNC. Autor: Elaboración propia.

Nota. Confirmación de servicio VNC activo.

Desde la computadora cliente se debe descargar el cliente de VNC para poder acceder a la Raspberry Pi mediante interfaz grafica

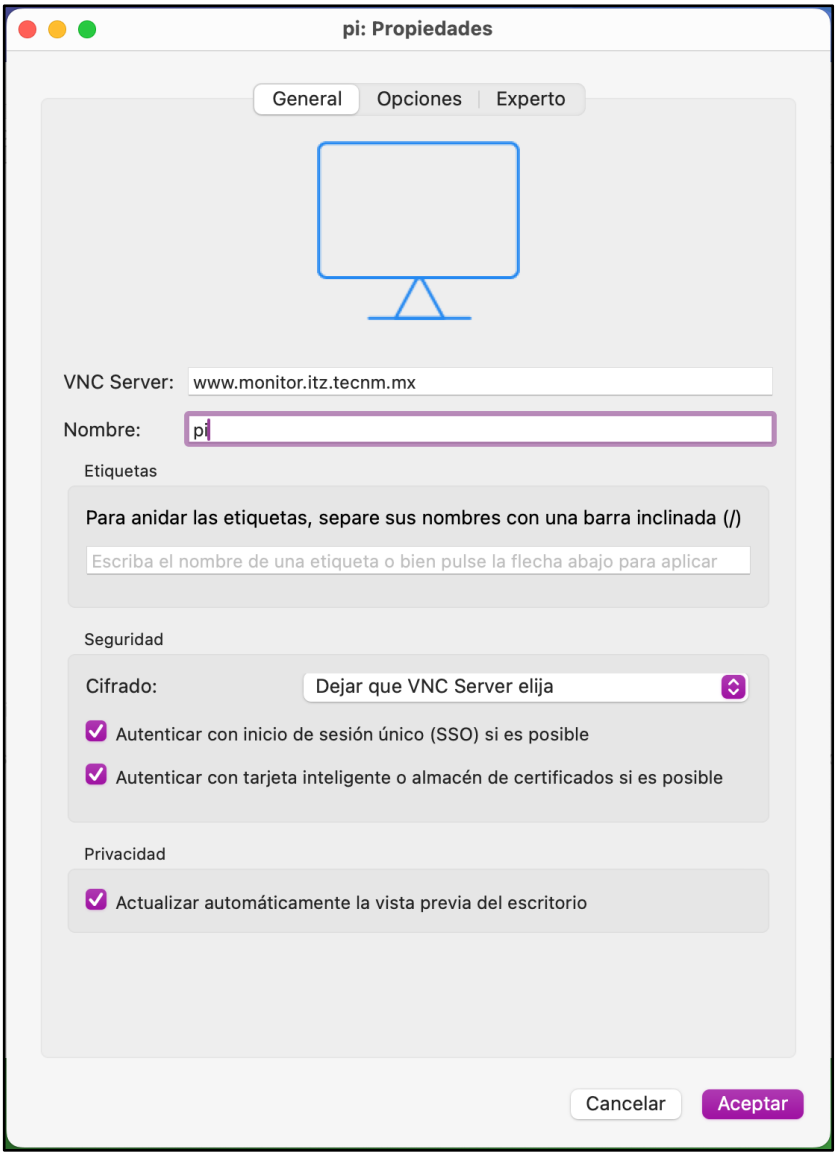
Figura 45. VNC viewer app. Autor: Elaboración propia.



Nota. Pantalla de aplicaciones activas en máquina de usuario.

Dentro de la aplicación tendremos que seleccionar Archivo->nueva conexión

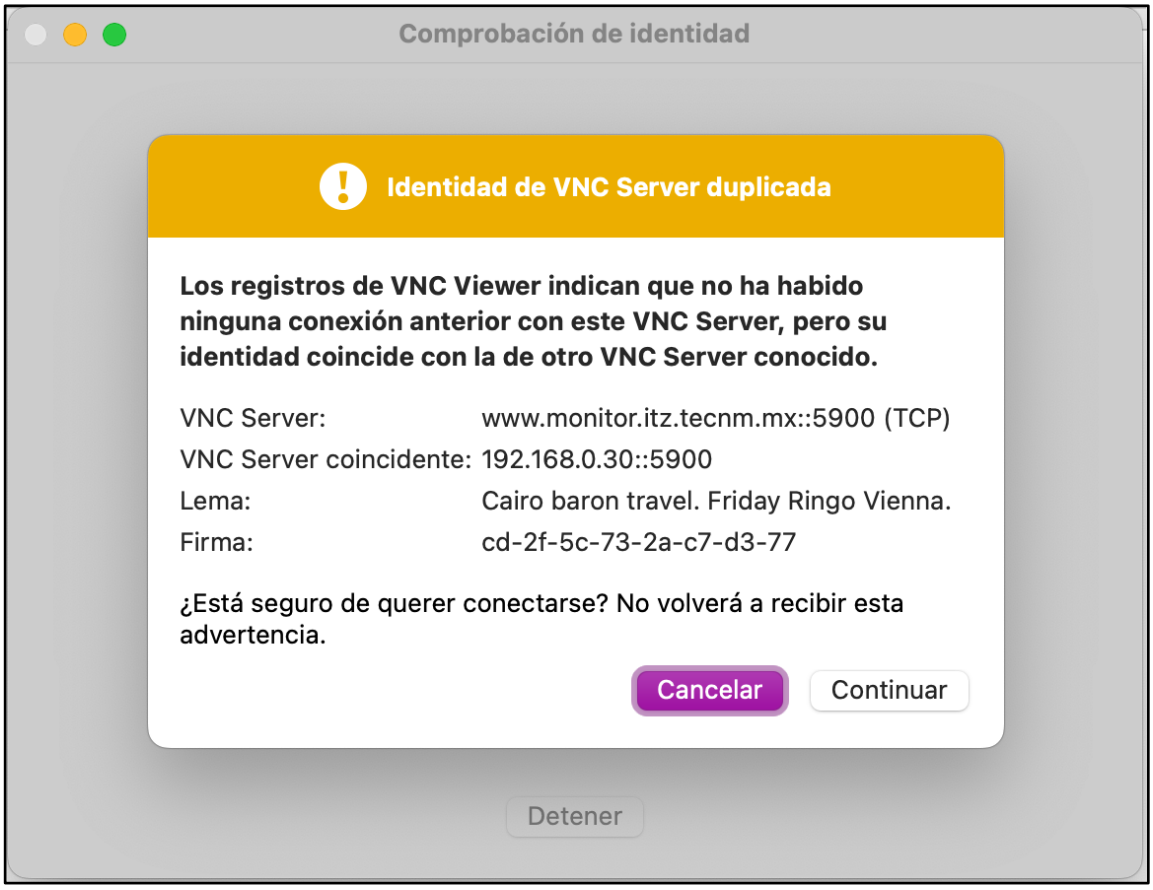
Figura 46. Pantalla de conexión inicial de VNC App. Autor: Elaboración propia.



Nota. Se debe establecer el FQDN o la dirección IP para realizar la conexión, el usuario debe ser el creado para acceder a la tarjeta Raspberry PI tipo Root.

Al continuar se mostrarán los datos de acceso como el servidor que corre el servicio de VNC, dirección IP y puerto de servicio (5900 por default)

Figura 47. confirmación de relación de confianza VNC x Raspberry PI. Autor: Elaboración propia.



Nota. Introducción de datos correctos, se recibe la confirmación para establecer la relación de confianza entre los dispositivos.

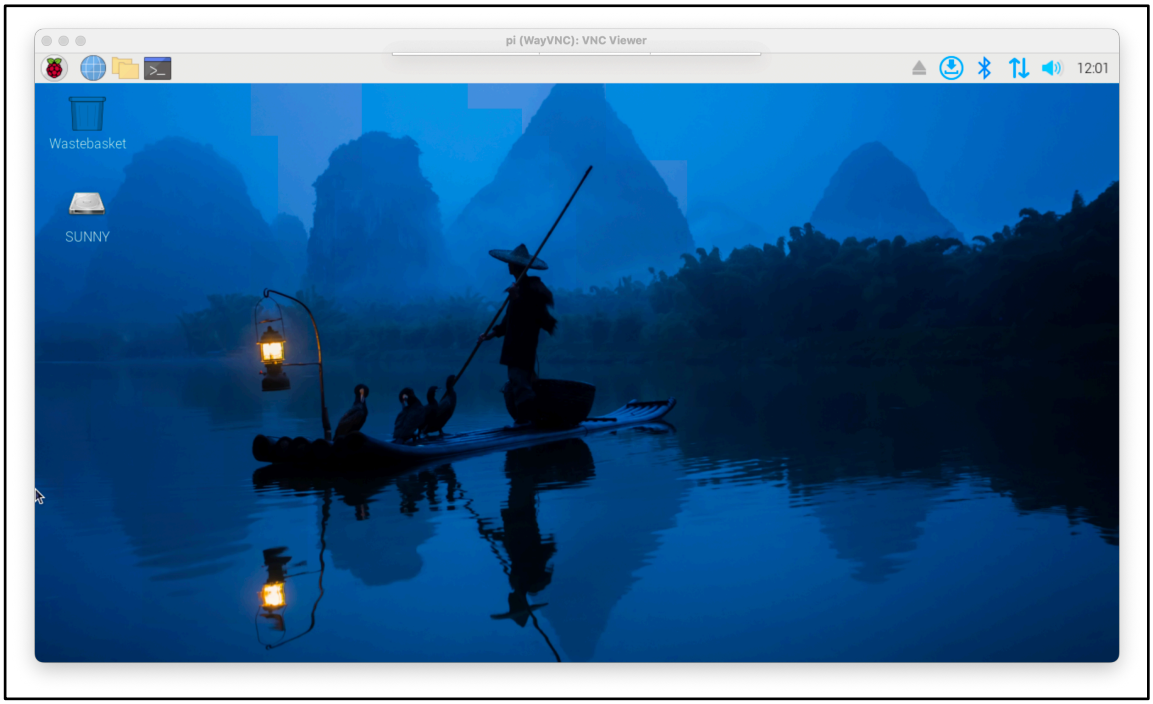
Posteriormente se pedirán los datos de conexión de un usuario valido dentro del servidor VNC Raspberry PI en nuestro caso usuario PI (default)

Figura 48. Solicitud de usuario y password de Raspberry PI (root user). Autor: Elaboración propia.

Nota. Introducción de datos de usuario root, por defecto se establece sobre el puerto 5900 de TCP.

Al concluir los pasos anteriores al presionar aceptar se mostrará la interfaz gráfica de la Raspberry PI

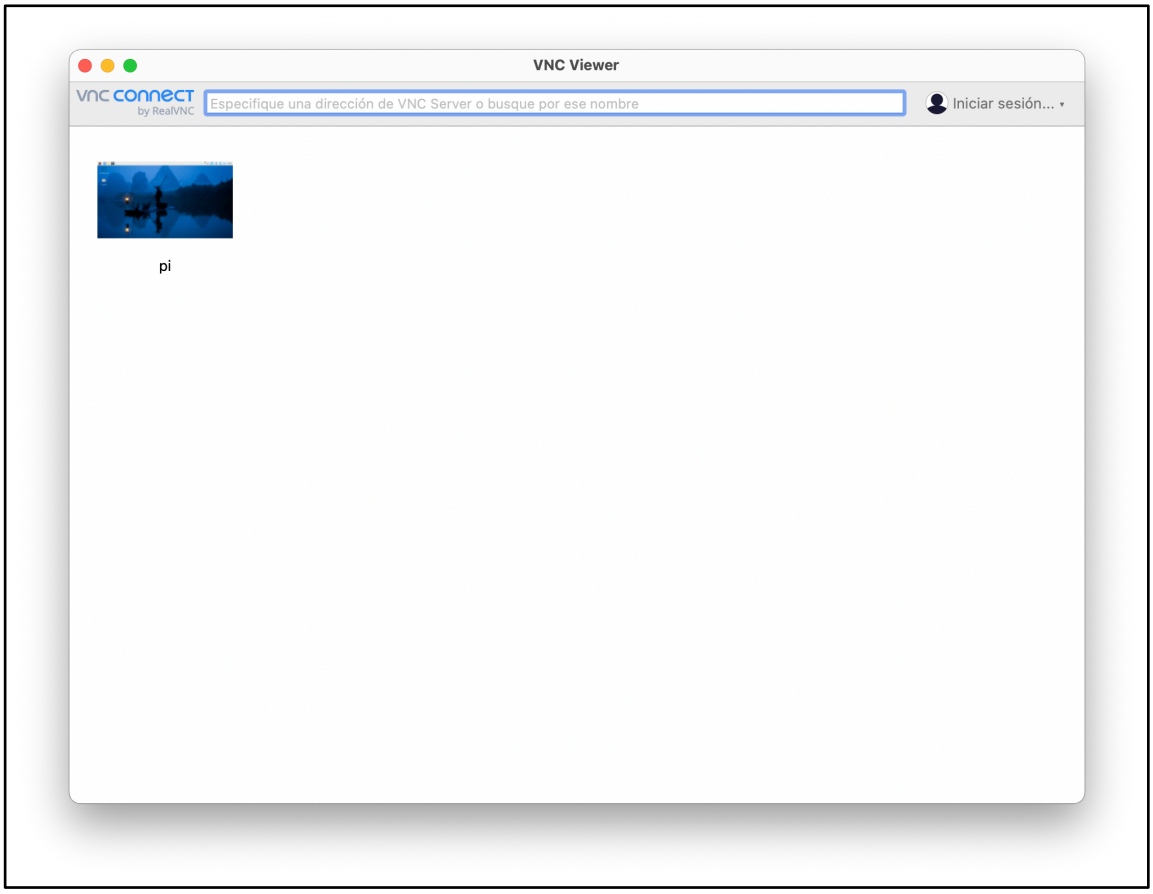
Figura 49. Escritorio de Raspberry PI (vista web). Autor: Elaboración propia.



Nota. Imagen de vista de interfaz web.

Por último, se estará guardando nuestra conexión de forma automática en el panel de navegación de la aplicación VNC para mayor comodidad de acceso

Figura 50. VNC connect. Autor: Elaboración propia.



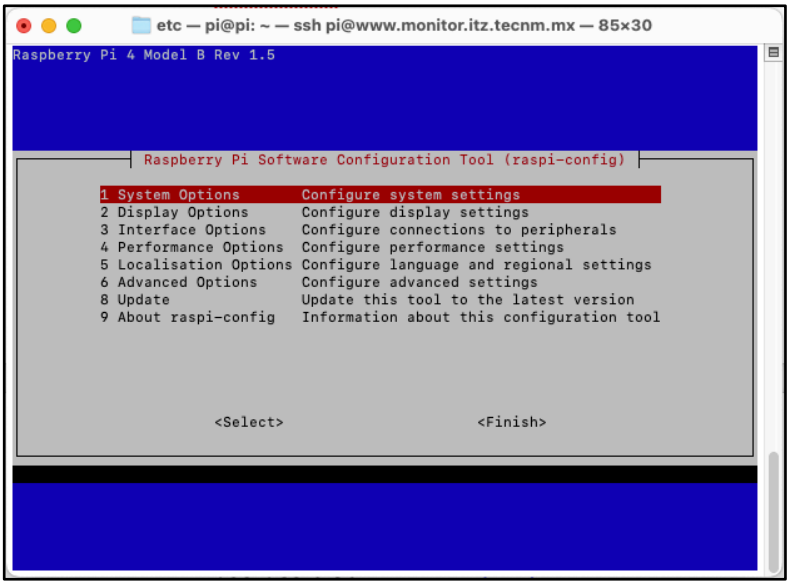
Nota. Conexiones de confianza guardadas en la interfaz web del cliente de VNC.

Activar servicio de SSH

Desde la terminal de nuestra Raspberry PI, ejecutamos el siguiente comando:

```
sudo raspi-config
```

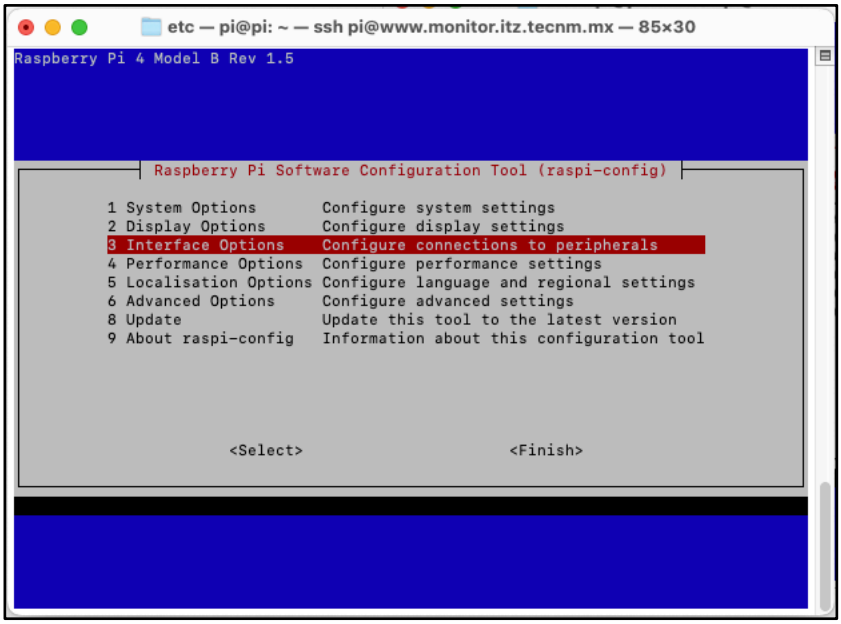
Figura 51. Pantalla de configuración de Raspberry PI. Autor: Elaboración propia.



Nota. Menú de opciones de configuración de Raspberry PI. Elaboración propia.

Seleccionamos la opción 3 – Opciones de interfaz

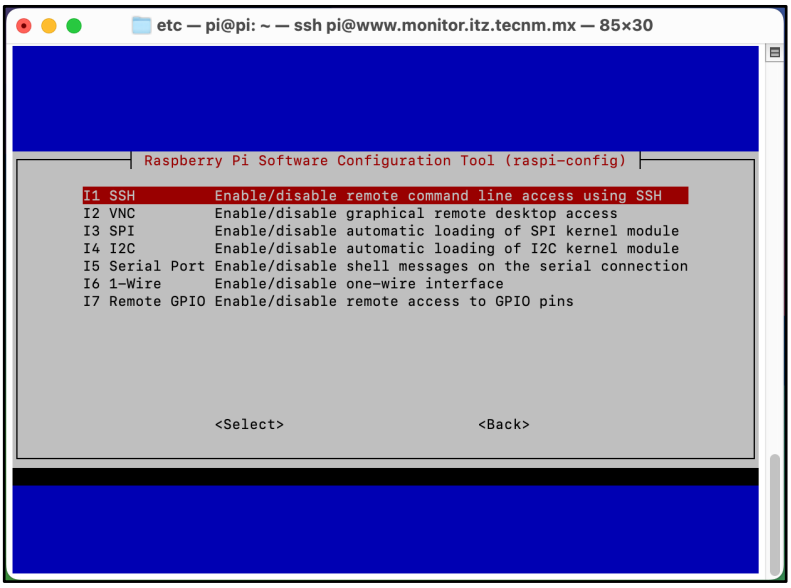
Figura 52. Pantalla de configuración de Raspberry PI (opción de interfaces). Autor: Elaboración propia.



Nota. SSH Raspberry PI opción de configuración de interfaces.

Se mostrará la opción de I1 SSH, seleccionamos

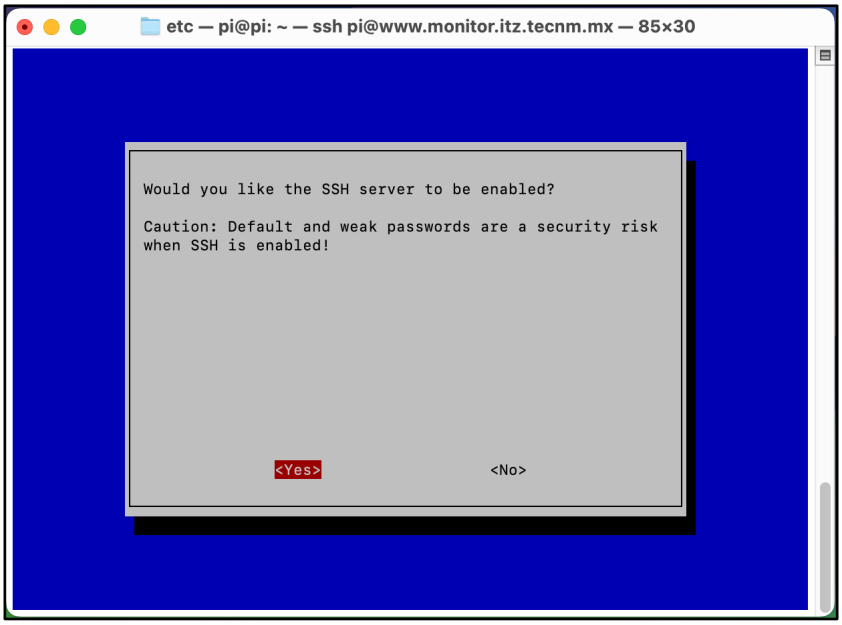
Figura 53. Pantalla de configuración de Raspberry PI (I1 SSH). Autor: Elaboración propia.



Nota. Menú de opciones de configuración de Raspberry PI (SSH).

Finalmente habilitamos la opción de habilitar el acceso por SSH (puerto 22 TCP) para cualquier origen perteneciente al mismo dominio de red.

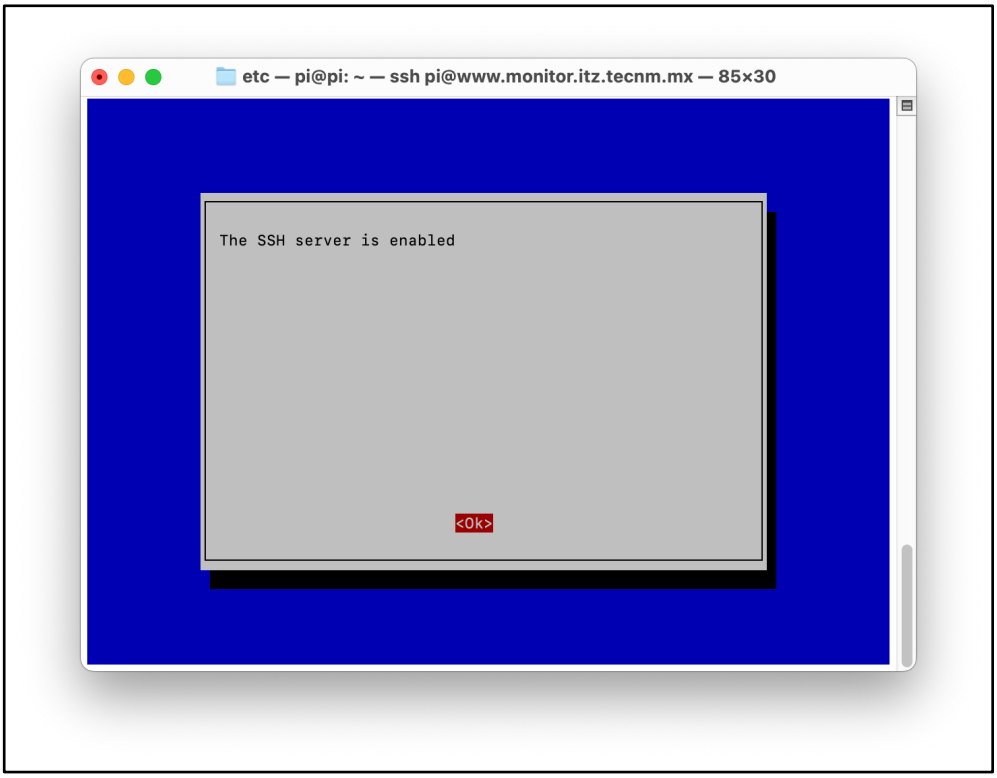
Figura 54. Pantalla de solicitud de confirmación de activación de servicio SSH. Autor: Elaboración propia.



Nota. Solicitará confirmación de activación de servicio SSH.

Por último, obtenemos la confirmación de SSH activo

Figura 55. Pantalla de confirmación de servicio SSH. Autor: Elaboración propia.

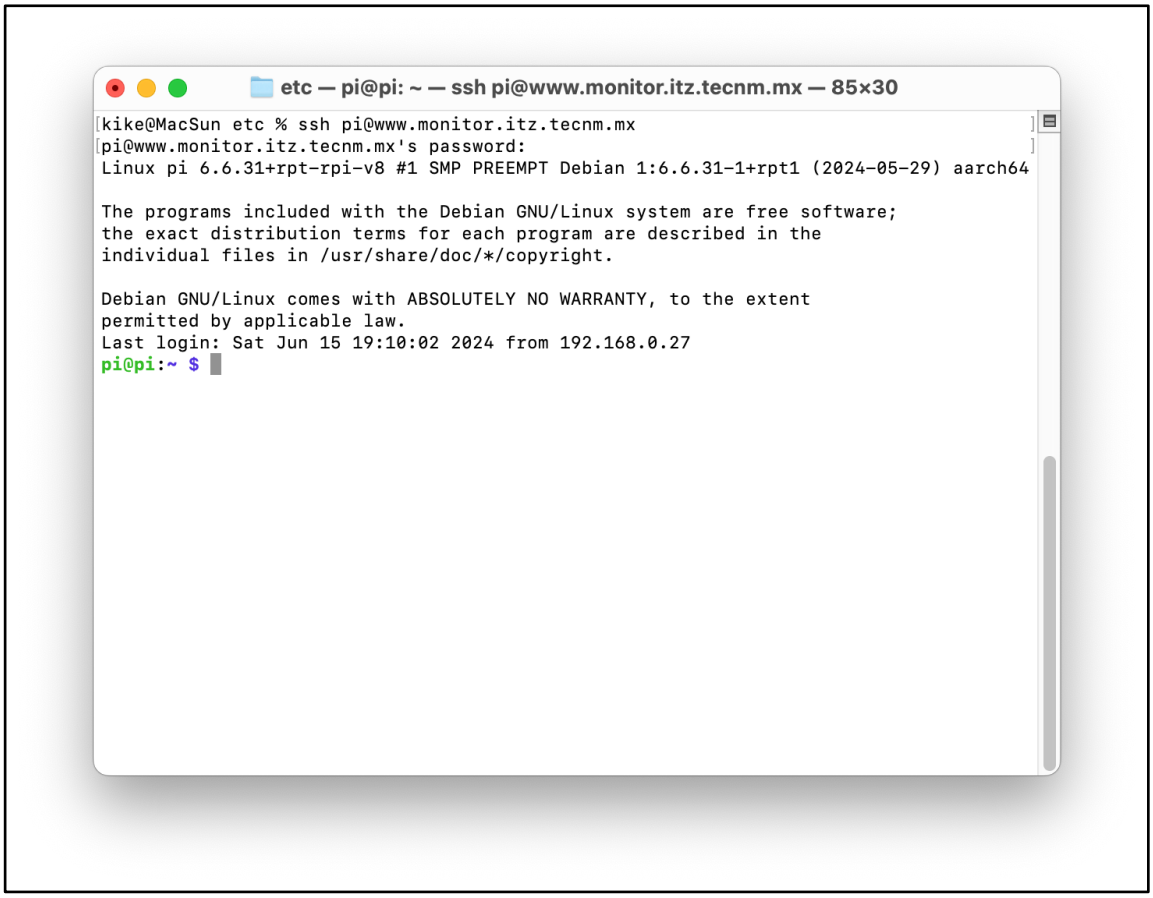


Nota. Confirmación de activación de servicio SSH.

Acceso por SSH desde terminal de maquina usuario, ejecutando el siguiente comando:

```
ssh pi@www.monitor.itz.tecnm.mx
```

Figura 56. Acceso a la Raspberry PI mediante SSH. Autor: Elaboración propia.



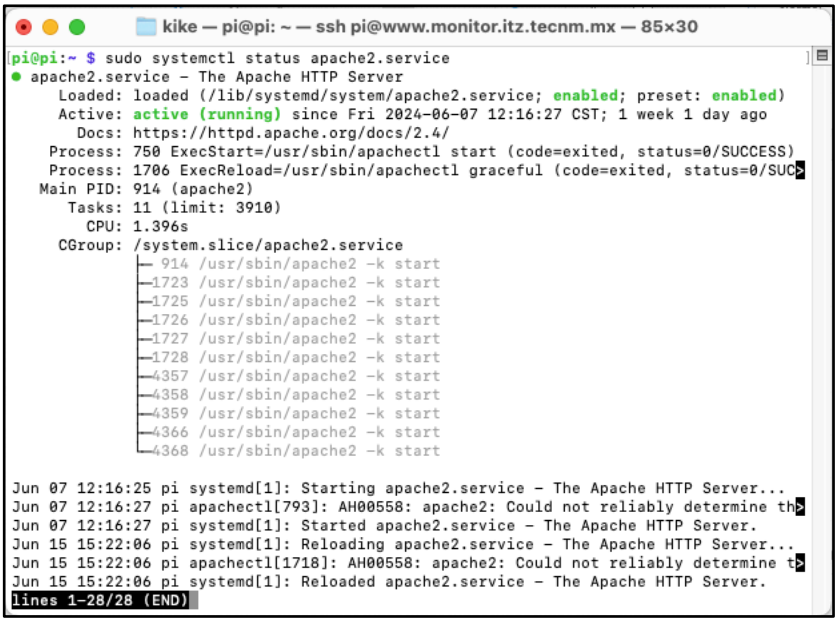
Nota. Acceso por la línea de comandos SSH puerto 22.

Revisión de servicios

Servicio de apache con el siguiente comando mediante terminal:

```
Sudo systemctl status apache2.service
```

Figura 57. Revisión de servicio apache mediante SSH. Autor: Elaboración propia.

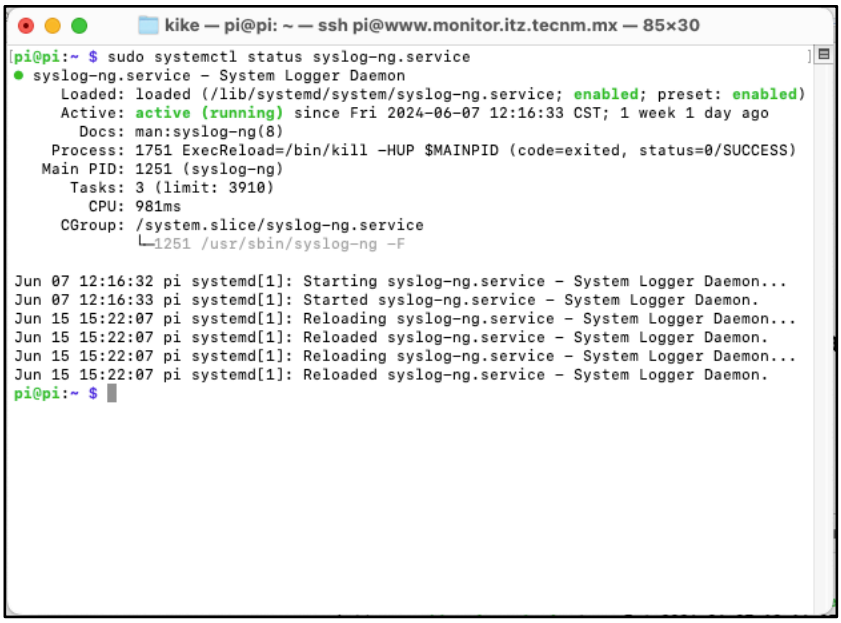


Nota. Revisión de estatus de servicio apache mediante SSH puerto 22.

Servicio de Syslog mediante el siguiente comando:

```
sudo systemctl status syslog-ng.service
```

Figura 58. Revisión de servicio syslog mediante SSH. Autor: Elaboración propia.



Nota. Revisión de estatus de servicio syslog mediante SSH puerto 22.

Configuración de gráficos en Nagios

Para configurar gráficas en Nagios Core, es común integrar una herramienta adicional que gestione la recopilación y visualización de datos de rendimiento. Una de las herramientas más utilizadas para este propósito es PNP4Nagios. A continuación, te guiaré a través de los pasos necesarios para instalar y configurar PNP4Nagios con Nagios Core.

Paso 1: Instalar Dependencias

Antes de instalar PNP4Nagios, asegúrate de que tienes las siguientes dependencias:

```
sudo apt-get update
```

```
sudo apt-get install apache2 php libapache2-mod-php rrdtool librrds-perl
```

Paso 2: Descargar e Instalar PNP4Nagios

```
cd /tmp
```

```
wget https://github.com/lingej/pnp4nagios/releases/download/v0.6.26/pnp4nagios-0.6.26.tar.gz
```

```
tar xzf pnp4nagios-0.6.26.tar.gz
```

```
cd pnp4nagios-0.6.26
```

Paso 3: Instalar PNP4Nagios:

```
bash
```

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

```
make all
```

```
sudo make install
```

```
sudo make install-webconf
```

```
sudo make install-config
```

```
sudo make install-init
```

Paso 4: Configurar Nagios Core para Usar PNP4Nagios

Editar la Configuración de Nagios:

Edita el archivo nagios.cfg para habilitar el procesamiento de datos de rendimiento.

```
bash
```

```
sudo nano /usr/local/nagios/etc/nagios.cfg
```

Asegúrate de que las siguientes líneas no están comentadas:

```
cfg
```

```
process_performance_data=1
```

Añade o modifica las siguientes líneas:

```
cfg

   service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata


service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::...

   service_perfdata_file_mode=a
```

```
   service_perfdata_file_processing_interval=15

   service_perfdata_file_processing_command=process-service-perfdata-
file

   host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata

   host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::...

   host_perfdata_file_mode=a

   host_perfdata_file_processing_interval=15

   host_perfdata_file_processing_command=process-host-perfdata-file
```

Paso 5: Definir los Comandos de Procesamiento de Datos:

Edita el archivo commands.cfg para definir los comandos que procesarán los datos de rendimiento.

```
bash
```

```
sudo nano /usr/local/nagios/etc/objects/commands.cfg
```

Añade las siguientes definiciones de comando:

```
cfg

   define command {

       command_name    process-service-perfdata-file

       command_line       /bin/mv  /usr/local/pnp4nagios/var/service-
perfdata /usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$

   }

define command {
```

```
        command_name    process-host-perfdata-file

        command_line    /bin/mv /usr/local/pnp4nagios/var/host-perfdata
/usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$

    }
```

Paso 6: Configurar PNP4Nagios

Edita el archivo `config.php` de PNP4Nagios:

```
bash
```

```
sudo nano /usr/local/pnp4nagios/etc/config.php
```

Asegúrate de que las siguientes líneas están configuradas correctamente:

```
php

$conf['nagios_base'] = '/nagios/cgi-bin';

$conf['rrdtool'] = '/usr/bin/rrdtool';

$conf['rrdtool_opts'] = '';
```

Paso7: Reiniciar los Servicios:

```
bash
```

```
sudo systemctl restart apache2
```

```
sudo systemctl restart nagios
```

```
sudo systemctl restart npcd
```

Paso 8: Verificar la Configuración

Generar Datos de Rendimiento

Provoca algunas verificaciones de servicios y hosts para asegurarte de que se generan datos de rendimiento.

Paso 9: Acceder a las Gráficas

Abre tu navegador y accede a la interfaz web de Nagios Core. Navega a un servicio o host y deberías ver enlaces a las gráficas generadas por PNP4Nagios.

```
http://<IP_PI>/pnp4nagios/
```

Siguiendo estos pasos, deberías poder configurar y visualizar gráficas en Nagios Core usando PNP4Nagios.

Configuración de alertas mediante correo electrónico en Nagios

Para configurar el envío de notificaciones a correo electrónico en Nagios Core, es necesario seguir los siguientes pasos:

Requisitos Previos

Postfix o Sendmail: Necesitarás tener un servidor de correo (Postfix, Sendmail, etc.) instalado y configurado en el mismo servidor que Nagios para enviar correos electrónicos.

Paso 1: Configuración del Servidor de Correo

Instalar Postfix:

```
bash
```

```
sudo apt-get update
```

```
sudo apt-get install postfix
```

Paso 2: Configurar Postfix

Durante la instalación, selecciona Internet Site y configura el nombre del sistema.

Paso 3: Configuración de Nagios Core

Edita el archivo commands.cfg para configurar el comando de notificación por correo electrónico.

```
bash
```

```
sudo nano /usr/local/nagios/etc/objects/commands.cfg
```

Añade o modifica el siguiente comando:

```
cfg

   define command{

       command_name    notify-host-by-email

       command_line    /usr/bin/printf "%b" "Notification Type:
$NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress:
$HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" |
/usr/bin/mail -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is
$HOSTSTATE$ **" $CONTACTEMAIL$

   }

   define command{

       command_name    notify-service-by-email

       command_line    /usr/bin/printf "%b" "Notification Type:
$NOTIFICATIONTYPE$\nService: $SERVICEDESC$\nHost:
$HOSTNAME$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
```

```
Info:\n\n$SERVICEOUTPUT$\n" | /usr/bin/mail -s "** $NOTIFICATIONTYPE$
Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **"
$CONTACTEMAIL$

   }
```

Paso 4: Configurar contactos

Edita el archivo contacts.cfg para definir los contactos que recibirán las notificaciones por correo electrónico.

```
sudo nano /usr/local/nagios/etc/objects/contacts.cfg
```

Configura el contacto como sigue:

```
cfg

   define contact{

      contact_name                    nagiosadmin

      use                             generic-contact

      alias                           Nagios Admin

      email                        isc.enrique.alanis@dominio.com

    }
```

Paso 5: Asignar contactos a hosts y servicios

Edita los archivos de configuración de hosts y servicios para asignar el contacto definido anteriormente.

Ejemplo en un archivo de configuración de un host:

```
cfg

   define host{
```

```
        use                     generic-host
        host_name               example-host
        alias                   Example Host
        address                 192.168.1.1
        contacts                nagiosadmin
        }
```

Ejemplo en un archivo de configuración de un servicio:

```
cfg
   define service{
        use                             generic-service
        host_name                       example-host
        service_description             HTTP
        check_command                   check_http
        contacts                        nagiosadmin
        }
```

Paso 6: Reiniciar Nagios

Guarda los cambios y reinicia el servicio de Nagios para aplicar la configuración.

```
bash
```

```
sudo systemctl restart nagios
```

Paso 7: Verificación

Generar una alerta:

Provoca una alerta en uno de los servicios o hosts configurados para asegurarte de que se envíen las notificaciones por correo electrónico.

Revisar el correo:

Verifica que el correo electrónico haya sido recibido en la bandeja de entrada del contacto configurado.

Con lo anterior, deberíamos poder configurar Nagios Core para enviar notificaciones por correo electrónico correctamente.