Universidad Inca Garcilaso de la Vega

FACULTAD DE INGENIERIA DE SISTEMAS, COMPUTO Y TELECOMUNICACIONES

Sistema de monitoreo para mejorar la oportuna atención de incidentes que presenten los dispositivos de una red, utilizando protocolo SNMP.

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Ingeniero de Sistemas y Cómputo

AUTOR

Garcia Mena, Carlos Eduardo

(https://orcid.org/0009-0001-9298-4566)

ASESOR

Mg. Muñoz Muñoz, Ricardo

(https://orcid.org/0000-0002-1768-0650)

Lima, Octubre 2023

Turnitin TSP Garcia Mena

INFORME DE ORIGINALIDAD

19%	18%	1%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	Submitted to Universidad Inca Garcilaso de la Vega Trabajo del estudiante	2%
3	repositorio.uigv.edu.pe Fuente de Internet	2%
4	www.cisco.com Fuente de Internet	1%
5	www.coursehero.com Fuente de Internet	1%
6	bibdigital.epn.edu.ec Fuente de Internet	<1%
7	repositorio.uta.edu.ec Fuente de Internet	<1%
8	Submitted to Universidad Privada Antenor Orrego Trabajo del estudiante	<1%

DEDICATORIA

Este trabajo de suficiencia profesional está dedicado, a Dios agradeciéndole por todas las bendiciones que he recibido; a mi padre que me iluminó y cuidó desde el cielo; a mi pareja por su apoyo inquebrantable.

AGRADECIMIENTO

Agradezco a la Oficina de Grados y Títulos de la Universidad Inca Garcilaso de la Vega por promover la oportunidad de titulación mediante esta modalidad de trabajo de suficiencia.

Mi agradecimiento especial a mi asesor Mg. Ricardo Muñoz, quien constantemente me brindó su apoyo con su guía, sabia orientación y consejos durante el desarrollo del presente trabajo.

Finalmente, mi total gratitud hacia mis seres queridos, que son personas importantes que le dan valor a mi vida. Su apoyo incondicional ha sido fundamental para lograr mis metas académicas y profesionales

RESUMEN Y PALABRAS CLAVE

El presente trabajo proporcionará una descripción teórica de cómo funciona el protocolo SNMP, incluida información sobre cómo utilizar la herramienta de monitoreo de software gratuito, su proceso de instalación y despliegue en la gestión de impresoras de una institución estatal. Un sistema de monitoreo completo es esencial para las empresas de tecnología en el mercado actual, ya que puede mejorar el valor de un producto o servicio para el cliente y permitir el funcionamiento eficiente de los dispositivos o servicios. Los consumidores exigen más de sus productos a medida que aumenta la competencia y la variedad. Por las razones anteriores, establece la necesidad de crear un sistema de monitoreo de dispositivos tecnológicos mediante protocolo SNMP y software libre, con el objetivo de verificar continuamente la funcionalidad de los elementos de la red y fiscalizar los dispositivos internos y externos dentro de la empresa. Los resultados reflejan que, con el presente sistema de gestión y monitoreo, ha mejorado considerablemente la atención de incidentes que presentaron en una red, ofreciendo así valor agregado que maximizó la eficiencia de los dispositivos y servicios. El presente trabajo reflejará como el sistema de monitoreo introduce enfoques orientados al servicio basados en principios proactivos, pues va a permitir que los técnicos reciban notificaciones por correo electrónico sobre eventos del dispositivo, mal funcionamiento del sistema entre otros tipos de incidentes de una red.

Palabras clave: Monitoreo, incidentes, SNMP, interfaz, impresoras

ABSTRACT

The present work will provide a theoretical description of how the SNMP protocol works, including information on how to use the free software monitoring tool, its installation process and deployment in the printer management of a state institution. A comprehensive monitoring system is essential for technology companies in today's market as it can improve the value of a product or service to the customer and enable efficient operation of devices or services. Consumers demand more from their products as competition and variety increase. Due to the above, the need arises to create a monitoring system for technological devices using the SNMP protocol and free software, with the objective of continually verifying the functionality of the network elements and supervising internal and external devices within the company. The results reflect that, with the present management and monitoring system, the attention to incidents that occurred on a network has considerably improved, thus offering added value that maximized the efficiency of the devices and services. This work will reflect how the monitoring system introduces a proactive service model instead of a reactive one, as it will allow technicians to receive email notifications about device events, system malfunctions, among other types of network incidents.

Keywords: Monitoring, incidents, SNMP, interface, printers

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad, la gestión remota de impresoras y equipos multifunción es una opción más asequible en entornos de oficina en red. Las métricas de los dispositivos se pueden capturar utilizando sofisticadas herramientas de software que aprovechan la World Wide Web. Los proveedores de servicios pueden monitorear el desempeño de una flota en tiempo real a través de una computadora portátil o una estación de trabajo, tanto en casa como en el extranjero. Esto es ventajoso, puesto que, el uso de datos de uso de flujo continuo es un método confiable para maximizar el tiempo de actividad de la flota y mejorar drásticamente la productividad del grupo de trabajo. Además, el reporte obtenido de las métricas de los dispositivos permite a los distribuidores de servicios abordar rápidamente los requisitos tecnológicos actuales y futuros de sus clientes.

El presente trabajo se desarrolla en 04 capítulos. En el capitulo1 se describe el marco teórico del trabajo con la finalidad de conocer el funcionamiento del protocolo SNMP y el proceso de gestionar dispositivos de una red. En el capítulo 2 se entra en la problemática de las instituciones públicas y privadas, se determina casusas a través de un diagrama de Ishikawa y luego se trazan los objetivos generales y específicos. En el capítulo 3 presento la justificación, importancia y delimitación del estudio. En el capítulo 4 se desarrolla la metodología y diseño esquemático del sistema de monitoreo para lograr los objetivos propuestos. En el capítulo 5 se desarrolla la implementación y despliegue del sistema evidenciando el cumplimiento de los objetivos trazados.

CAPÍTULO 1: MARCO TEORICO DE LA INVESTIGACION

1.1 Marco histórico

A fines de la década de 1980, se inició la aparición del software de administración de redes. Su función principal es permitir que los ingenieros de TI respondan rápidamente a los eventos, detecten redes en problemas y analicen los esquemas de tráfico de la red en busca de comportamiento.

Simple Network Management Protocol (SNMP) se creó como un medio para administrar y monitorear la red sin consumir ancho de banda. Esto se conoce como método de gestión simple. El protocolo SNMP experimentó una evolución en 1996, lo que llevó a la creación de SNMP V2 usando RFC 1901 y reemplazando las trampas de la versión original con mejoras de seguridad y un formato de mensaje diferente.

El software de gestión de redes ha ido evolucionando junto con la introducción de los protocolos Flow. A pesar de haber sido creado por CISCO en 1995, el software NETFLOW se introdujo para uso LAN debido a sus problemas de uso de alto ancho de banda. Es por eso que se considera el primer enfoque exitoso. Para capturar flujos con mayor ancho de banda, NETFLOW.V1 se introdujo por primera vez como hardware en los enrutadores CISCO en 1996 para abordar el problema principal.

SNMP y NETFLOW brindan dos métodos distintos para monitorear redes, dado que ninguno de los protocolos se creó simultáneamente y no estaban destinados a funcionar de manera aislada. El uso de SNMP se justifica dónde está, gracias a su amplia personalización para proveedores, tipologías en tiempo real y bajo uso de recursos (principalmente usando versiones anteriores del protocolo SSMP, como aquellas sin autenticación y encriptación).

Antes del uso extendido de Internet, los equipos de vigilancia eran una propuesta costosa; cada dispositivo y su propio software de servidor necesitaban su propia línea telefónica. En el siglo XXI, las soluciones basadas en la nube excluyen la necesidad de costosas instalaciones in situ al compartir recursos "bajo demanda" a través de Internet.

Hoy en día, muchas personas utilizan sistemas basados en la nube como Dropbox, Google Drive y Apple iCloud para gestionar su información personal y financiera; todos ellos son fiables, versátiles y seguros. El acceso a valiosos activos de información en

cualquier momento es posible a través de servicios de almacenamiento e intercambio de archivos.

En mayo de 1998, Hewlett-Packard (HP) anunció una actualización de su solución de administración de impresión en web JETADMIN. Con esta solución, los administradores de LAN pueden instalar, administrar y monitorear periféricos conectados a la red a través de una interfaz de navegador. La solución Web JetAdmin permite que cualquier usuario acceda a la intranet y administre los periféricos conectados a la red desde cualquier lugar de la intranet.

En noviembre de 2010, Lexmark Corporation lanzó MARKVISION ENTERPRISE, la próxima generación de software de administración de dispositivos diseñada para ayudar a las empresas a disminuir el tiempo de inactividad así como los costos mediante la administración estratégica de su entorno de impresión.

En diciembre de 2015, Americal Perú compró las herramientas de OPMANAGER para el monitoreo de la red central, dado que el módulo de monitoreo del tráfico de red de OpManager puede brindar una descripción general de los modelos de tráfico de red y el consumo de ancho de banda, incluidos NetFlow, j-Flow, IPFIX, sFlow, etc.

En 2019, Kyocera lanzó una herramienta de administración remota llamada KFS (Flota de Servicios de Kyocera), que está basada en la nube y alojada por Microsoft. Esta herramienta maximiza el potencial de mantenimiento de su flota de equipos. Permite a los proveedores de servicios ver el estado del equipo e identificar y responder rápida y fácilmente a los problemas.

En América Latina, el control remoto de impresoras y dispositivos multifunción (MFP) es más rentable que nunca. Existen algunas herramientas de software avanzadas que utilizan la World Wide Web para obtener métricas de dispositivos. Con una computadora portátil o una estación de trabajo, los proveedores de servicios pueden observar en tiempo real el rendimiento de su flota a nivel local y global.

1.2 Bases teóricas

Gestión de Incidentes.

La gestión de incidentes de seguridad es un proceso que implica identificar, administrar, registrar y analizar los incidentes o amenazas de seguridad ocurridos en una organización. El propósito de este enfoque es proporcionar una perspectiva integral y sólida sobre cualquier desafío de seguridad de la información dentro del dominio tecnológico. (Ciberseguridad Chihuahua, s.f.)

Monitoreo de red

El monitoreo de red es el proceso de recopilar, analizar y procesar paquetes de datos enviados o recibidos en una red informática. Estos paquetes se pueden analizar considerando varias métricas, como el consumo de ancho de banda, el total de desconexiones y la tasa de pérdida de paquetes (Cisco, s.f.)

El software de monitoreo de red se maneja para recopilar información de la red, monitorear y analizar el rendimiento de la red. Puede ser utilizado para una diversidad de propósitos, como:

- Gestión del rendimiento de la red de información.
- Más información sobre problemas de rendimiento.
- Notificar al personal de red del problema
- Ayudar en el diagnóstico y resolución de problemas

Tipos de protocolos de monitoreo de red

A. SNMP:

   El Protocolo simple de administración de redes es un protocolo de capa de aplicaciones que emplea un sistema de llamada y respuesta para cotejar los estados de varios tipos de dispositivos, desde switches hasta impresoras. SNMP se puede utilizar para monitorear el estado y la configuración de los sistemas.

B. ICMP:

Los dispositivos de red, como los servidores y routers, utilizan el Protocolo de mensajes de revisión de Internet para el envío de información de operaciones por IP y para alertar mediante mensajes algunas fallas de dispositivos.

C. Protocolo de detección de Cisco:

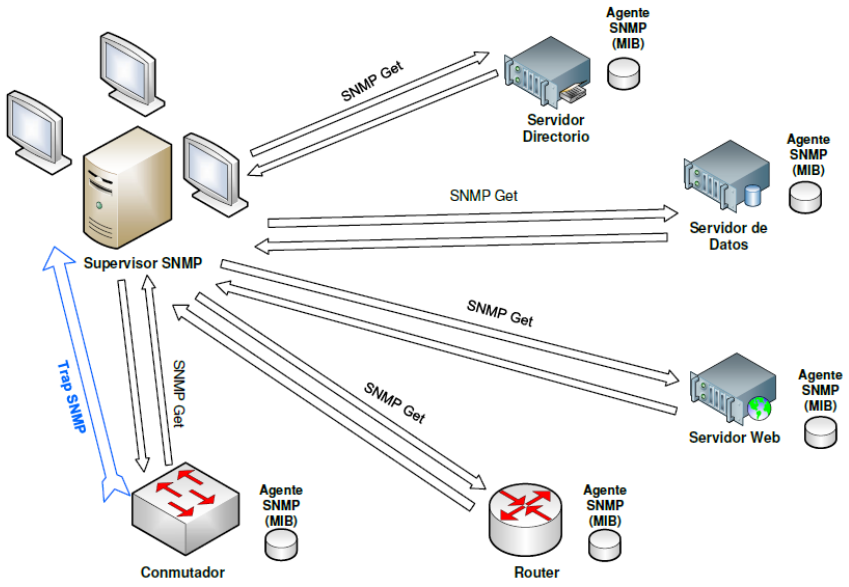
Cisco Discovery Protocol proporciona la administración de dispositivos de Cisco al establecer la identificación de dispositivos, establecer su configuración y permitir que los sistemas utilicen diversos protocolos de capa de red para intercambiar información entre sí. (Ciberseguridad Chihuahua, s.f.)

SNMP a fondo:

RFC1157 define SNMP como un protocolo de capa de aplicación, que permite el intercambio de información de gestión entre dispositivos de red, de manera fácil. Es un componente de la familia de protocolos TCP/IP.

SNMP es uno de los protocolos más utilizados para administrar y monitorear componentes de red. El agente SNMP se incluye con la mayor parte de los elementos de red a nivel profesional. Estos agentes deben estar configurados para comunicarse con el sistema de gestión de red (NMS) a través de la activación y configuración.

Figura 1. Funcionamiento del protocolo SNMP



Nota. La Figura 1 muestra el funcionamiento del protocolo SNMP por sondeo (poling) pregunta – respuesta a través de un comando Get.

Agente SNMP

El componente de red contiene un programa conocido como agente. Si el agente está habilitado, la base de datos de información de gestión de dispositivos se puede recopilar localmente y ponerse a disposición del administrador de SNMP a pedido. Estos agentes vienen en una variedad de formas, incluidas el estándar como Net SNMP y las de proveedores como HP Information Agent. (Digital Guide IONOS, 2019)

Características clave del agente SNMP:

- Obtenga información de gestión a nivel local sobre su área.
- Mantiene y accede a la información de administración como se describe en la MIB.
- Reportar una ocurrencia al administrador.
- Funciona como sustituto de determinados nodos de red independientes de SNMP que no están gestionados.

Arquitectura de SNMP

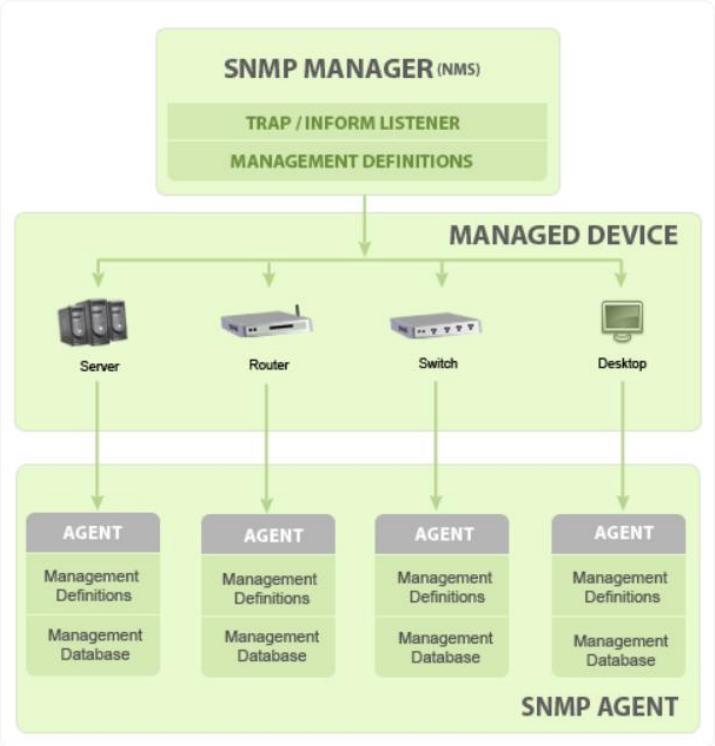
El sistema SNMP es un conjunto de estaciones que gestionan los componentes de la red. Una estación de administración realiza un seguimiento de los elementos de la red mediante la ejecución de aplicaciones de administración.

Elementos de red como enrutadores, computadoras y servidores que tienen agentes de administración que realizan las tareas de administración solicitadas en la red por las estaciones de administración de red. (Digital Guide IONOS, 2019)

La MIB local de cada dispositivo es responsable de administrar la información en forma emparejada, como el valor del atributo. Todas las herramientas de gestión y seguimiento poseen este tipo de información.

SNMP facilita la comunicación entre los administradores de monitoreo y los dispositivos de red dentro de la infraestructura de la empresa.

Figura 2: Diagrama básico de comunicación de SNMP



Nota. La Figura 2 muestra el Diagrama básico de comunicación de SNMP

Comandos básicos del SNMP

La facilidad con la que pueden ocurrir los intercambios de información ha hecho de SNMP un protocolo ampliamente aceptado. La razón clave es una breve lista de comandos:

- GET: El dispositivo administrado recibe una solicitud del administrador a través de la operación GET. Se logra recuperar uno o más valores del dispositivo administrado.
- GET NEXT: Similar a GET, se ejecuta la siguiente operación obtenida. GET NEXT es el método utilizado para obtener el valor de un OID en el árbol MIB, que es bastante distinto.
- GETBULK.: Se puede acceder a los datos de una tabla MIB grande mediante la operación GETBULK.
- SET: Los administradores usan SET para cambiar o asignar el valor del dispositivo.

- TRAPS: Los agentes inician TRAPS, en lugar de los comandos anteriores que emitía el administrador de SNMP. El agente envía una notificación sobre el evento al administrador de SNMP.
- INFORM es comparable al TRAP iniciado por el Agente, pero con la característica adicional de recibir confirmación de un Administrador SNMP automatizado. El proceso sigue este método.
- RESPONSE: Las acciones del administrador de SNMP se devuelven mediante este comando para devolverle el valor o la señal.

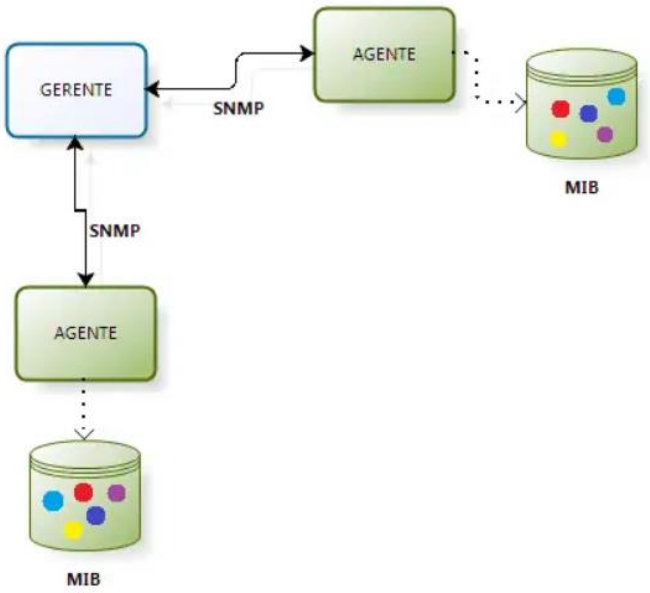
El papel de las trampas SNMP.

Un agente puede enviar un mensaje SNMP no solicitado al administrador NSMP correspondiente para notificarle eventos significativos, que luego son trampas. Los protocolos de captura SNMP comprenden el valor actual de sysUpTime, un OID que especifica el tipo de captura y variables de vinculación opcionales. El direccionamiento de destino de las trampas SNMP es específico para cada aplicación y, por lo general, lo determinan las variables de configuración de trampas en la MIB. Se cambió el nombre de las unidades de datos del protocolo a SNMPv2 Trap y el formato de los mensajes de trampa se modificó en la versión 2.

Ventajas del SNMP. (Telco Manager, 2022)

- El protocolo de capa siete proporciona una mayor abstracción de las otras capas de la red. Esta es una ventaja significativa.
- También permite al administrador controlar un dispositivo fuera de su red doméstica.
- Su bajo consumo de recursos de red y procesamiento le permitió extenderse, dando como resultado su aplicación en dispositivos relativamente simples como impresoras.
- SNMP ayuda a los administradores de red a identificar posibles dificultades y errores en su red. Mediante el uso de un administrador SNMP como SLAview, es posible mostrar gráficos que detallan estadísticas de tráfico, niveles de tóner en las impresoras, uso de CPU y memoria, y la cantidad de procesos en ejecución en un dispositivo específico.

Figura 3. Modelo de Gestión del SMNP.



Nota. La figura 3 muestra la estructura de todos los dispositivos que deban etiquetarse deben tener un agente SNMP junto con el administrador SNMP. El gerente enviará las solicitudes al agente, quien luego regresará con la información.

1.3 Antecedentes del estudio

Acuña García, Edith & Caicedo Urresta, Verónica (2005) *Gestión de redes de un centro de cómputo utilizando protocolo SNMP/RMON* (Tesis de Grado en Ingeniería de Sistemas) Universidad Técnica de Ambato – Ecuador. Concluye que al estudiar varias herramientas para el monitoreo de red en centros de cómputo orientado al protocolo SNMP/RMON, el instrumento elegido fue PATROL DashBoard porque facilita la ordenación de los perfiles de los usuarios, optimizando y centralizando así la información recopilada por todos los usuarios de manera confidencial, permite a los usuarios calcular la cantidad de servicio que reciben debido a su interfaz basada en Web-Browser. El software genera sus propios informes y tendencias, alertas, estadísticas y eventos de red son parte del trabajo. Además, recoge e improvisa los datos generados y transmitidos. Patrol DashBoard ofrece los protocolos necesarios clasificando las alertas según las responsabilidades del perfil de cada usuario. Acuña señala que la gestión de la red es un problema persistente que no puede resolverse con herramientas debido a la ausencia de procedimientos específicos o personal calificado.

Ramos et al (2011) *Monitoreo de impresoras multifuncionales con protocolo SNMP* (Tesina de Grado en Ingeniería de Comunicaciones y Electrónica) Escuela Superior de Ingeniería Mecánica de Culhuacán- México. Indica que la implementación de la red garantiza que los servicios estén siempre disponibles, lo que mejora la satisfacción financiera del cliente y del negocio, lo que convierte a la empresa en un proveedor de servicios con un retorno de la inversión del 99.99 %. La herramienta ASG SENTRY monitorea los recursos de equipos en diferentes sistemas operativos, observa el estado de la red en un tiempo real a través de su interfaz web, esto permite generar gráficas e informes de comportamientos. También contiene información del cliente como nombre, descripción y dominio asociado; uno o más objetivos de nivel de servicio para identificar tendencias en vulnerabilidades o infracciones; crear varios servicios internos y externos que ayudan a obtener una imagen completa de los servicios prestados al cliente.

Ibarra Zuleta, Edwin Fernando (2000). *Desarrollo de software para implementar un sistema supervisor computarizado de monitoreo y control de impresoras de inyección de tinta a chorro marca Domino* (Proyecto previo para Título de Ingeniero en Electrónica y control) Escuela Politécnica Nacional de Quito – Ecuador. Señala que el programa de aplicación está desarrollado para corresponder completamente a las tareas establecidas. Si bien el terminal de programación portátil puede realizar todas sus funciones, el software puede asumir esa función. Los usuarios deben tener conocimiento de cómo funcionan estas impresoras de inyección de tinta para comprender su función al ejecutar el comando. La herramienta prepara el escenario para otros avances que facilitan la disponibilidad de aplicaciones nuevas e inventivas para impresoras de inyección de tinta. El usuario puede manipular el puerto y los métodos de impresión controlados por otros dispositivos electrónicos utilizando el programa, con algunas modificaciones. Por lo tanto, tener conocimiento de este software permite desarrollar programas comparables para diseños de impresoras mejorados.

La mayoría de los comandos descritos en el protocolo probado necesitan enviar la respuesta adecuada a la impresora y leerla desde allí, lo que limitaría la velocidad de ejecución ya que estará controlada principalmente por la velocidad de la conexión de comunicación entre la computadora y la impresora.

Oré Alvaro, Cristian (2019) *Implementación de un sistema de monitoreo para asegurar la continuidad de los servicios en un data center utilizando protocolo SNMP*. (Para obtener el Título Profesional de Ingeniero de Sistemas e Informática) Universidad Tecnológica del Perú – Perú. Señala que su trabajo se basó en la urgente necesidad de contar con un sistema de monitoreo para todo el departamento del Data Center en la empresa Netsecure Perú dado que la empresa ha incrementado sus equipos tecnológicos y actividades a lo largo de los años teniendo como rol primordial a las empresas brindar información de valor a todos sus clientes. Durante la verificación bibliográfica sobre el protocolo SNMP realiza una colaboración sumamente significativa para comprender el mecanismo por el cual se puede recuperar datos pertinentes de los dispositivos que forman parte de la empresa Netsecure Perú y obtiene así los resultados positivos de su uso y despliegue. En cuanto al análisis de las aplicaciones de monitoreo más utilizadas en las empresas, se convence que PRTG NETWORK MONITOR es una herramienta idónea para el despliegue de Netsecure en Perú, pues está basado en un diseño confiable, práctico y escalable adaptado a la necesidad de mejorar la red y los trabajos que brinda la empresa. Se concluye que un sistema de monitoreo puede predecir la ocurrencia de situaciones críticas de suma importancia para mantener el ejercicio de los recursos de TI sin impactar los procesos de negocio. Esto es crucial para mantener la eficiencia organizacional.

Quispe Ccuno, Jeniffer Reyna (2019). *Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce* (Tesis para optar el Título Profesional de Ingeniera en Telecomunicaciones) Universidad Nacional Mayor de San Marcos - Perú. Señala en su tesis como objetivo crear y poner en práctica un patrón que permita monitorear al instante los terminales de comunicación (acces point, switches, router) y los beneficiarios finales (fotocopiadoras, impresoras, computadores personales, laptop) utilizando el protocolo SNMP (Simple Network Management Protocol) y software gratuito para que la organización comercial compre, venda y distribuya productos y servicios a través de la red y mejorar su rendimiento. El modelo que propone permite a los profesionales de las comunicaciones y redes gestionar alarmas y notificaciones de los imprevistos de varios dispositivos de comunicación en caso de deficiencia o irregularidades en el funcionamiento recurrente de estos dispositivos. Para realizar este monitoreo, el modelo controla el tamaño de la red de la organización mediante una encuesta monitorea el protocolo SNMP su actividad para determinar

periódicamente la condición de los nodos de la red mediante ICMP (Protocolo de mensajes de control de Internet) y los servicios de estos nodos o con solicitudes especiales SNMP- que prueban si el recurso responde correctamente o si conecta solo un puerto TCP/IP con el puerto conveniente. Al analizar y estudiar un protocolo SNMP, su proyecto de tesis propuso un monitoreo real basado en la escasez de una empresa de comercio electrónico auténtico como se describe en su investigación de tesis que colabora a mejorar la duración de respuesta ante percances en su red de transmisión de datos de la empresa de comercio electrónico analizada.

Casas Reque, R. M & Sempértegui Tocto, M. L (2017). *Implementación de un sistema de monitoreo y supervisión de la infraestructura y servicios de red para optimizar la gestión de TI en la Universidad Nacional Pedro Ruiz Gallo*. (Tesis para optar el título de Ingeniero de Sistemas) Universidad Pedro Ruiz Gallo – Perú. Indica que ahora que una de las principales inquietudes de las compañías es garantizar que los servicios de red e infraestructura estén disponibles todos los días y a todas horas, es de vital consideración que los que dirigen una red estén al tanto de cualquier incidente que impida que la infraestructura y los servicios de red funcionen correctamente. Esto permite al supervisor de la red tener comunicación sobre esta de manera oportuna para conocer el estado de los servicios básicos e infraestructuras de la red, adicional a ello producir reportes para la toma de decisiones. Señala que tomó distintos criterios desde la evaluación de las herramientas seleccionadas para el propósito de la investigación hasta su estudio comparativo, elegidas cautelosamente debido a las fuentes de investigación, y Nagios Core fue el ganador con el 92% porque cumplió con la mayoría de los indicadores recomendados. Mejora la cantidad de tiempo que tardan los administradores de red en conocer los problemas con el desempeño de los dispositivos y servicios de red para que tengan suficiente tiempo para actuar y solucionarlos después de recibir notificaciones por correo electrónico. Recomienda asegurarse de estructurar de manera correcta el protocolo SNMP en los acces point, routers y switches para evitar contratiempos a la hora de monitorearlas.

Dett Sotelo, Bryan Alexis & Vega Santiago, Edwin Cesar (2020). *Aplicación de protocolos SNMP y Netflow para operar una LAN de 4 sedes de la empresa DETCOM Lima 2020.* (Tesis para optar el título profesional de Ingeniero Electrónico) Universidad Ricardo Palma – Perú. Indica con base en los resultados del trabajo realizados puede dar

una visión general de lo importante de las herramientas actuales de monitoreo y gestión usando los protocolos SNMP y NETFLOW sobre la Red LAN, de lo cual puede concluir que la disponibilidad se puede mejorar a través de una buena administración de los recursos en los servicios de Internet y, por tanto, en la gestión del ancho de banda, la supervisión de dispositivos las 24 horas ha mejorado el rendimiento de la LAN al permitir a los administradores de TI predecir problemas que podrían disminuir la productividad de la red. Las redes monitoreadas pueden administrar y solucionar problemas. Nos explica que el empleo de los protocolos SNMP y NETFLOW contribuye a la visualización y el análisis del ancho de banda dentro de la red de las empresas, ya que los administradores de red ahora pueden monitorear su uso. Con la ayuda de herramientas de monitoreo y administración, puede evaluar indicadores del ancho de banda de Internet saliente para evitar la congestión y con la ayuda de los informes que recibe, puede analizar a fondo cómo sus usuarios están usando el sistema y tomar acciones para aumentar la accesibilidad y disponibilidad.

1.4 Marco conceptual

Sistema.

Un sistema es una colección ordenada de componentes (o subsistemas) que están estrechamente relacionados con el objetivo general. El sistema comprende varios insumos que se someten a procesos específicos para producir resultados particulares, todos los cuales contribuyen al objetivo general de lograr el resultado previsto del sistema. (Etecé, 2021)

Monitoreo.

Es el seguimiento, observación y el registro regular de las actividades que tienen lugar en un programa o proyecto. Es un proceso de recopilación habitual de información sobre todos los aspectos de los dispositivos de una red. (Bartle, 2011)

Gestionar.

Es la administración y coordinación de tareas para lograr un objetivo. Las actividades de gestión implican diseñar el plan de la organización y coordinar los esfuerzos del personal para lograr objetivos específicos utilizando los recursos disponibles. (Otalora, s.f.)

Gestión de incidentes

Es un campo de la gestión de servicios de la tecnología de la información (TI) que se ocupa de restaurar el funcionamiento de un servicio rápidamente después de una interrupción. Un computador que no inicia o un firewall que no funciona son algunos ejemplos de interrupciones.

Involucra a los equipos de ayuda y servicio, y su principal objetivo es reducir los efectos negativos en el cliente y su negocio. (Zendesk, 2023)

Sistema de Gestión de Red

Los sistemas de gestión de redes están diseñados para ayudar a los ingenieros a abordar varios desafíos:

- Simplificar la configuración y administración de dispositivos.
- Garantizar la interoperabilidad entre diferentes sistemas.
- Optimizar la interfaz de usuario del fabricante y su NMS estándar.
- Resolver cortes de red, cuellos de botella y congestión. (SRGWIN, 2022)

SNMP (Simple Network Management Protocol)

Este es el protocolo fundamental que permite transferencias entre computadoras que no son de consola de administración y aquellas que están monitoreadas y administradas. En las redes IP, este protocolo fue diseñado para manejar nodos, servidores, enrutadores, estaciones de trabajo (también conocidas como "grupos de trabajo"), conmutadores y dispositivos de protección. El intercambio de dispositivos de red es compatible con SNMP, un protocolo de capa de aplicación. Los administradores NMS, los nodos administrados y MIB son los componentes de SNMP. El protocolo SNMP utiliza los puertos 161 y 162 y forma parte del Protocolo de datagramas de usuario (UDP).. (Redes Informáticas UPEL, s.f.)

MIB (Management Information Base)

Es una base de datos virtual que administra dispositivos en redes de comunicaciones celulares, comúnmente conocida como MBR. Se incluyen objetos para representar

diversos aspectos de un dispositivo, como el rendimiento y las conexiones. Además, incluye configuración y estadísticas.

Considere la MIB como una "interpretación" de los sistemas de gestión de redes. De manera similar a los diccionarios, la MIB define objetos de red que permiten una comunicación fluida entre el dispositivo y el sistema de gestión de red. (VASExpert, 2023)

Software Libre

Richard Stallman, un estadounidense que buscó crear un sistema operativo libre, es el responsable de darnos el término software libre en conjunto con otros informáticos. El desarrollo gratuito y basado en la comunidad es posible con la participación de cualquier número (de usuarios) que consideren conveniente. Introdujo una cultura informática similar a la que se encontraba en los grandes grupos informáticos. (1x1am, 2022)

Software Propietario

Un software que es de naturaleza privativa o propietaria tiene su código fuente en privado y es propiedad de su dueño. La propiedad intelectual incluye derechos de autor, patentes y otras formas de software propietario que prohíben su uso o distribución sin el consentimiento del propietario. (Martinez, 2023)

Red LAN

Una red de área local (LAN) es un conjunto de computadoras y dispositivos periféricos conectados a un servidor dentro de un área geográfica específica a través de una línea de comunicaciones común o un enlace inalámbrico. Tan solo dos o tres clientes en una oficina en casa o miles en la oficina central de una corporación pueden ser atendidos por una red de área local.

Para permitir la comunicación y el intercambio de recursos como impresoras o almacenamiento en red, los propietarios de viviendas y los administradores de TI establecen una red local (LAN). (Hwang, 2021)

CAPITULO II: PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción de la realidad problemática

Actualmente, existen innumerables empresas tecnológicas que necesitan monitorear sus equipos de red remota para evitar pérdidas de tiempo y altos costos en trasladar personal técnico para verificar las fallas y mal desempeño de sus equipos localmente, cuando pueden tener la oportunidad de tener un sistema de monitoreo completo y robusto que les permita conocer en tiempo real el funcionamiento y estado de los equipos técnicos, como tomar medidas correctivas de manera inmediata, además de datos y estadísticas reales, las evidencias necesarias deben ser contrastadas con los reportes de servicio brindados por los prestadores de servicios.

El mundo de la gestión de redes es muy importante, y debido a la alta sistematización de las empresas, la necesidad de saber qué ocurre en los dispositivos de red se ha vuelto crítica. En general, la gestión de red es la actividad de anticipar fallas en la red e identificar su impacto potencial en la prestación de servicios a los usuarios. La esencia de la gestión de redes se puede precisar de la siguiente manera: "La gestión lo es todo y sobre todo la proactividad, cualidad que lamentablemente no es fácil de encontrar en las herramientas que ofrece el mercado. Es importante no sólo conocer los fallos que pueden aparecer en la red en cualquier momento, pero también saber anticiparse a ellos, estar preparado y saber reaccionar cuando sucedan”

En general, el objetivo de la administración de la red es minimizar los riesgos de posibles fallas, minimizar los costos operativos al prevenir ciertos tipos de problemas y mantener la red operativa brindando servicios gratuitos. Los instrumentos de administración de red pueden verse como un mecanismo de seguridad de la red, toda vez que con su ayuda podemos obtener información sobre el funcionamiento de los dispositivos y ayudan a predecir problemas futuros, es decir. fortalecer la disponibilidad de los servicios.

Varios fabricantes de interfaces ofrecen varios sistemas de monitoreo, como Enterasys, CISCO, etc. La desventaja de las pequeñas organizaciones comerciales o instituciones públicas es que el uso de estos sistemas requiere el pago de licencias, cuyos precios son muy elevados.

Tabla 1.

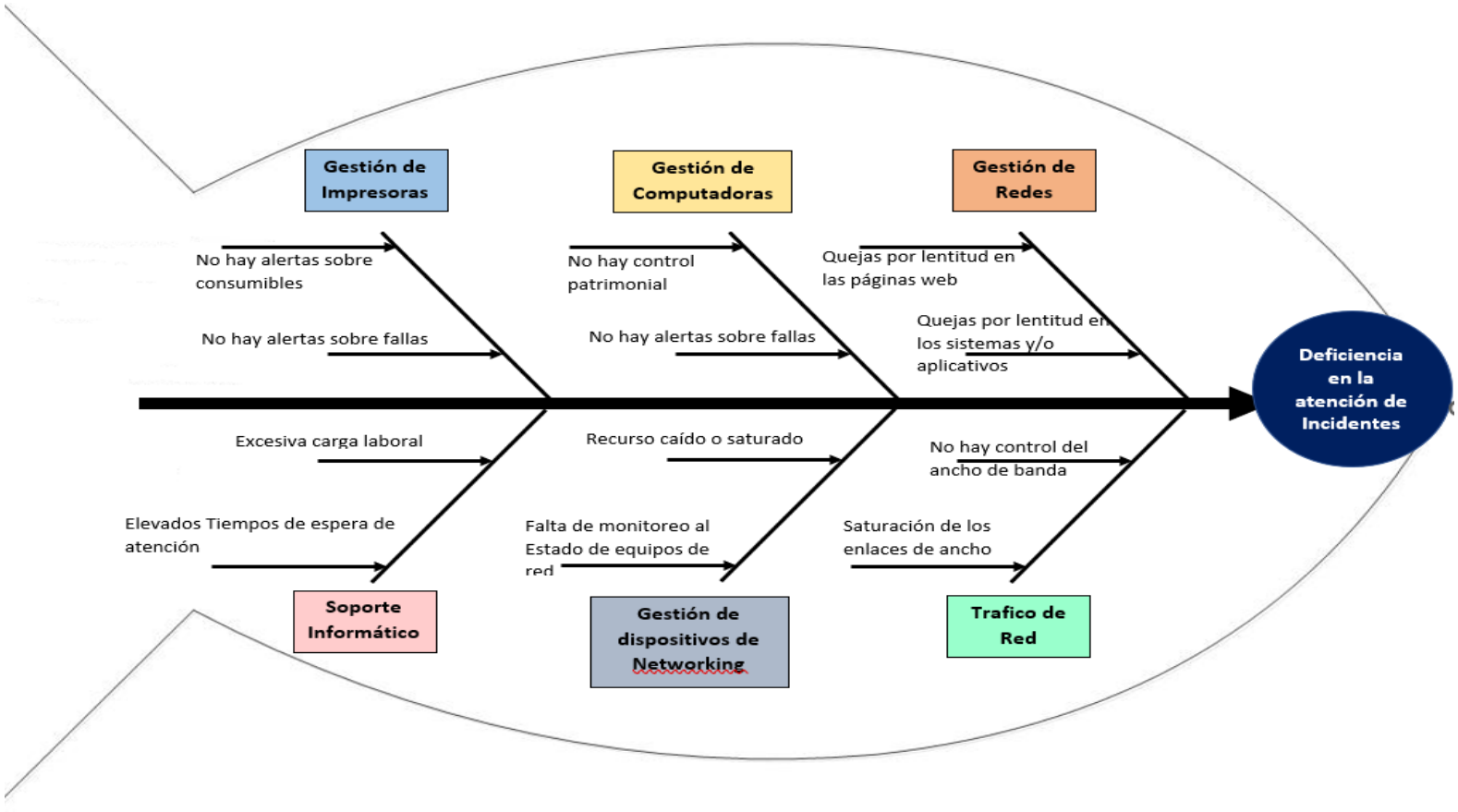
Nombre de las causas

Causas	Nombre de las causas
C1	No hay alertas sobre consumibles ni fallas en impresoras
C2	No hay gestión de control patrimonial ni alertas de fallas en computadoras
C3	Existen quejas por lentitud en sus páginas web y aplicativos
C4	Excesiva carga Laboral y elevados tiempos de espera en atención
C5	Falta de monitoreo del estado de equipos de red
C6	No hay control del ancho de banda Saturación en los enlaces

Nota. Fuente Elaboración propia, 2023

Luego de ello se elaboró el Diagrama de Ishikawa, representado en la figura 4.

Figura 4: Diagrama de causa y efecto de Ishikawa.



Nota. La Figura 4 muestra el Diagrama de causa y efecto de Ishikawa.

2.2 Formulación del problema general y específicos

Problema General:

¿De qué manera la implementación de un sistema de monitoreo mejorará la oportuna atención de incidentes que presenten los dispositivos de una red, utilizando protocolo SNMP?

Problema Específicos:

- ¿De qué forma se obtiene información de un dispositivo equipo agregado al sistema para realizar su monitoreo?
- ¿Cómo se configuran las alertas y reglas en los dispositivos agregados al sistema para realizar un monitoreo efectivo?

2.3 Objetivo general y específicos

Objetivo General:

Implementar un sistema de monitoreo para mejorar la oportuna atención de incidentes que presenten los dispositivos de una red, utilizando protocolo SNMP.

Objetivos específicos:

- Obtener información de un dispositivo agregado al sistema para realizar su monitoreo.
- Determinar las configuraciones de las reglas, alertas en los dispositivos agregado al sistema para realizar un monitoreo efectivo.

CAPITULO III: JUSTIFICACION Y DELIMITACION DE LA INVESTIGACION

3.1 Justificación e importancia del estudio

3.1.1. Justificación

La implicación del hombre en la necesidad de globalizar las comunicaciones las ha ido complejizando con el tiempo. Las redes de comunicación siguen siendo fundamentales en la actualidad, especialmente las redes LAN, que se han transformado en la columna vertebral de las organizaciones.

En la actualidad, las redes LAN sirven como medio de comunicación entre diferentes subredes y usuarios. Sin embargo, también deben ofrecer servicios distintos. La creciente complejidad de las redes LAN dificulta el mantenimiento de los enlaces de comunicación y la gestión del equipo que conecta las diferentes partes de las organizaciones.

Se debe implementar un sistema de monitoreo de red para permitir la identificación inmediata de problemas en la red y asegurar la continuidad con los servicios de las redes.

Para el proyecto actual se está considerando un sistema de monitoreo que sea propietario, ya que brinda los mismos beneficios que un sistema propietario y también cuenta con la garantía y respaldo de miles de usuarios en todo el mundo que contribuyen a mejorar estas aplicaciones.

El protocolo SNMP es la base del sistema de monitoreo propuesto en este proyecto, ya que permite una medición precisa del estado del enlace punto a punto para revelar la congestión y tomar las medidas adecuadas.

Para ilustrar, una impresora puede notificar al administrador que no hay suficiente papel o suministros, mientras muestra una alerta de mayor carga del sistema para asegurar el servidor. SNMP permite la alteración remota de la configuración del dispositivo, lo que significa que puede cambiar la dirección IP de una computadora a

través de un agente o forzar la ejecución de comandos (según las capacidades del agente).

3.1.2. Importancia

La importancia del presente trabajo de suficiencia radica a través de la mitigación de la realidad problemática presentada en las instituciones públicas y privadas, que será lograda a través de la implementación de un buen software de monitoreo de red que ofrezca información a tiempo real sobre el rendimiento, disponibilidad e interconexión de los equipos de cómputo, redes e impresoras; esto conllevará a una mejor gestión de los incidentes presentados.

3.2 Delimitación del estudio

Teórica:

Las áreas de conocimiento que se aplican en el presente trabajo de suficiencia, están comprendidas en la gestión de una Red LAN mediante protocolo SNMP

Espacial:

Se focaliza en la emulación de una sede central ubicada en la ciudad de Lima y varias unidades orgánicas situadas a nivel nacional.

Temporal:

El presente trabajo de suficiencia está siendo diseñado en un periodo de tiempo de setiembre 2022 a octubre del 2023.

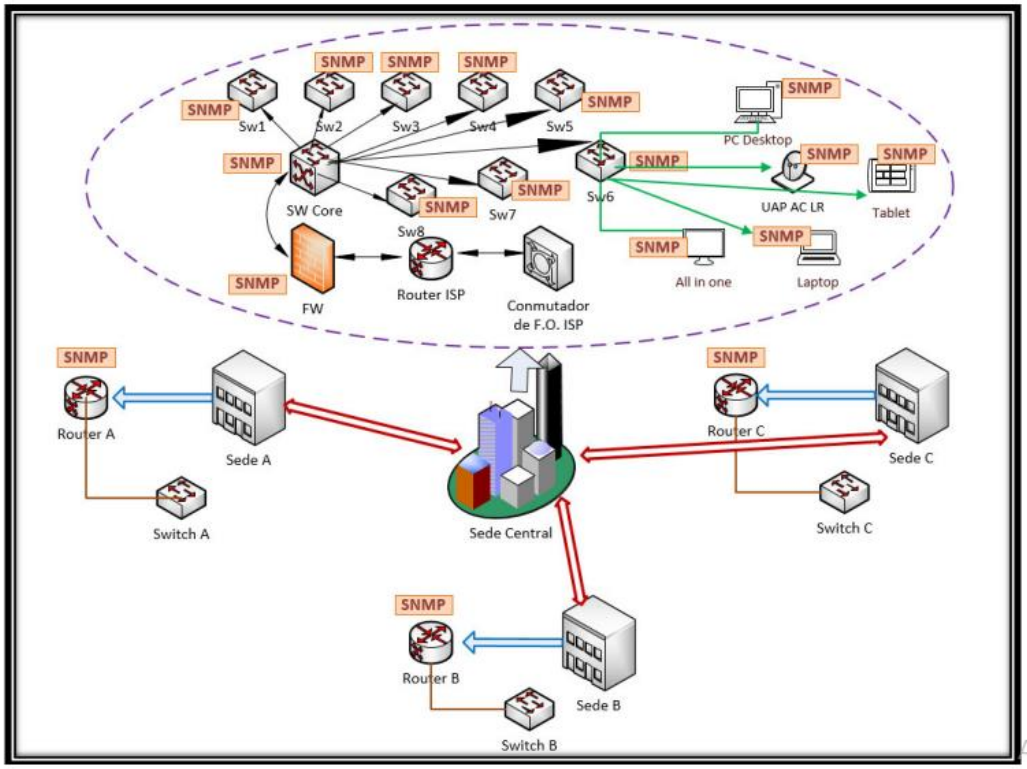
CAPITULO IV: FORMULACION DEL DISEÑO

4.1 Diseño esquemático

El diseño del sistema de monitoreo y gestión de dispositivos utilizando el protocolo SNMP y software libre, está dirigido a empresas o instituciones que comercializan o laboran con dispositivos en red cableada o wifi y no a una empresa en específico, considera la necesidad de un monitoreo y detección general de posibles fallos técnicos y garantizar la capacidad de documentar fallos de hardware y software de estos dispositivos para permitir a estas empresas ahorrar tiempo y costes laborales relacionados con el traslado de personal técnico a sitios remotos y difíciles para llegar

Este trabajo de suficiencia estará dirigido a monitorear los dispositivos que cuenta la red de la *Contraloría General de la República* (CGR) y sus sedes desconcentradas.

Figura 5. Interconexión de dispositivos de comunicación que son monitoreados en la CGR

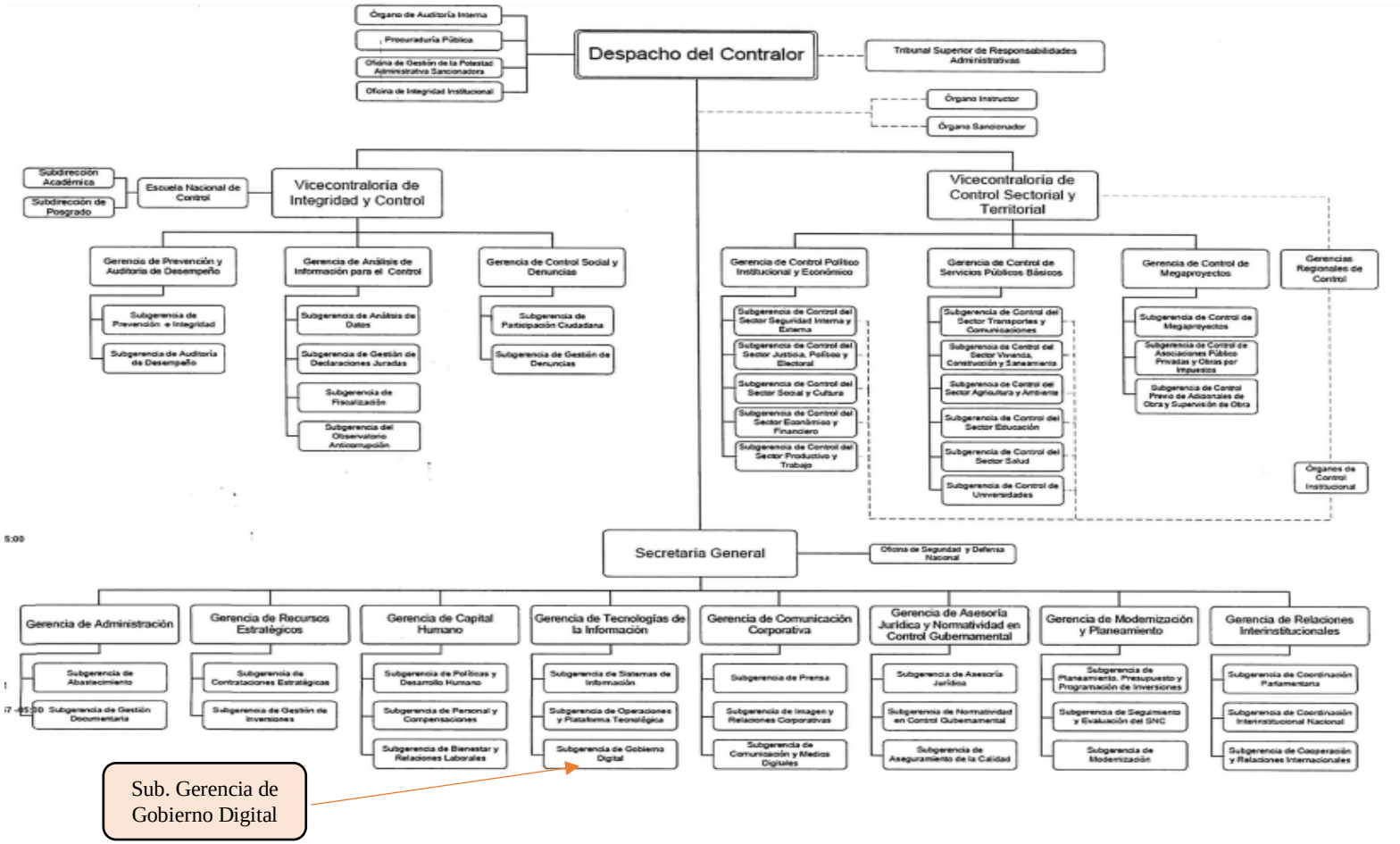


Nota. Elaboración propia basado en la información de la empresa

Figura 6. Proceso de la gestión de incidentes de la CGR

Nota En la figura 6, se evidencia el Proceso de la gestión de incidentes basados en el "Procedimiento de Atención de Mesa de Ayuda" PR-TI-01. de la CGR.

Figura 7. Organigrama de la Contraloría General de la Republica
[Elaboración propia basado en la información de la empresa]



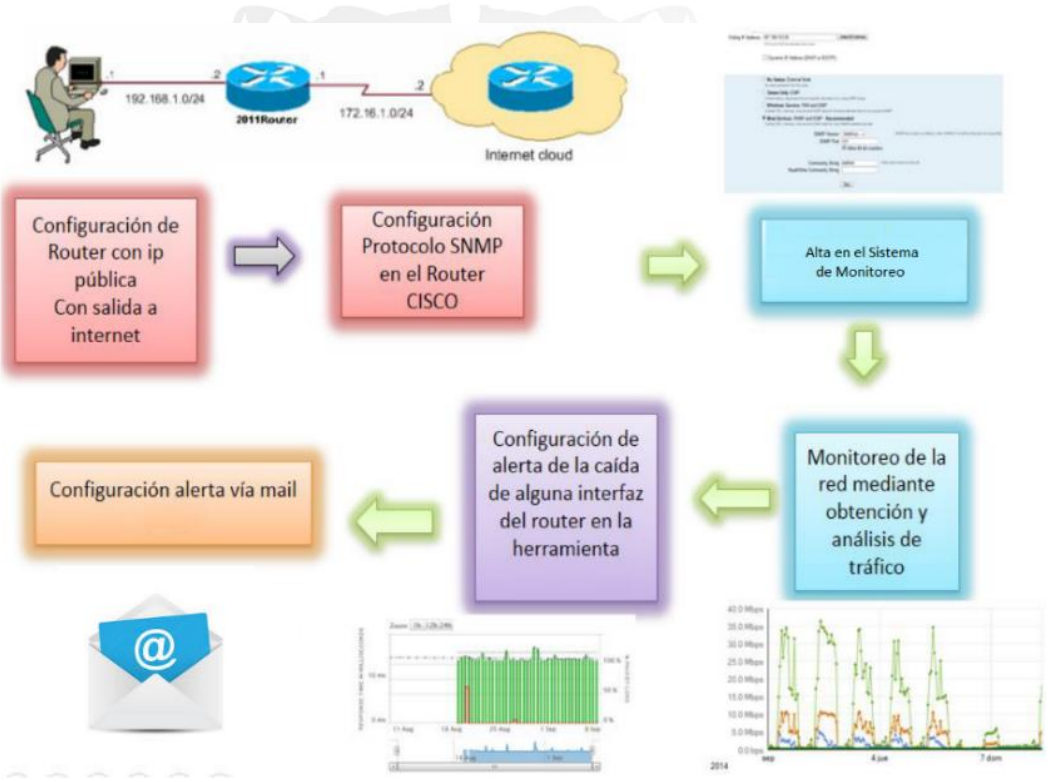
En la figura 7, se observa el Organigrama de la Contraloría General de la Republica. El área señalada es la SubGerencia de Gobierno Digital que pertenece a la Gerencia de Tecnologías de la Información, es mi área laboral donde será implementado el Sistema de monitoreo.

4.2 Descripción de los aspectos básicos del diseño

Metodología

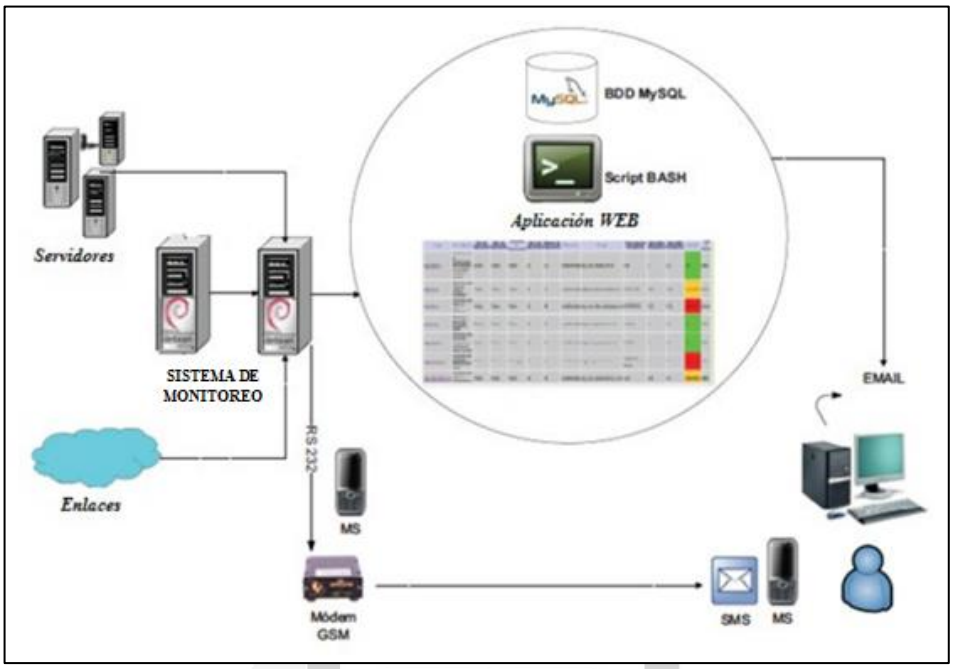
Para la implementación del sistema se deben utilizar varios equipos administrados (agente, dispositivos o equipos remotos conectados a la LAN), junto con la estación de administración principal, configuración y activación del protocolo SNMP, luego se agrega una base de datos con MIB.

Figura 8. Monitoreo de una red usando protocolo SMTP
[Elaboración propia]



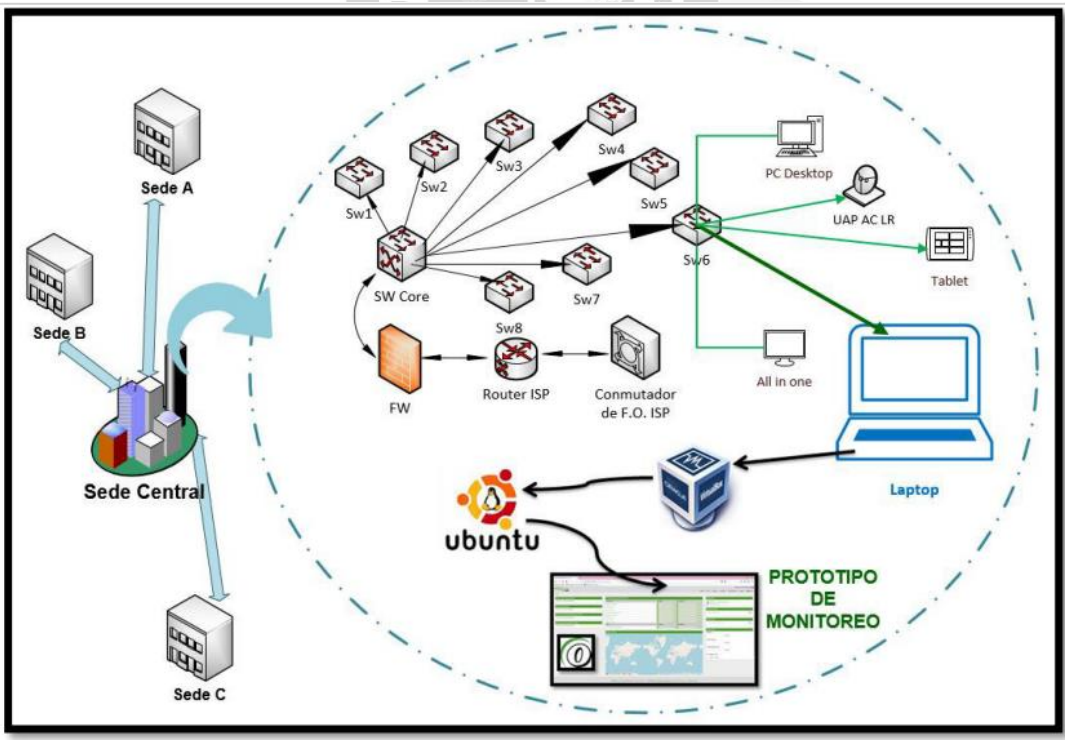
Nota La operación del sistema se caracteriza por la comunicación entre el agente en ejecución en la computadora administrada y el monitor de red, como se ilustra en la Figura 8. Después de detectar el agente, el monitor utiliza tecnología de subprocesos múltiples para administrar varias conexiones y obtener información sobre su software y hardware. características de los equipos gestionados mediante el protocolo SNMP.

Figura 9. Esquema del sistema de monitoreo a implementar



Nota. La Figura 9, muestra la comunicación entre el sistema de monitoreo y los dispositivos que serán gestionados.

Figura 10. Topología de la propuesta



Nota. Elaboración propia basado en el prototipo de monitoreo de red propuesto

CAPITULO V: PRUEBA DE DISEÑO

5.1 Aplicación de la propuesta de solución

"Sistema de monitoreo para mejorar la oportuna atención de incidentes que presenten los dispositivos de una red, utilizando protocolo SNMP"

- Institución: Contraloría General de la República (CGR)
- Rubro: Sector público
- Ubicación: Jr. Camillo Carrillo 114 – Jesus Maria – Lima
- Equipos a monitorear: Impresoras de la Sede Central (Lima) y de los órganos de control (provincias)

Tabla 2.

Consolidado Impresoras CGR

Ubicación	Cantidad
Lima	85
Provincias	157
Total	**242**

Nota. Fuente Elaboración propia, 2023

De acuerdo al objetivo general del presente trabajo de investigación se implementará un sistema de monitoreo para mejorar la oportuna atención de incidentes que presenten las 242 impresoras de la CGR, las cuales se encuentran distribuidas en la Sede central Lima y en diversas provincias, pero en la misma red de la institución.

Se pondrá en funcionamiento el sistema de monitoreo desde la Sede Central (Lima) donde se evidenciará las funciones del sistema las cuales se dividen en: Herramientas de administración y monitoreo.

1) **Herramientas de Monitoreo**

   Las herramientas de monitoreo brindan a los usuarios acceso a datos en tiempo real desde dispositivos conectados, incluido contadores, el estado de insumos, mapas, registros, informes y más.

   - Tablero

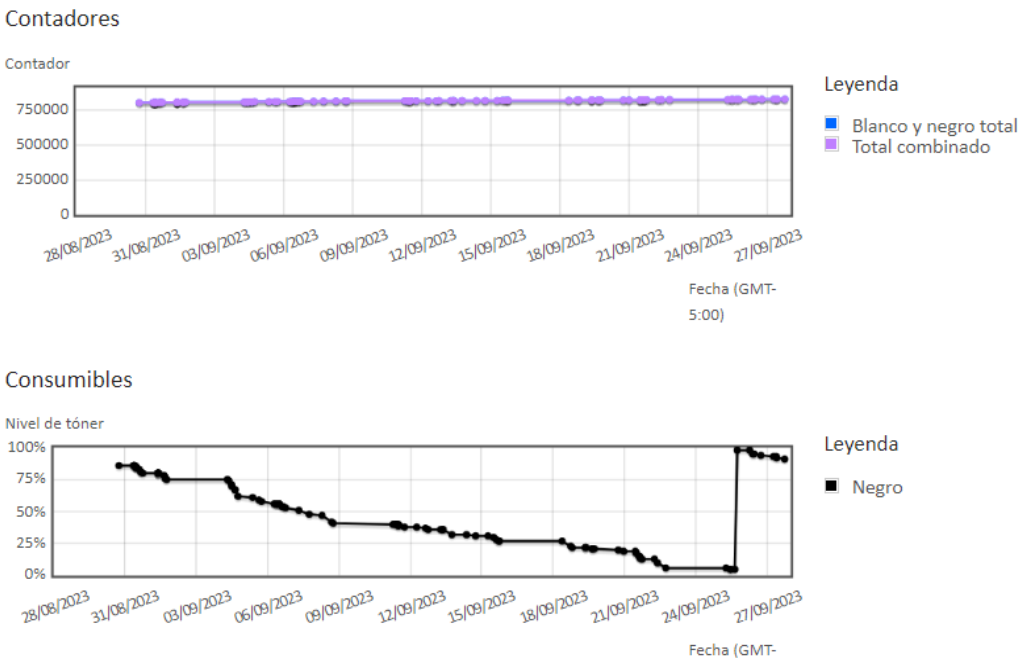
- Registros de E-mail y Auditoría
- Estado del Panel
- Informes
- Contadores
- Notificaciones
- Propiedades del Dispositivo
- Registros del Dispositivo
- Mapas

Tablero

Al utilizar el Panel, puede monitorear los cambios en la actividad y los errores e ingresar datos de una flota. Dentro de un plazo designado, como 24 horas, 7 días, 14 días o 30 días. Esto le permite analizar y ver varios tipos de datos, incluidos los niveles de tóner y los tamaños de impresión y escaneo. Al hacer esto, puede mejorar el tiempo de actividad del dispositivo, disminuir las colas de la mesa de ayuda y detectar brechas de manera proactiva.

Contadores

Figura 11. Pantalla Contadores y consumibles



Nota. Sistema de monitoreo de impresoras de la CGR

Tal como se observa en la figura 11, se obtiene la siguiente información en una página impresa:

- Nombre del modelo
- Número de serie
- Páginas a color
- Páginas en blanco y negro
- Páginas en un solo color
- Total de páginas escaneadas
- Páginas en dos colores

Registros del Dispositivo

Para determinar rápidamente el estado de la flota, se buscan eventos del sistema utilizando un enfoque basado en listas. El campo de descripción ofrece una respuesta al problema si hay algún problema.

Informes

Hay informes visuales o de inventario disponibles que muestran la cantidad de tóner, el volumen de páginas y el color utilizado. La generación de informes se puede realizar utilizando más de 30 plantillas. Ejecute informes con frecuencia o según un cronograma.

- Contadores
- Administración de insumos
- Verificación de estado (mantenimiento preventivo)

Estado del Panel

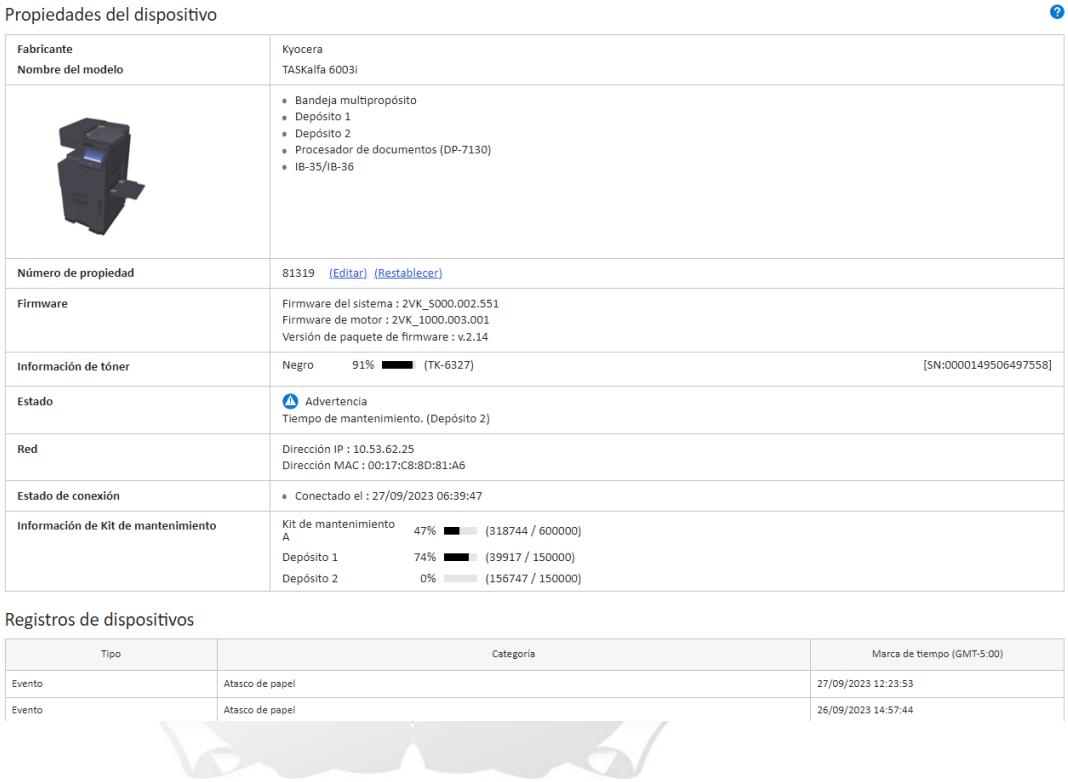
Una manera conveniente de diagnosticar problemas es examinando el estado del panel, lo que permite al técnico identificar cualquier indicación que deba abordarse y actuar en tiempo real. Varios usuarios pueden observar el estado del panel a la vez

Notificaciones

El código de servicio, los detalles del evento (como atascos de papel), los contadores o los niveles de suministro se envían automáticamente como notificaciones por correo electrónico

Propiedades del Dispositivo

Figura 12. Pantalla Propiedades del dispositivo
[Sistema de monitoreo de impresoras de la CGR]



Nota. En la figura 10, puede observarse las siguientes propiedades del dispositivo:

- Nombre del modelo
- Fabricante
- Número de activo
- Accesorios instalados
- Información del tóner
- Versiones del firmware
- Direcciones de red
- Estado de la conexión
- Estado

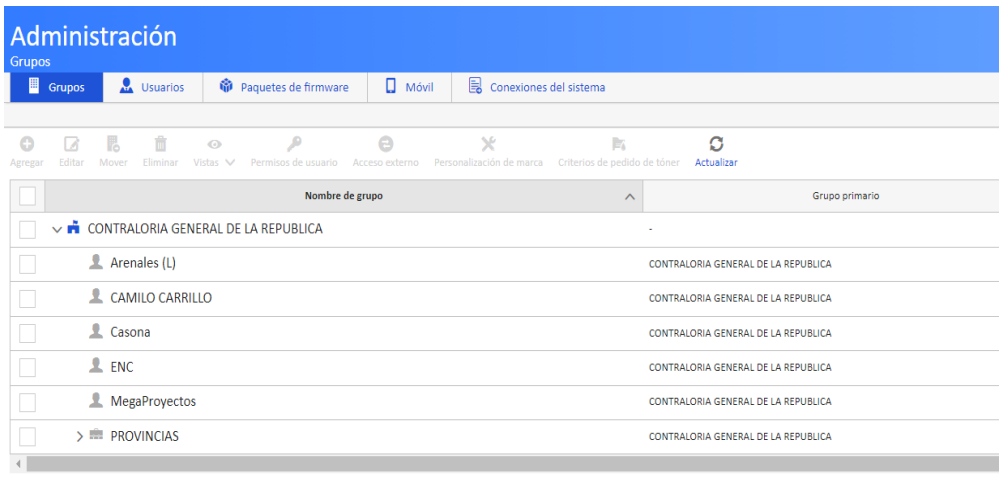
Mapas

Puede ver las ubicaciones de los dispositivos y el estado del sistema en mapas, que proporcionan una representación gráfica de las ubicaciones de los usuarios y dispositivos dentro de un espacio físico.

Herramientas de Administración

Los proveedores de servicios pueden regular muchos aspectos de las operaciones de la flota gracias a las herramientas de administración.

Figura 13. Pantalla Opción de Administración
[Sistema de monitoreo de impresoras de la CGR]



Nota. Como se observa en la figura 11, entre otras cosas, puede reiniciar su impresora de forma remota, actualizar el firmware y cambiar ajustes de configuración., asimismo otras funciones son.

- Reinicio de Dispositivo
- Configuración del Dispositivo
- Modo de Mantenimiento
- Instantáneas
- Nota del Panel
- Foto de Pantalla del Panel
- Captura de Datos
- Envío de Archivo
- Registros USB
- Orden de Compra de Tóner

Resultados:

Se realizaron pruebas en una laptop que sirvió como Estación gestor principal, el cual tenía las siguientes características: sistema operativo Windows 10 (64 bits), 8.0 Gb de memoria RAM, procesador de 4 núcleos, configurado, además habilitado el servicio SNMP y conexión a la LAN.

Se desarrolló la primera versión del sistema para monitoreo de equipos remotos mediante SNMP, el cual mantiene la información actualizada cada segundo gracias al uso de la tecnología multi-hilo de Java y para mejorar el rendimiento y productividad se implementaron patrones de diseño como el Modelo-Vista-Controlador (MVC) y Singleton.

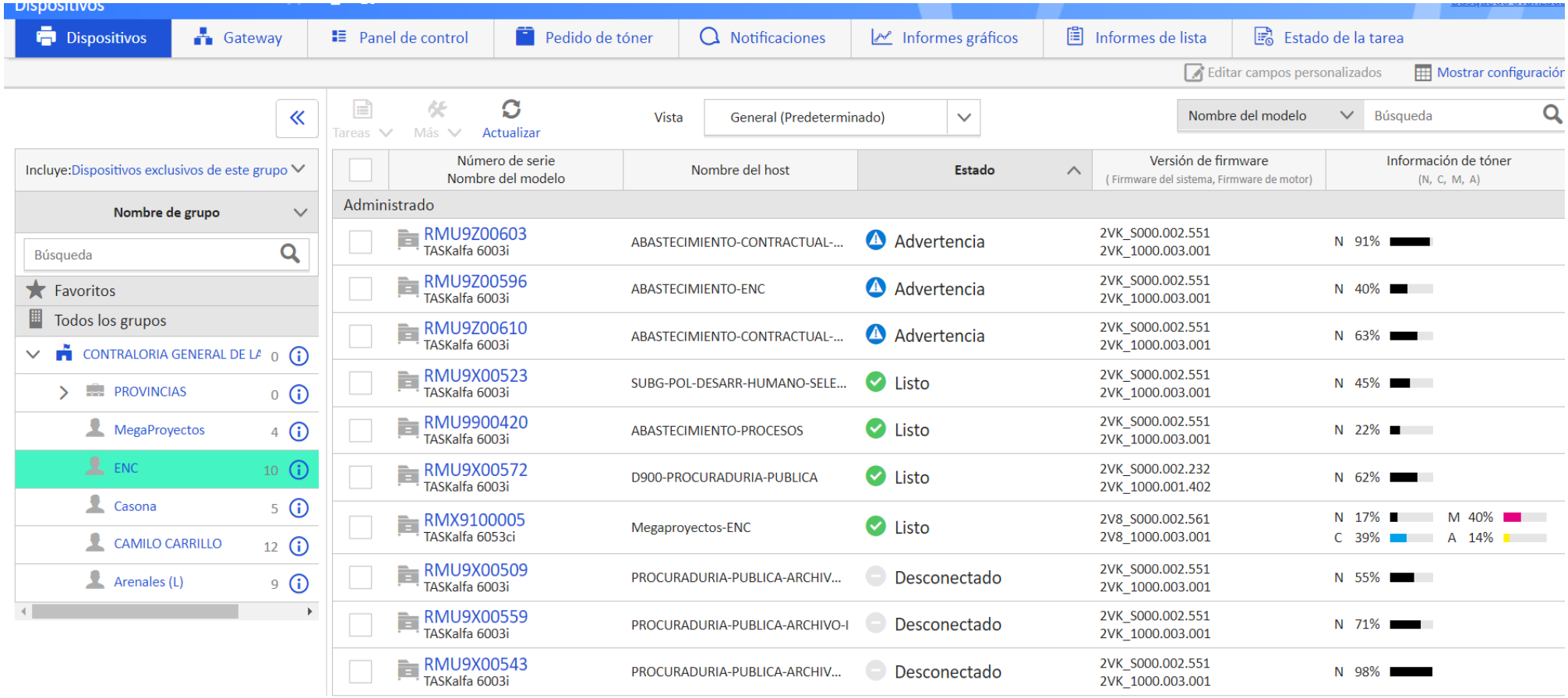
De acuerdo al primer objetivo específico se obtuvo información de todos los dispositivos (impresoras) agregados al sistema para realizar su monitoreo., tal como se muestra en la Figura 12.

De acuerdo al segundo objetivo específico, se determinó las configuraciones de las reglas, alertas en las impresoras agregadas al sistema para realizar un monitoreo efectivo en tiempo real de la siguiente manera:

1. Notificaciones: Se generan 03 alertas por e-mail de forma automática.
2. Análisis instantáneo. Se detectaron 03 advertencias de impresoras del área de Abastecimiento de la CGR, las cuales eran por ataco de papel.
3. Respuesta rápida. Se reportó las fallas al proveedor de las impresoras, quien llegó al lugar con todos los componentes necesarios a mano.
4. Periodo fuera de servicio minimizado. Se pudo resolver el problema en una sola visita: minimizando así el periodo fuera de servicio del equipo multifuncional y maximizando la productividad de los usuarios.

El sistema de monitoreo recientemente desarrollado proporciona una interfaz fácil de usar pues permite una visualización fácil e intuitiva de la información del tráfico de la red sin el uso de comandos laboriosos. La capacidad de almacenar un historial puede ayudar en el rol de administrador de red al brindar explicaciones sobre cualquier cambio realizado en computadoras remotas, independientemente de su software o hardware.

Figura 14: Despliegue del Sistema de Monitoreo para Impresoras de la CGR



En la figura 14 se puede observar los grupos de impresoras de la CGR, las cuales están monitoreadas por el sistema en tiempo real evidenciando las características del equipo, serie, ubicación, advertencias, firmware instalado y nivel de consumibles (tóner)

CONCLUSIONES

Se implementó el sistema de monitoreo en una institución pública peruana, con ello, se pudo mejorar considerablemente la oportuna atención de incidentes, que presentaron los dispositivos de su red, utilizando protocolo SNMP, disminuyendo los tiempos de espera de atención y minimizando el periodo de fuera de servicio de los equipos.

Se obtuvo excelentes resultados evidenciando así, que se pudo obtener información de varios dispositivos agregados al sistema para realizar su monitoreo en tiempo real, tal como lo muestra la Figura 14, donde la información de las impresoras de la CGR fue agrupada por Subgerencias de la sede central y provincias.

Se determinó que mediante el despliegue del sistema de monitoreo se pudo gestionar las configuraciones de las reglas, alertas en los dispositivos agregados, en este caso las impresoras de la CGR, para realizar un monitoreo efectivo. Estas alertas llegaron al correo electrónico, previamente indicado en el Sistema, y se brindó la solución rápida y efectiva los incidentes reportados.

RECOMENDACIONES

Se recomienda que, al momento de administrar dispositivos de una red como impresoras, computadores, routers etc, primero se debe tener el árbol MIB del dispositivo para luego convertirlo a un archivo que puede ser reconocido por el sistema.

Es importante conocer los parámetros que deberán pasar para la verificación del equipo de red antes de implementarla, como la temperatura y los errores de entrada y salida, parámetros como estos se pueden almacenar en el árbol MIB para evitar fallas en los equipos.

Para implementar la gestión de red mediante el protocolo SNMP, es importante saber qué equipos lo soportan y si será gestionado mediante software o hardware. Esto requiere experiencia en ambas áreas.

REFERENCIAS BIBLIOGRAFICAS

1x1am. (15 de Noviembre de 2022). *Software libre: características y ventajas de su uso.* https://www.ixiam.com/es/blog/software-libre-caracteristicas-y-ventajas-de-su-uso/

Bartle, P. (30 de Setiembre de 2011). *La naturaleza del seguimiento y la evaluación.* https://cec.vcn.bc.ca/cmp/modules/mon-wht.htm

Ciberseguridad Chihuahua. (s.f.). *Gestión de incidentes informáticos.* https://ciberseguridad.uach.mx/empresas/gestion-de-incidentes-informaticos/

Cisco. (s.f.). *¿Qué es el monitoreo de red?.* https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

Digital Guide IONOS. (29 de Mayo de 2019). *SNMP: el protocolo base para la gestión de redes*. https://www.ionos.es/digitalguide/servidores/know-how/snmp/

Hwang, D. (Abril de 2021). *Red de área local o LAN*. https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

Martinez, E. (03 de Mayo de 2023). Qué es el software propietario y las ventajas de usarlo en nuestra empresa. https://www.iebschool.com/blog/software-propietario-digital-business/

Otalora, A. (s.f.). Qué es gestión. https://www.academia.edu/44514223/Que_es_gestion

Redes Informáticas UPEL. (s.f.). *Protocolos elementales de enlace.* https://riupel.wordpress.com/protocolos-elementales-de-enlace/

SRGWIN. (12 de Mayo de 2022). *¿Qué es un sistema de gestión de redes?.* https://www.sgrwin.com/es/what-is-network-management-system/

Telco Manager. (2022). *Que es el SMTP*. https://www.telcomanager.com/es/blog/que-es-el-snmp/

VASExpert. (14 de Agosto de 2023). *MIB (Management Information Base)*. https://vasexperts.com/es/resources/glossary/mib-management-information-base/

Zendesk. (07 de Agosto de 2023). *Guía introductoria a la gestión de incidentes.* https://www.zendesk.com.mx/blog/gestion-de-incidentes/