NOMBRE DEL TRABAJO

PROPUESTA DE UN MÓDULO PARA OPTIMIZAR EL SERVICIO DEL ÁREA HELPDESK FRENTE A INCIDENCIAS UTILIZANDO

AUTOR

FRANKLIN QUISPE QUINTO

RECUENTO DE PALABRAS

7753 Words

RECUENTO DE CARACTERES

39955 Characters

RECUENTO DE PÁGINAS

50 Pages

TAMAÑO DEL ARCHIVO

1.2MB

FECHA DE ENTREGA

Jun 5, 2024 10:02 AM GMT-5

FECHA DEL INFORME

Jun 5, 2024 10:03 AM GMT-5

20% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 20% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 8 palabras)

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45° de la ley N° 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (X)

DATOS PERSONALES

Apellidos y Nombres:	Quispe Quinto Franklin
D.N.I.:	71377998
Otro Documento:	
Nacionalidad:	Peruana
Teléfono:	960 536 821
e-mail:	Frann15sc@gmail.com

DATOS ACADÉMICOS

Pregrado

Facultad:	Facultad de Ingeniería y Gestión
Programa Académico:	Trabajo de Suficiencia Profesional
Título Profesional otorgado:	Ingenio de Sistemas

Postgrado

Universidad de Procedencia:	
País:	
Grado Académico otorgado:	

Datos de trabajo de investigación

Título:	Propuesta de un módulo para optimizar el servicio del área Helpdesk frente a incidencias utilizando la herramienta Zabbix en la empresa Securesoft periodo 2020
Fecha de Sustentación:	19/12/2020
Calificación:	Aprobado
Año de Publicación:	2024

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo __X__ No autorizo _____

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	(X)

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	( )
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

Motivos de la elección del acceso restringido:

Quispe Quinto Franklin

APELLIDOS Y NOMBRES

71377498

DNI

Firma y huella:

Lima, 13 de junio del 2024

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“PROPUESTA DE UN MODULO PARA OPTIMIZAR EL SERVICIO DEL AREA HELPDESK FRENTE A INCIDENCIAS UTILIZANDO LA HERRAMIENTA ZABBIX EN LA EMPRESA SECURESOFT PERIODO 2020”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

QUISPE QUINTO, FRANKLIN
ORCID: 0009-0008-5147-0375

ASESOR

OCHOA CARBAJAL, HERNÁN
ORCID: 0000-0003-1466-4548

Villa el Salvador

2020

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

"Año de la Universalización de la Salud"

IV Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional
Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

En Villa El Salvador, siendo las 11:00:00 AM del día sábado 19 de diciembre de 2020, y debido a la emergencia sanitaria y aislamiento social por el COVID-19, se reunieron en la Sala Virtual N° 01 vía Google meet (https://meet.google.com/rip-pnvz-rmg), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: Dr. Angel Fernando Navarro Raymundo	CIP	N° 85997
Secretario	: Dr. Julio Elvis Valero Cajahuanca	CIP	N° 87161
Vocal	: Dr. Alfredo César Larios Franco	CIP	N° 78376

Designados con RESOLUCIÓN DE FACULTAD DE INGENIERÍA Y GESTIÓN N° 497-2020-UNTELS-CO-V.ACAD-FIG, de fecha 10 de diciembre de 2020.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero de Sistemas, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional. (Resolución de Comisión Organizadora Nº 119-2020-UNTELS de fecha 22 de julio de 2020, en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del IV Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur", así como la Resolución Presidencial Nº 293-2020-UNTELS de fecha 14 de diciembre de 2020, que APRUEBA modificar el Artículo Segundo de la Resolución de Comisión Organizadora Nº 119-2020-UNTELS, de fecha 22 de julio de 2020, que designa a la "Comisión del IV Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur"); siendo que el Art. 4º del precitado Reglamento establece que: **"La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo de Suficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otras modalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar un mínimo de seis (06) meses de experiencia laboral, de acuerdo a lo establecido en la Resolución Nº 174-2019- SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)..."**, en el cual;

El Bachiller: **FRANKLIN QUISPE QUINTO**

Sustentó su Trabajo de Suficiencia Profesional: **PROPUESTA DE UN MODULO PARA OPTIMIZAR EL SERVICIO DEL AREA HELPDESK FRENTE A INCIDENCIAS UTILIZANDO LA HERRAMIENTA ZABBIX EN LA EMPRESA SECURESOFT PERIODO 2020**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición **Aprobado** Equivalencia **Regular** de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las 11:41 am del día, se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado.

SECRETARIO
Dr. Julio Elvis Valero Cajahuanca
CIP N° 87161

PRESIDENTE
Dr. Angel Fernando Navarro Raymundo
CIP N° 85997

VOCAL
Dr. Alfredo César Larios Franco
CIP N° 78376

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del Presidente del jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del jurado, la sustentación será reprogramada durante los 05 días siguientes.

DEDICATORIA

A mis padres por todo el apoyo que siempre me han brindado y aun lo siguen haciendo pese a todo me siguen alentando a seguir adelante.

AGRADECIMIENTOS

Mi agradecimiento a la universidad UNTELS por haberme permitido formarme en ella, así como también a todo el personal de la escuela de ingeniería de sistemas por su apoyo incondicional durante el desarrollo de la carrera.

Agradezco también a mi asesor el Ing. Hernán Ochoa por brindarme la orientación necesaria para el desarrollo del presente trabajo de investigación.

Del mismo modo, agradezco también a mis amigos y familiares que colaboraron de manera directa e indirecta en mi formación profesional, permitiéndome desarrollar y aplicar los conocimientos adquiridos durante mis años de estudio.

ÍNDICE

Contenido

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

Dentro de la Empresa Securesoft existe un área (Helpdesk) que es la encargada de dar soporte a los usuarios en el ámbito informático, así como también el de velar por la calidad de servicio y de brindar la seguridad de que las redes de comunicaciones siempre se encuentren operativas.

En este trabajo se pretende ayudar a mejorar u optimizar la detección y solución oportuna de los incidentes que pueden ocurrir dentro de la Empresa Securesoft. Para ello se hará uso del software libre y de código abierto Zabbix, el cual nos permitirá monitorear en tiempo real todos los equipos de la empresa. Se empleará un módulo del Zabbix en el cual se engancharán los equipos que se encuentran en el área del SOC.

Después de emplear la propuesta de un módulo del software Zabbix se espera tener como resultado una mejora en el rapidez y eficacia de solución de los incidentes, así como también de acuerdo a la información recolectada por el Zabbix poder prevenir futuros incidentes.

INTRODUCCIÓN

En el presente trabajo se centra en el uso del software Zabbix para mejorar el servicio brindado por el área de Helpdesk.

En la actualidad para las empresas la infraestructura tecnológica es un activo muy importante que se emplea para comunicarse, recolectar información, entre otras actividades. El no tener un control de estos recursos informáticos pueden causar pérdidas de bienes materiales o inmateriales a la organización.

Para ello se plantea usar la herramienta Zabbix para el monitoreo de estos recursos informáticos y así poder analizar y determinar las posibles fallas de los recursos informáticos en tiempo real.

El módulo en el Zabbix que se propone nos permitirá monitorear aplicaciones web, análisis de logs mediante un panel de control (dashboard), donde se observarán las incidencias que se presenten en tiempo real en forma de alertas, así como también se notificara por correo electrónico, telegram, slack, Otros.

Al tener un interfaz amigable e intuitiva el usuario podrá tener un control de los dispositivos y así poder mantener la disponibilidad y calidad de servicio hacia los clientes.

A continuación, veremos el capítulo I y capítulo 2 en las cuales se detalla las bases teóricas y la metodología usada para el desarrollo del presente trabajo.

OBJETIVOS

General

- Implementar un módulo de gestión de incidencia utilizando el software Open Source Zabbix en la empresa Securesoft - 2020

Específico

- Configurar el software Zabbix para administrar y monitorear los recursos informáticos.
- Considerar el protocolo SNMP en los dispositivos para intercambiar datos y así supervisar el correcto funcionamiento de los recursos informáticos.
- Diseñar un modelo de incidencias para la organización Securesoft.

CAPÍTULO I: MARCO TEÓRICO

1.1. Bases teóricas

Mesa de ayuda o Helpdesk.

La mesa de ayuda o helpdesk según Razo (como se citó en Lanchero, 2016) sostiene que:

> Es la prestación del servicio interno de sistemas y del apoyo para la solución de las problemáticas que se les presentan a los usuarios en los sistemas; este servicio lo presta personal especializado, contrato ex profeso para ello; el cual proporciona los servicios o auxilios informáticos a las áreas de la empresa, a fin de mantener el funcionamiento de los sistemas de la institución; por lo general, dicho servicio se presta por medio de la red de cómputo, y la mayoría de servicios se realizan vía telefónica o a través de la propia red. (pag.18)

figura 1: Help Desk

Fuente: Recuperado de: https://helppeoplecloud.com/sitio/archivos/8782

El personal encargado de mesa de ayuda o helpdesk debe tener conocimientos de hardware, software y telecomunicaciones para proporcionar respuestas y soluciones a clientes finales, así como también el asesoramiento en relación con equipos o sistemas informáticos.

Gestión de Incidencias.

Según Bon (como se citó en Aguilar, 2017) afirma que:

> Es el Proceso responsable de registrar todas las incidencias que afecten a la calidad del servicio y restaurarlo a los niveles acordados de calidad en el más breve plazo posible, tiene como objetivo resolver, de la manera más rápida y eficaz posible, cualquier incidente que cause una interrupción en el servicio. (pag.49)

Incidencias.

Un incidente es un acontecimiento ocurrido que influye en el desarrollo de una acción y tendrá consecuencias de la misma. Es la indisponibilidad temporal de un servicio, o el fallo de algún elemento que trae como consecuencia la reducción de la calidad del servicio brindado.

Es un evento no planificado que se tiene que dar solución lo más pronto posible, identificar y controlar las causas para prevenir y evitar su propagación y así evitar futuros eventos no deseados.

Tabla 1

Diferencias entre evento, incidencia y problema

EVENTOS	INCIDENCIAS	PROBLEMAS
Es todo suceso detectable que tiene importancia para la estructura de TI	Es la interrupción o reducción de la calidad no planificada del servicio.	Son incidencias recurrentes y que tienen la misma problemática
Es toda situación que se produzca y que pueda afectar a la prestación de los servicios	Es un evento que no forma parte de la rutina de operación	son incidentes que afectan a muchos usuarios

Fuente: Autoría propia

¿Qué es software libre?

El software libre es aquel en donde los usuarios tienen acceso al código fuente y tiene libertad plena de ejecutar, modificar copiar, estudiar y distribuir el software con cambios o sin ellos. En otras palabras, el usuario u organización puede usar el programa sin la necesidad de pedir permiso al desarrollador o alguna entidad.

(Stallman, 2004) refiere que el software libre tiene cuatro clases de libertad para los usuarios de software.

- Libertad 0: libertad para ejecutar el programa con cualquier propósito.

- Libertad 1: libertad para poder estudiar el código fuente y así modificarlo de acuerdo con nuestras necesidades
- Libertad 2: libertad de distribuir o redistribuir el programa con o sin modificaciones
- Libertad 3: libertad de mejorar el programa y poder publicarlo en beneficio de la comunidad

¿Qué es linux?

Linux es un sistema operativo que fue desarrollado por el finlandés Linus Torvalds basado en el sistema Minix que a su vez está basado en el sistema Unix. Linux es un sistema operativo de código abierto por lo cual puede ser ejecutado, estudiado, modificado y compartido. Además, el código modificado se puede redistribuir o en su defecto puede ser vendido.

Las características que más destacan de la variedad de las distribuciones de Linux según Guijarro, Molina, Galarza y Trejo (2020) sostienen que son:

- Sistema operativo multiusuario, multitarea y multiprocesador.
- El almacenamiento en disco se organiza en sistemas de archivos.
- Los espacios de paginación permiten incrementar la memoria disponible.
- Comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de la RAM física.
- Trabaja con el protocolo de red TCP/IP
- Cada programa en ejecución consta de uno o más procesos, con identificador único y con una relación de parentesco.
- Permite usar bibliotecas enlazadas tanto estática como dinámicamente. (pag.10)

Linux puede manejarse desde una interfaz gráfica o también puede ejecutarse desde línea de comandos. Linux se ha ido perfeccionando gracias al aporte de miles de usuarios que unen sus esfuerzos para poder desarrollar mejoras y como prueba de ello se tienen una gran variedad de distribuciones como son CentOS, Ubuntu, fedora y entre otros.

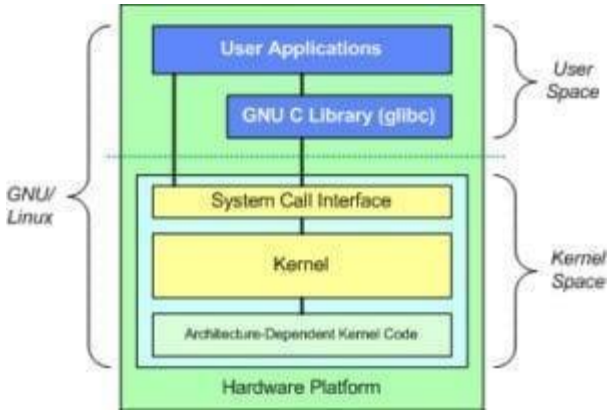

figura 2: Arquitectura fundamental del SO Linux

Fuente: (Guijarro et al. 2020)

CentOS 7 (sistema operativo).

Lance Davis es el creador de CentOS (Community ENTerprise Operating) es una de las distribuciones de Linux que se basa en el código fuente de Red Hat Enterprise Linux. Las versiones nuevas de CentOS son liberadas cada 2 años y cuentan con un periodo de 7 años de actualizaciones de seguridad (Guijarro et al., 2020).

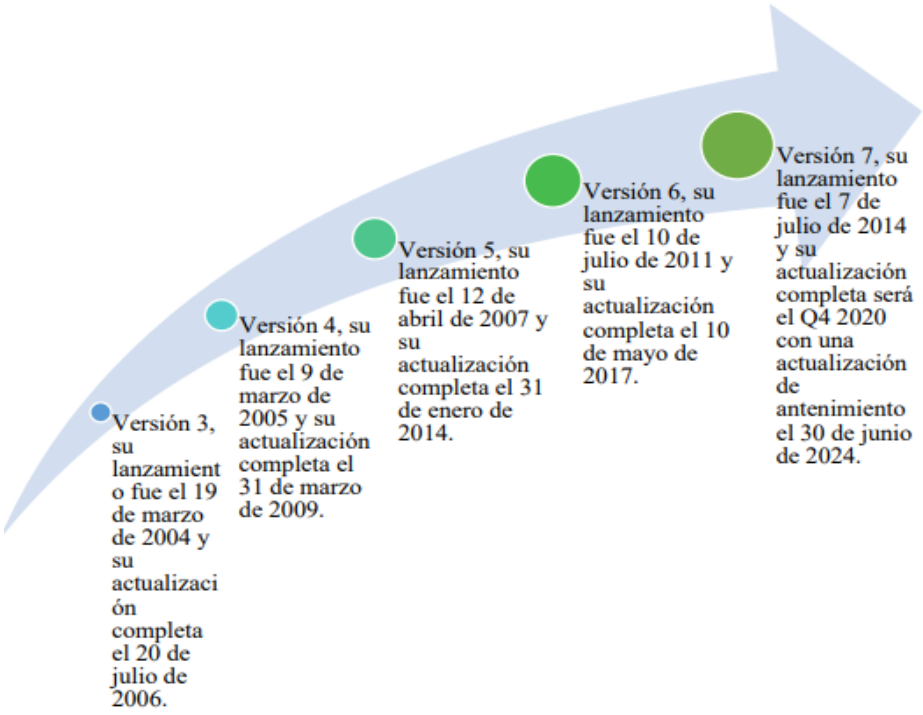

figura 3: Línea de Tiempo CentOS

Fuente: (Guijarro et al. 2020)

MySQL (base de datos).

figura 4: Gestor de Base de Datos MySQL

Fuente: recuperado de: https://www.mysql.com/

Es un sistema de gestión de base de datos de código abierto y el más popular y conocido por su gran rendimiento. Tiene una gran comunidad activa de usuarios que participan en la mejora del servidor.

La gestión de datos se usa desde un simple listado de compras, ventas, nombres, entre otros, así como o también para manejar una gran cantidad de información de empresas.

MySQL usa la consulta estructurada (SQL). Es un lenguaje utilizado por las bases relacionales que nos permiten agregar, modificar y eliminar datos de acuerdo a criterios específicos (López, 2016).

Apache.

Apache es uno de los softwares de servidor web HTTP gratuito de código abierto más antiguos y que a lo largo del tiempo ha ido ganando terreno. Es desarrollado y mantenido por una comunidad de usuarios en torno al Apache Software Foundation.

El servidor Apache brinda contenido de acuerdo a las peticiones que realizan los clientes web es decir cumple la función de repartidor virtual. El servidor apache está disponible para Windows, Mac, Linux y Unix.

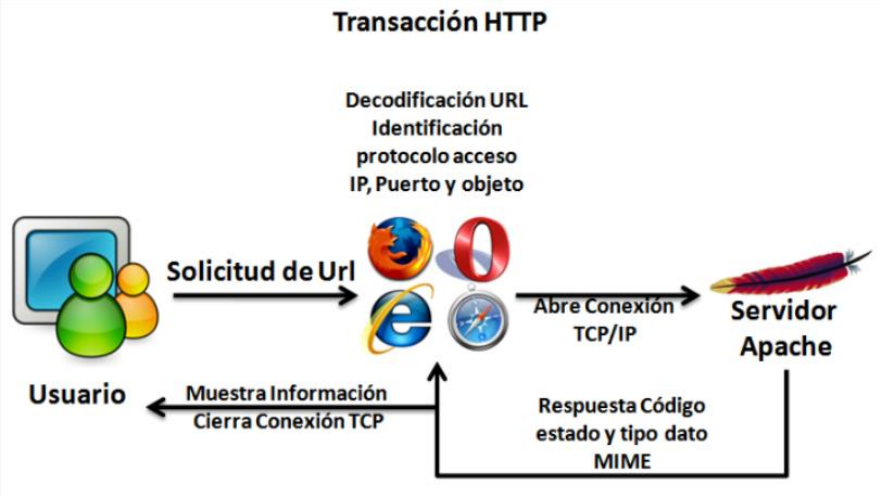

figura 5: Etapas de una Transacción HTTP

Fuente: (Monsalve, 2017)

¿Qué es el ZABBIX?

Es un software de monitoreo gratuito que es distribuido bajo la licencia GPL v2 (Licencia Pública General), fue creado por Alexei Vladishev en un proyecto que inició en Francia y actualmente su sede se encuentra en Letonia.

Zabbix monitorea el rendimiento, disponibilidad e integridad de un servidor. "Esta herramienta que se sirve de mecanismos de comunicación que les permite a los operadores configurar alertas para casi todo tipo de evento fuera de lo común que se dé en algún dispositivo en la red" (Marín, 2017, p.90).

Las características más importantes del Zabbix son las siguientes:

- Recopilación de datos
- Definiciones de umbral flexibles
- Alertas altamente configurables
- Gráficos en tiempo real
- Capacidad de supervisión web
- Almacenamiento histórico de datos
- Fácil configuración
- Uso de plantillas
- Detección de redes

- Interfaz web rápida
- Sistema de permisos

Para el funcionamiento del Zabbix se necesita instalar la aplicación en un servidor, el cual recolectará toda la información de los diferentes equipos para luego presentárnoslo en una interfaz web, en el cual podremos ver la información recolectada en tiempo real en forma de gráficos para facilitarnos el análisis y así mismo ver data histórica. Se podrá observar los estados de cpu, memoria, disco, etc.

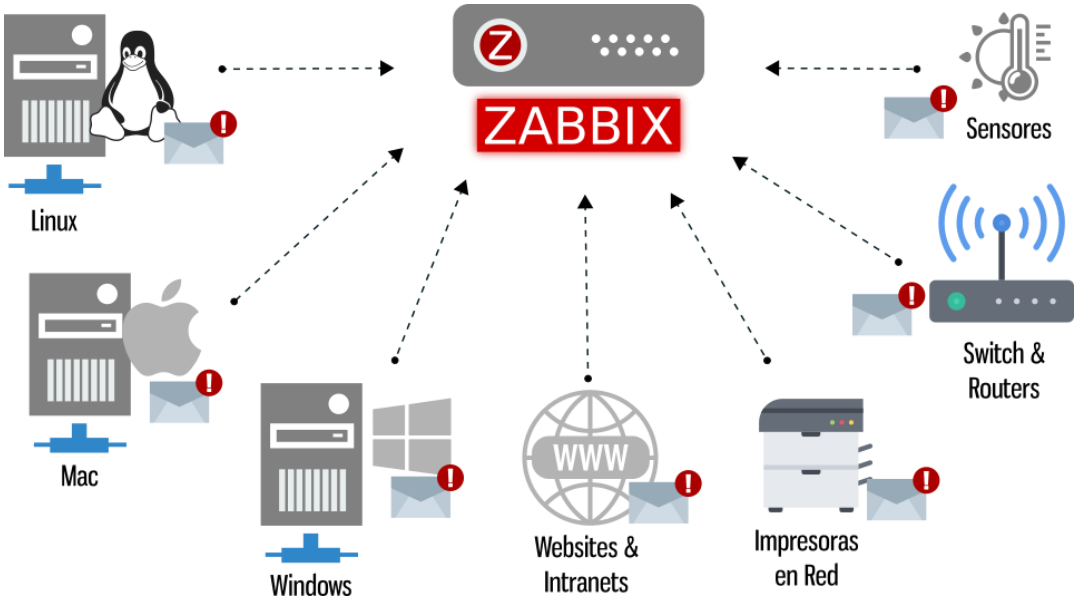

figura 6: Funcionamiento del Zabbix

Fuente: Recuperado de http://911-ubuntu.weebly.com/zabbix_como_funciona

¿Cómo funciona el monitoreo usando el software Zabbix?

El servidor Zabbix (2) recolecta toda la información brindada por los servidores monitoreados (1), para poder visualizar esta información recolectada se tiene que registrar los equipos y dispositivos a través de la interfaz web.

Se le denomina host (3) a un equipo registrado para su respectivo monitoreo, un host está constituido de ítems que son básicamente los módulos que recogen los datos. Los ítems nos permiten indicar qué tipo de información en específico vamos a solicitar al agente Zabbix (1).

Los trigger son módulos que creamos y asociamos a uno o múltiples ítems para evaluar o comparar el umbral que definimos para que se nos pueda disparar una alerta. Cuando se cumplan los requisitos para que se dispare una alerta este se mostrará en la pantalla de administración.

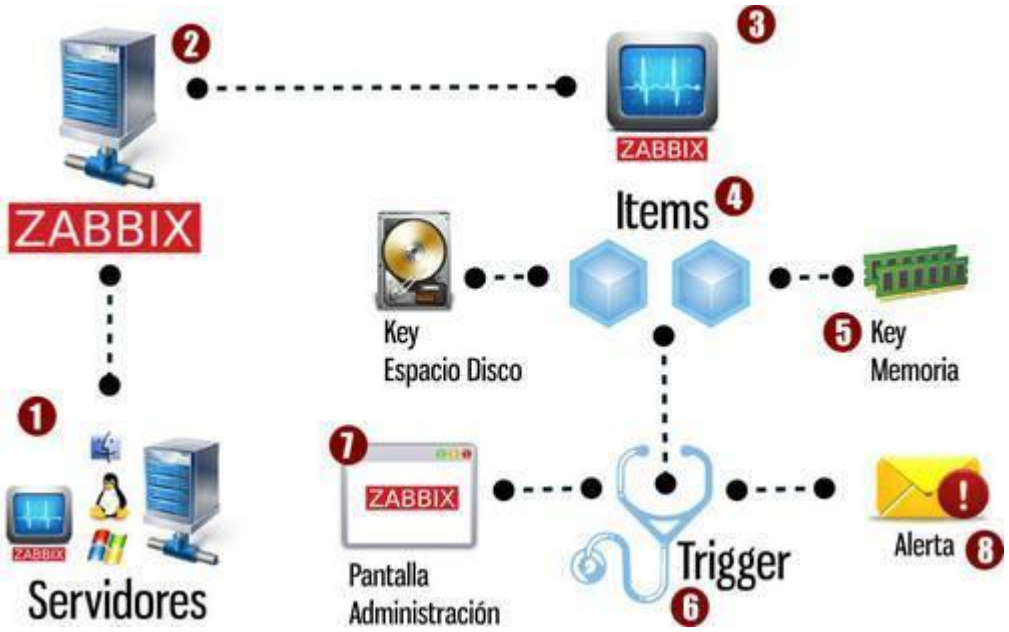

figura 7: ¿Cómo funciona Zabbix?

Fuente: Recuperado de http://911-ubuntu.weebly.com/zabbix_como_funciona

Una vez que nuestro sistema de monitoreo esté en funcionamiento nos informará de cualquier incidente por medio de las alertas que pueden ser sonoras, visuales en la misma herramienta Zabbix o también pueden ser enviados por correo electrónico. También se tendrá la facilidad de monitorear todos los recursos de manera remota.

SNMP o Simple Network Management Protocol.

El protocolo simple de administración de red fue el primer protocolo de gestión creado en el año 1988. Millán (como se citó en Báez, 2017) opina que "Se trata de un protocolo de capa aplicación cuyo origen fue provisional, sin embargo, llegó a convertirse en el estándar de facto debido a su masiva utilización en redes empresariales" (p17). Así como también facilita el intercambio de información entre dispositivos de red.

El SNMP se puede usar para monitorear servidores, ruteadores y otros componentes de red. Naranjo (2016) afirma que: “se puede monitorizar información que pueden ser “simple, como la cantidad de tráfico que entra o sale en una interface, o puede ser algo más complejo como la temperatura del aire dentro de un ruteador” (p20).

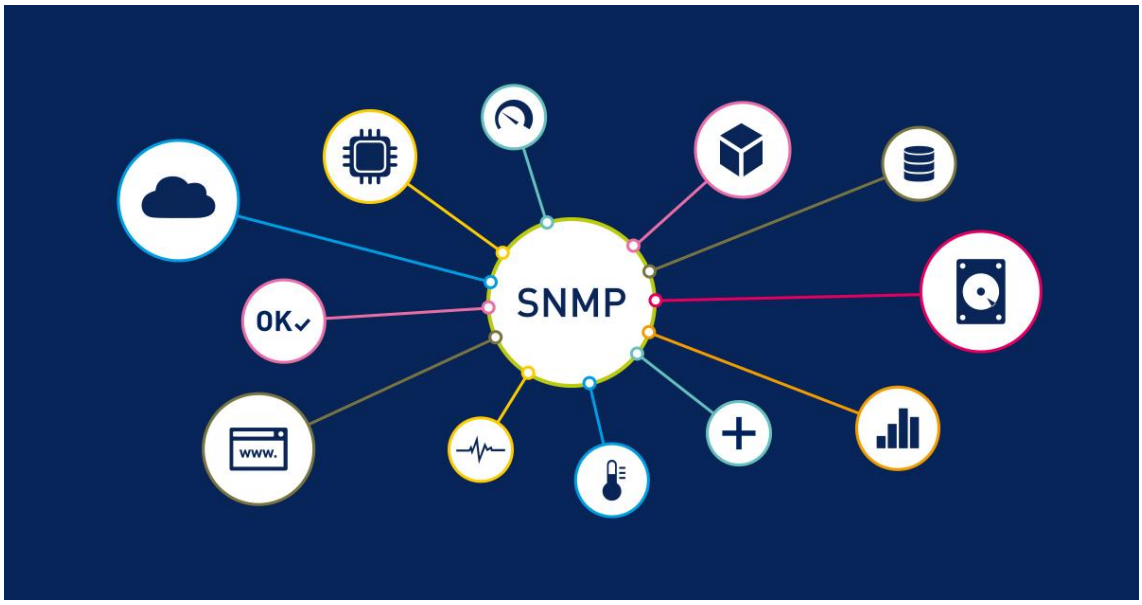

figura 8: SNMP

Fuente: Recuperado de: https://www.es.paessler.com/it-explained/snmp

Los puertos más comunes usados para el SNMP son los siguientes:

- 161-snmp
- 162-snmp-trap

Versiones del SNMP.

SNMP versión 1 (SNMPv1)

Hace su aparición en 1988, proporciona una funcionalidad básica de sondeo de datos y al no tener un algoritmo de cifrado no genera demasiada sobrecarga. Se recomienda usar solo en redes LAN por cuestiones de seguridad. Su principal limitación es que tiene una arquitectura de contador de 32 bits que dificulta la transferencia de grandes volúmenes de datos.

SNMP versión 2 (SNMPv2)

Este protocolo aparece en 1993 como la versión mejorada de snmpv1, mantiene muchas características en común, pero ofrece mejoras con la incorporación de nuevas operaciones de protocolo: como son el GetBulk que ayuda con la recuperación de forma eficiente de grandes volúmenes de datos; Inform para que un agente envíe información al gestor y reciba una confirmación; y Report para que el agente envíe información de los errores y excepciones de protocolo.

SNMP version3 (SNMPv3):

La última versión del SNMP que hace su aparición en 1997 no es un estándar que reemplaza a las versiones anteriores (snmpv1 y snmpv2) sino que incluye nuevas capacidades adicionales como es el de reforzar la prestación de seguridad incluyendo autenticación, privacidad y control de acceso.

Tabla 2

Diferencias SNMP v1, v2 y v3

	SNMPv1	**SNMPv2**	**SNMPv3**
Estándares	RFC-1155.1157.1212	RFC-1441,1452 RFC-1909.1910 RFC-1901 a 1908	RFC-1902 a 1908 RFC-2271 a 2275
Versión	Fue la primera versión de SNMP	SNMPv2 actualmente existe en al menos tres variantes, SNMPv2c, SNMPv2u y SNMPv2	Es la versión más nueva
Seguridad	Ninguna seguridad	No mejoró la seguridad	Su principal característica es la mejora en la seguridad
Complejidad	Limitaciones en rendimiento y seguridad	Más potente pero más complejo que en la primera versión	Se centra en mejorar el aspecto de la seguridad
Tipos de paquetes	Get-Request Get-Next-Request Set Request Get Response	* Get-Request * Get-Bulk Request * Get-Next Request * Set Request * Inform-Response	Las funciones básicas de v3 son de v1 y v2. La versión 3 tiene un nuevo formato de mensaje SNMP

		* SNMP v2 Trap	
Secuencias de Comunidad en texto plano	Si	Si	No
Encriptación de tráfico	No	Si	Si

Fuente: (Baéz, 2017)

¿Cómo funciona SNMP?

La información enviada y recibida entre los administradores y los agentes se comparan con la funcionalidad de la arquitectura cliente servidor. De forma general se necesita instalar un administrador SNMP en una entidad administrativa y los agentes SNMP en dispositivos a administrar.

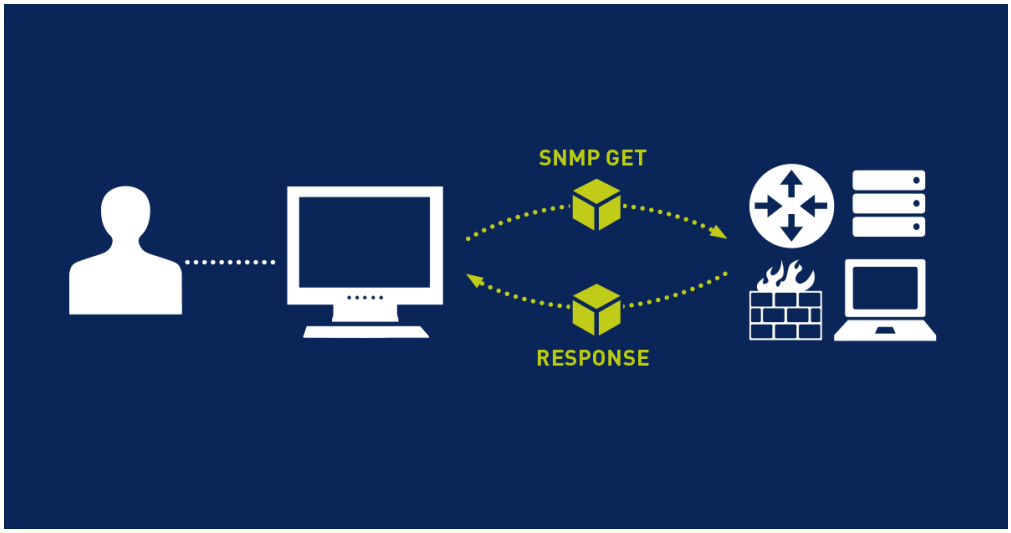

figura 9: Funcionamiento de transferencia de mensajes SNMP

Fuente: Recuperado de https://www.es.paessler.com/it-explained/snmp

La entidad administradora envía una solicitud GET hacia uno o varios dispositivos administrados con la finalidad de obtener una respuesta. Los dispositivos administrados reciben el evento y envían una respuesta RESPONSE con el mensaje del evento solicitado.

Stallings (2004) sostiene que el modelo de gestión SNMP tiene 4 elementos fundamentales:

- Estación de gestión

- Agente de gestión
- Base de información de gestión
- Protocolo de gestión de red

Elementos fundamentales del modelo de gestión SNMP.

La estación de gestión: Funciona como una interfaz mediante el cual el administrador puede acceder al sistema de gestión de red.

Como mínimo contará con una interfaz para que el administrador supervise y controle la red, una base de datos de información con todas las entidades gestionadas en la red, así como también contará con aplicaciones para análisis de datos, recuperación de fallos, etc. (Stallings, 2004).

El agente de gestión: "el agente responde a solicitudes de información y acción provenientes de una estación de gestión y puede, de forma asíncrona, proporcionar a la estación de gestión información importante, aunque no haya sido solicitada" (Stallings, 2004, p.263).

La base de información de gestión (MIB): Ávila (como se citó en Ramírez 2019) opina que "La Management Information Base (MIB) almacenan datos de los dispositivos que se pueden administrar cuya estructura jerárquica está definida en forma de árbol" (p32).

Cada recurso es representado por un objeto y un objeto es en esencia una variable de datos que representa ciertas características específicas del agente gestionando.

El protocolo de gestión de red: Para que la estación gestora se comunique con los agentes lo hace mediante el protocolo de gestión de red. El protocolo TCP/IP que se usa para la gestión de red es el SNMP. El cual tiene las siguientes capacidades fundamentales: get, set y notify (Stallings, 2004).

¿Qué son los OID?

OID que significa Identificador de objetos (Object Identifier) son los que identifican los objetos gestionados que se definen en los archivos MIB. Son definidos por números enteros positivos y su jerarquía es representada como un árbol con diferentes niveles.

Según F5 (2020) sugiere que:

> Los OID identifican entradas individuales u objetos dentro del MIB. Los OID se especifican mediante una convención de nomenclatura "x,y", definida por Abstract Syntax Notation One (ASN.1). En esta convención de nomenclatura, "x" es un valor numérico que identifica la posición de un OID dentro del árbol MIB y "y" es un nombre OID legible por humanos, también llamado nombre de variable. Los OID numéricos facilitan la búsqueda a través del MIB y el informe de información legible por el ser humano.

ICMP o Internet Control Message Protocol.

El protocolo de mensajes de internet cumple la función de enviar mensajes de los errores que ocurren en la red. Este protocolo nace de la necesidad de poder controlar y comprobar la conectividad ya que dentro del conjunto de protocolos IP no existía ninguno que brindara funciones de control.

El protocolo ICMP como ya antes mencionado solamente informa, no corrige las incidencias que pueden presentarse en la entrega de paquetes o de errores de red. Al ser un protocolo de la “capa de Red” en general no es usado para intercambiar información entre equipos, con excepción de algunas herramientas como el ping y traceroute que se usan con fines de diagnóstico.

“Los mensajes ICMP se transmiten como datagramas IP normales, con el campo de cabecera "protocolo" con un valor 1, y comienzan con un campo de 8 bits que define el tipo de mensaje de que se trata” (Becerra, 2016, p.27).

El comando ping comprueba los estados de los equipos remotos, para ello envía paquetes de ECO ICMP al equipo y este recibe paquetes de respuesta eco, de forma predeterminada el comando ping envía 4 paquetes eco de 32 bytes de datos. Todos los paquetes recibidos se comparan con el mensaje emitido.

figura 10: Comando Ping

Fuente: Autoría propia

1.2. Definición de términos básicos

- SNMP: Protocolo simple de administración de red que facilita el intercambio de información.
- ZABBIX: Es un software de monitoreo de código abierto diseñado para la supervisión de redes y aplicaciones.
- GPL: la licencia pública general es una licencia usada en el mundo del software libre.
- TRIGGER: Es un disparador de alerta del Zabbix al cumplir ciertos umbrales definidos.
- SNMP TRAP: Es un tipo de mensaje que contiene información como tiempo de evento y nivel de gravedad.
- LAN: La red de área local es una red que conecta ordenadores dentro de un área pequeña.
- RFC: Son documentos que hacen referencia a protocolos y tecnologías de internet.
- MIB: Contiene información jerárquica y estructurada en forma de árbol de dispositivos gestionados en una red.
- TCP/IP: Es un conjunto de protocolos que se emplean para transferir datos por internet.
- OID: Es una secuencia de números que nos permiten identificar objetos en la red.

- ASN1: Es un protocolo que usa el SNMP para representar sus objetos gestionables.
- ICMP: Es un protocolo que permite administrar errores de red.
- IP: Es un protocolo de Internet que se encarga de establecer comunicación con casi todas nuestras redes.

CAPÍTULO II: METODOLOGÍA DE DESARROLLO DEL TRABAJO PROFESIONAL

2.1. Delimitación temporal y espacial del trabajo

Delimitación Temporal.

Los datos considerados para el trabajo de investigación serán considerados durante el periodo 2020.

Delimitación Espacial.

El trabajo de investigación se enfoca en optimizar la atención de incidencias de Helpdesk para el área del SOC de la empresa Securesoft, que se encuentra ubicado en el departamento de Lima, provincia de lima, Distrito de Santiago de Surco.

2.2. Determinación y análisis del problema

Las organizaciones en la actualidad están muy ligadas a las tecnologías de información ya que es un elemento muy determinante en el éxito de las organizaciones. Algunas de las organizaciones tienen sedes esparcidas en diferentes ubicaciones geográficas y para ello deben de tener la capacidad de examinar el estado actual hasta de la oficina más remota con un botón.

A medida del avance tecnológico y crecimiento de las organizaciones, el uso de las tecnologías de información aumenta y por ende también aumenta la dificultad de la gestión de los mismos, al tener una gran cantidad de dispositivos se hace complicado poder verificar que todos ellos se encuentren en correcto funcionamiento.

Frente a ello el producirse una falla puede causar que los empleados no puedan laborar o cumplir sus funciones de forma correcta, los usuarios pueden quedar incomunicados, así como también no podrían acceder a informaciones que son importantes para la empresa.

La problemática que se observa dentro de la empresa Securesoft, específicamente en el área del SOC es la no detección oportuna de los incidentes que se presentan y como consecuencia se tarda un mayor tiempo en la solución de la misma. Por tal motivo se realizó una encuesta a los

Analistas para verificar los problemas relacionados a lo antes expuesto, a continuación, se detalla la información recolectada por la encuesta.

Tabla 3

Tiempo de detección de un Incidente

TIEMPO DE DETECCIÓN DE UN INCIDENTE	USUARIOS	PORCENTAJE (%)
5 - 19 min	0	0%
20-39 min	1	10%
41 - 59 min	4	40%
más de 60 min	5	50%

fuente: Autoría Propia

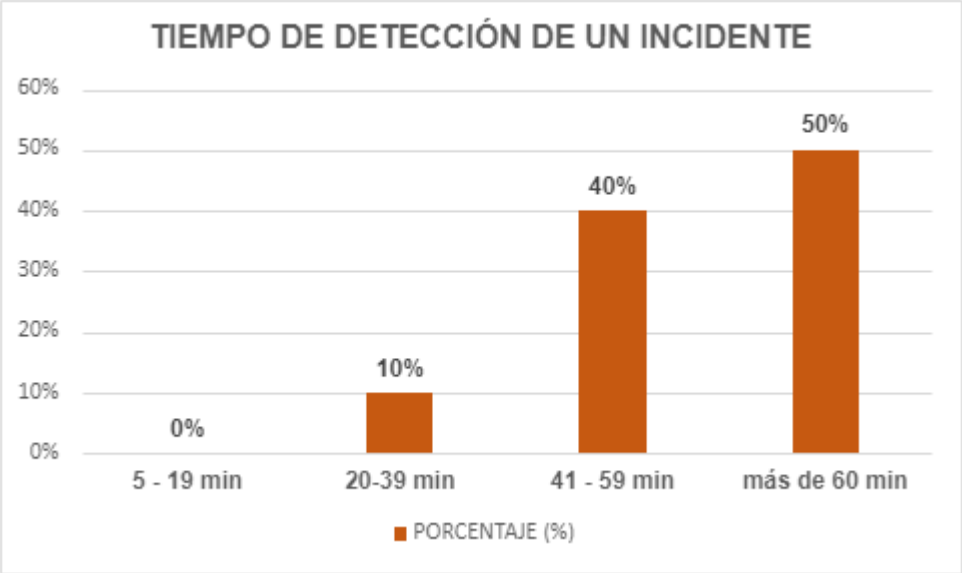

figura 11: Tiempo de detección de un incidente

fuente: Autoría Propia

De los resultados a la pregunta realizada, se determina que para el 50% de los encuestados opinaron que el tiempo de detección de un incidente es más de 60 min, el 40% de los encuestados opinaron que están entre 41 a 60 min y para el 10% de los encuestados están entre 20 a 39 min. En conclusión, para los usuarios la detección de un incidente se tarda más de 41 min.

Tabla 4

Importancia de la prevención y anticipación de incidentes

IMPORTANCIA DE LA PREVENCIÓN Y ANTICIPACIÓN DE INCIDENTES	USUARIOS	PORCENTAJE (%)
Bajo	0	0%
Medio	0	0%
Alto	10	100%

Fuente: Autoría propia

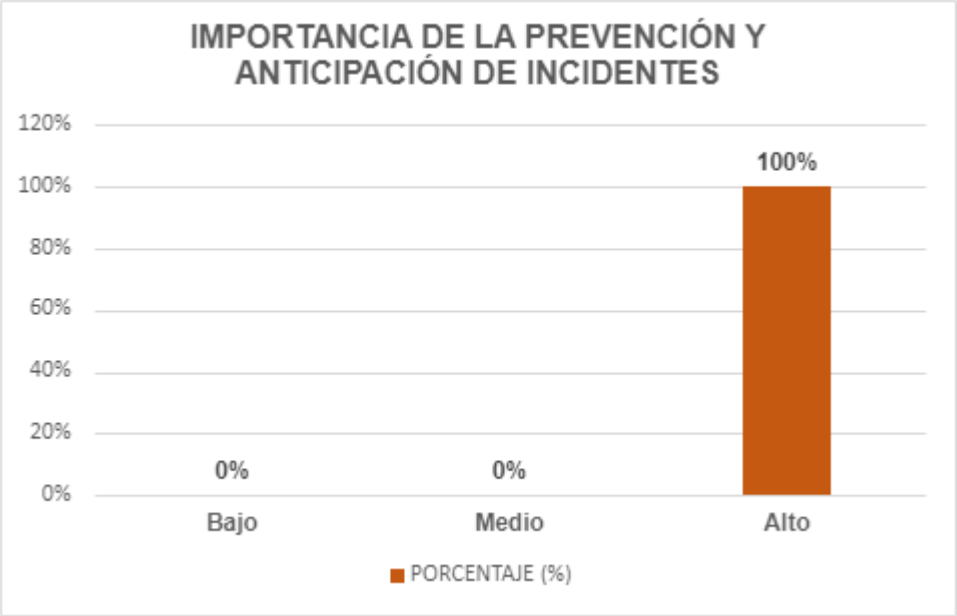

figura 12: Importancia de la prevención y anticipación de incidentes

Fuente: Autoría propia

De los resultados a la pregunta realizada, se determina que para el 100% de los encuestados opinaron que la importancia de la prevención y anticipación de incidentes es de nivel alto. En conclusión, para los usuarios es muy importante la prevención y anticipación de incidentes.

Tabla 5

Importancia del mantenimiento planificado del hardware

IMPORTANCIA DEL MANTENIMIENTO PLANIFICADO DEL HARDWARE	USUARIOS	PORCENTAJE (%)
Bajo	0	0%
Medio	3	30%
Alto	7	70%

Fuente: Autoría propia

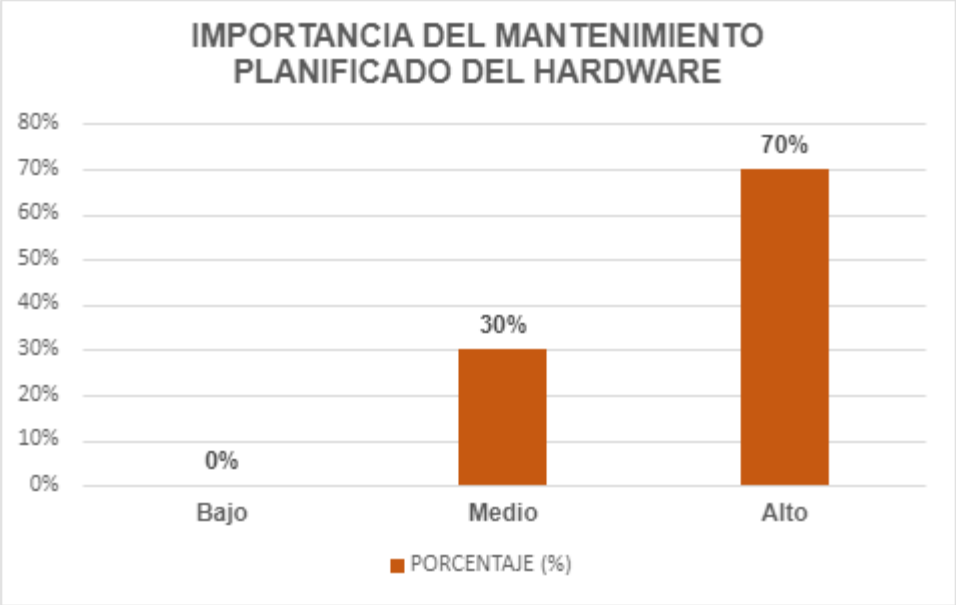

figura 13: Importancia del mantenimiento planificado del hardware

Fuente: Autoría propia

De los resultados a la pregunta realizada, se determina que para el 70% de los encuestados opinaron que el mantenimiento planificado tiene importancia alta, para el 30% el mantenimiento planificado tiene una importancia media. En conclusión, el mantenimiento planificado de hardware tiene una importancia alta.

Tabla 6

Influye la detección temprana de un incidente en el tiempo de solución

INFLUYE LA DETECCIÓN TEMPRANA EN EL TIEMPO DE SOLUCIÓN	USUARIOS	PORCENTAJE (%)
Si	10	100%
No	0	0%

Fuente: Autoría propia

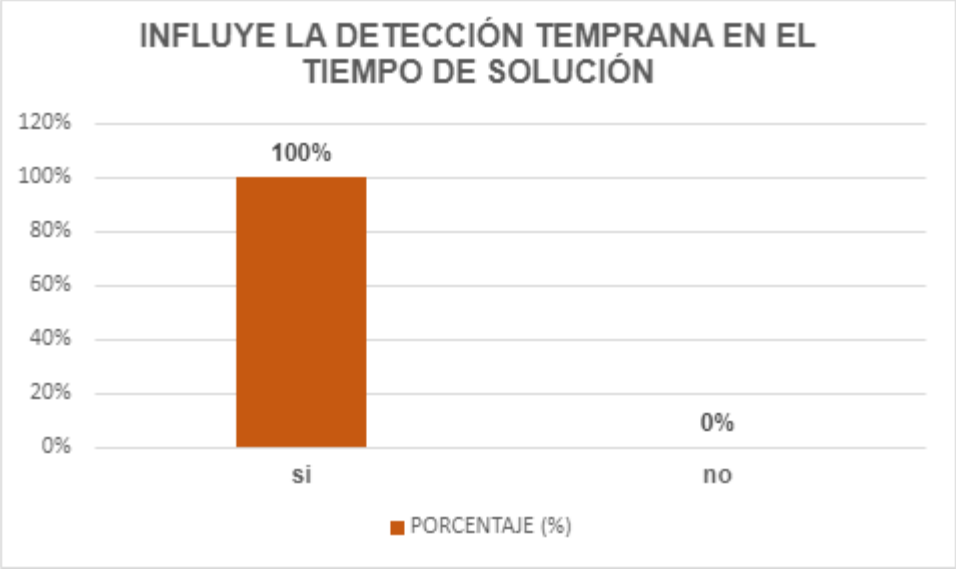

figura 14: Influye la detección temprana de un incidente en el tiempo de solución

Fuente: Autoría propia

De los resultados a la pregunta realizada, se determina que para el 100% de los encuestados opinaron que la detección temprana de un incidente influye en el tiempo de solución de la misma.

Tabla 7

Seguimiento realizado a incidencia

SEGUIMIENTO REALIZADO A INCIDENCIA	USUARIOS	PORCENTAJE (%)
Bajo	0	0%
Medio	8	80%
Alto	2	20%

Fuente: Autoría propia

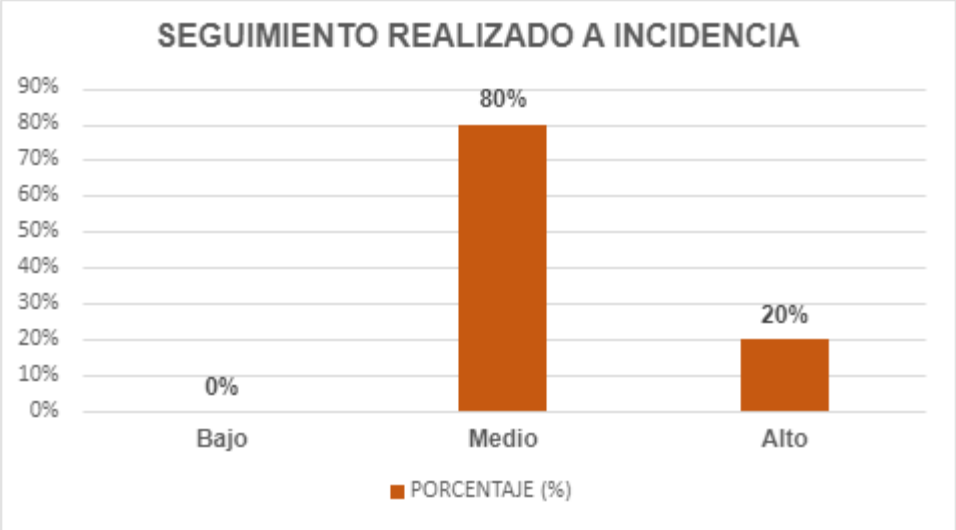

figura 15: Seguimiento realizado a incidencia

Fuente: Autoría propia

De los resultados a la pregunta realizada, se determina que para el 80% de los encuestados opinaron que el seguimiento de su incidencia lo califican como medio y para el 20% de los encuestados el seguimiento de su incidente es calificado como alto. En conclusión, el seguimiento realizado a una incidencia está calificado como medio.

A continuación, detallaremos la función que cumple el operador dentro del área del SOC. El operador cumple la función de responder a los requerimientos de los clientes y en base al análisis del requerimiento derivar a un área especializada para la solución de la misma.

Para brindar los servicios de forma óptima hacia los clientes, las diferentes plataformas web, aplicativos y ordenadores que se usan deben de estar disponibles las 24 horas del día, los 7 días de la semana. La indisponibilidad de cualquiera de ellos trae como consecuencia un retraso en la entrega de solución de los requerimientos solicitados por el cliente.

Por tal motivo es muy importante una detección temprana de cualquier incidente que pueda perjudicar el flujo normal de los servicios brindados hacia los clientes. Por ello se propone monitorear las diferentes plataformas web, aplicativos y ordenadores para así poder alertar al área de helpdesk de forma rápida y así ellos poder brindarnos una solución temprana.

2.3. Modelo de solución propuesto

Una vez definido el problema, se propone la siguiente alternativa como posible solución:

Monitoreo de los dispositivos, aplicaciones y páginas web usando el Zabbix: con esto nos referimos a que con el monitoreo de las distintas plataformas se tendrá una mayor visibilidad y detección desde el instante que la plataforma deje de estar disponible. Con ello derivar al área de helpdesk para la atención pronta del incidente.

Para la realización del proyecto se manejó el siguiente cronograma de actividades que está segmentado por semanas, así como también el detalle de las actividades con fecha de inicio y fin. En total la cantidad de días para la culminación del proyecto es de 80 días, iniciando el 03/08/20 y culminando el 20/11/20.

Nombre de Tarea	agosto				setiembre				octubre					noviembre		
	1ra	2da	3ra	4to	1ra	2da	3ra	4ta	1ra	2da	3ra	4ta	5ta	1ra	2da	3ra
INICIO																
Recolección de requerimientos	x	x	x													
PLANEACION																
Cronograma			x													
Declaracion de Alcances			x	x												
Diseño de diagrama de flujo				x	x											
Matriz de escalamiento					x	x										
EJECUCION																
Elaboración del módulo en Zabbix						x	x									
Enganchar equipos al Zabbix							x	x	x	x						
Configurar Triggers										x	x	x				
CONTROL																
Pruebas de alertas													x	x		
Validación data histórica														x	x	
CIERRE																
cerrar proyecto																X

figura 16: Cronograma de actividades

Fuente: Autoría propia

Tabla 8

Cronograma de actividades con fecha detallada

Nombre de tarea	Duración	Comienzo	Fin
INICIO	**15 días**	**lun 3/08/20**	**vie 21/08/20**
Recolección de requerimientos	15 días	lun 3/08/20	vie 21/08/20

PLANEACIÓN	**20 días**	**lun 17/08/20**	**vie 11/09/20**
Cronograma	5 días	lun 17/08/20	vie 21/08/20
Declaración de alcances	10 días	lun 17/08/20	vie 28/08/20
Diseño de diagrama de flujo	10 días	lun 24/08/20	vie 4/09/20
Matriz de escalamiento	10 días	lun 31/08/20	vie 11/09/20
EJECUCIÓN	**35 días**	**lun 7/09/20**	**vie 23/10/20**
Configuración del módulo en Zabbix	10 días	lun 7/09/20	vie 18/09/20
Enganchar equipos al Zabbix	20 días	lun 14/09/20	vie 9/10/20
Configurar Triggers	15 días	lun 5/10/20	vie 23/10/20
CONTROL	**15 días**	**lun 26/10/20**	**vie 13/11/20**
Pruebas de alertas	10 días	lun 26/10/20	vie 6/11/20
Validación de data histórica	10 días	lun 2/11/20	vie 13/11/20
CIERRE	**5 días**	**lun 16/11/20**	**vie 20/11/20**
Cerrar proyecto	5 días	lun 16/11/20	vie 20/11/20

Fuente: Autoría propia

Metodología para desarrollo del proyecto.

Una vez ya definido las plataformas y dispositivos que se desean monitorear y los umbrales, se procederá con el desarrollo del proyecto. La metodología usada en el proyecto será la metodología en prototipo, se procederá con instalar y después a ello con aplicar prueba y error para las necesidades que vayan surgiendo en el transcurso del tiempo (Quispe, 2018).

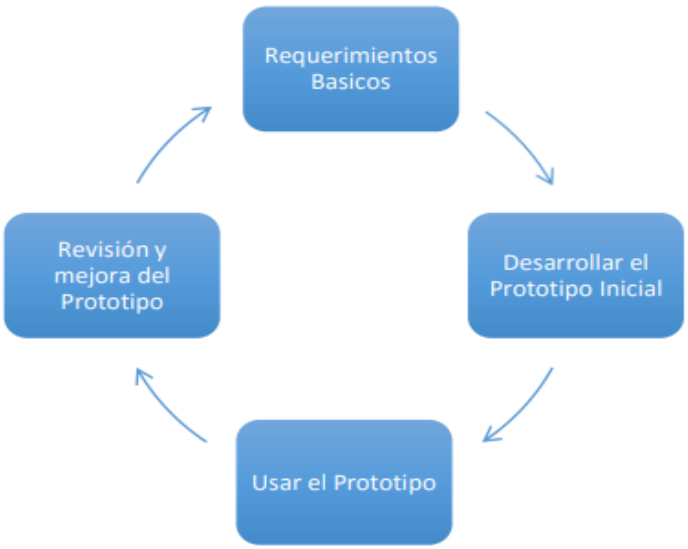

figura 17: Ciclo de vida de un prototipo

Fuente: (Quispe, 2018)

De acuerdo con las necesidades del área del SOC, se necesita tener la gran mayoría de las plataformas y dispositivos con disponibilidad alta, por ello es necesario un sistema que permita detectar si algún dispositivo está fallando.

La disponibilidad en este caso se verificará verificando que haya comunicación con el equipo.

CPU: verificar la cantidad de cpu usado o libre en el equipo.

Memoria: verificar la cantidad de memoria usada o libre en el equipo.

Disco: verificar el espacio disponible en todos los discos del equipo.

Red: verificar si existe conexión hacia el equipo

Las alertas se categorizaron por criticidad, de acuerdo al impacto que genera el incidente dentro del área de trabajo. Para identificar de forma más rápida el nivel de criticidad del incidente, se utilizarán colores asignados de acuerdo a la severidad de la alerta, a continuación, se detalla las alertas por colores.

Tabla 9

Criticidad de alertas observadas en el Zabbix

SEVERIDAD	DESCRIPCIÓN
DISASTER	El Host no tiene conexión a red
HIGH	El servicio supera o iguala los umbrales considerados altos
WARNING	El servicio supera o iguala los umbrales considerados como advertencia
INFORMATION	Alerta informativa

Fuente: Autoría Propia

Para el usuario se tiene una interfaz amigable en la cual se puede observar los distintos dispositivos, plataformas que se están monitoreando. Esta interfaz es muy útil ya que puede observar el estado de todos los equipos monitoreados en un intervalo de tiempo.

Asimismo, generar reportes de los equipos con la información recolectada y esta información será mostrada en forma de gráfico para un mejor análisis.

Para el monitoreo de recursos de los equipos se definió de forma estándar umbrales que deben de cumplir para gatillar las alertas.

Tabla 10

Umbrales para gatillar alertas referentes a estados de recursos

RECURSO	Umbral en %	SEVERIDAD
CPU	95%	Disaster
CPU	90%	High
CPU	80%	Warning
MEMORIA	95%	Disaster
MEMORIA	90%	High
MEMORIA	80%	Warning
DISCO	95%	Disaster
DISCO	90%	High
DISCO	-	-

Fuente: Autoría propia

Para la recolección de información de los equipos, se usó el agente SNMP el cual obtiene la información de estados de los dispositivos, uso de CPU, uso de memoria, espacio disponible en el disco, estado de conexión de las plataformas.

Herramientas utilizadas.

Las herramientas utilizadas para el presente proyecto de investigación serán los siguientes:

Tabla 11

Plataformas de instalación del Zabbix

ZABBIX VERSION	DISTRIBUCIÓN DEL SISTEMA OPERATIVO	VERSIÓN DEL SISTEMA OPERATIVO	BASE DE DATOS	SERVIDOR WEB
4.0 LTS	CentOS	7	Mysql	Apache

Fuente: Autoría propia

Zabbix versión 4.0

El software gratuito Zabbix se utilizará para el monitoreo de las diferentes plataformas web, aplicativos y ordenadores. Se utilizará la versión Zabbix 4.0 dentro de los cuales se mencionan las funcionalidades de mayor importancia de la versión.

- Visualización mejorada
- Escalabilidad y rendimiento
- Permisos basados en etiquetas
- Inicio de sesión único

CentOS 7

Los sistemas operativos CentOS es uno de los más populares en el sector web de código abierto. Se utilizará CentOS como nuestro servidor de código abierto.

Principales ventajas de usar CentOS Linux.

- Reducción de costos al ser de distribución gratuita.
- Seguridad, solo el administrador puede realizar cambios importantes y no se le puede ocultar ningún archivo.
- Estabilidad, su capacidad de poder ejecutar una gran cantidad de procesos al mismo tiempo.
- Comunidad de programadores

MySQL

Es un gestor de base de datos de código abierto que se puede ejecutar en los distintos sistemas operativos incluyendo Windows, Linux, UNIX ya que cuenta con una gran compatibilidad.

Por tal motivo se usará Mysql para gestionar la información recopilada a través de la herramienta Zabbix.

Apache Server

Es un software de servidor web gratuito y de código abierto, muy usado para la ejecución de sitios web. Se utilizará el servidor web Apache por la compatibilidad con el software de monitoreo Zabbix.

2.4. Resultados

Se realizó un diagrama de flujo para los incidentes para así tener un mejor panorama de todo el flujo que sigue un incidente durante todo su recorrido hasta su solución.

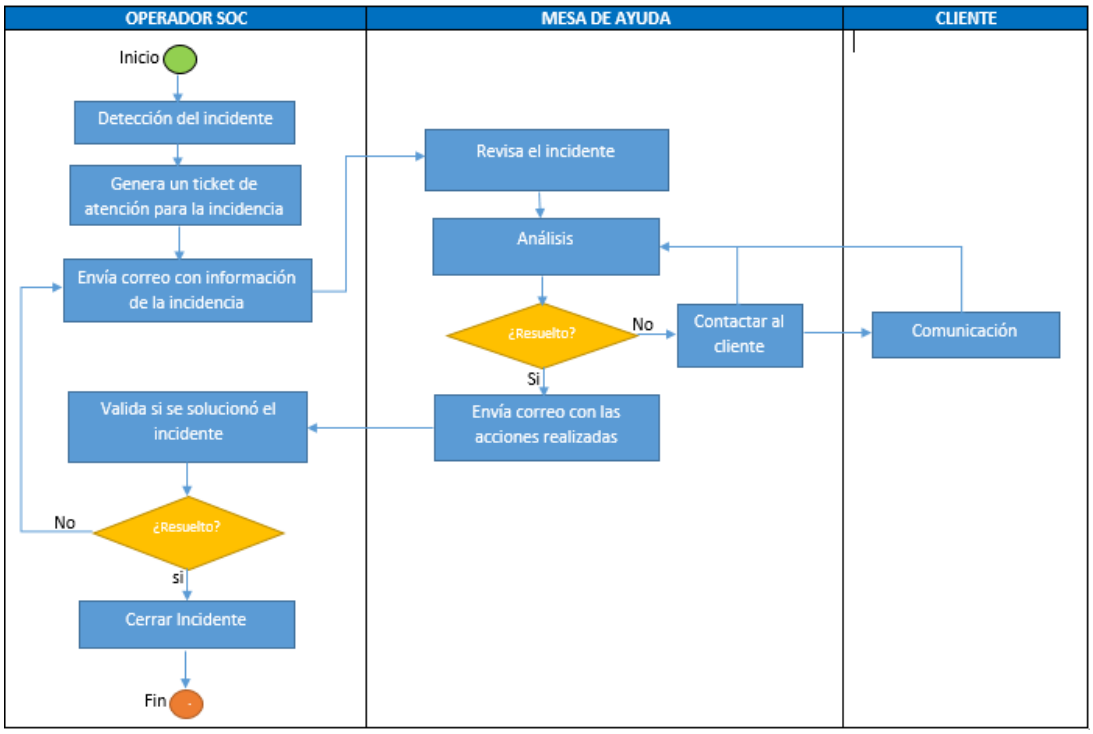

figura 18: Diagrama de flujo de Incidentes

Fuente: Autoría Propia

De igual forma se realizó un cuadro con la matriz de escalamiento a seguir cuando no se obtiene respuesta o solución en el tiempo pactado. La siguiente matriz de escalamiento se utilizará para los incidentes críticos que afecten los servicios para con el cliente.

Tabla 12

Matriz de Escalamiento de Incidentes

TIEMPO	Descripción	CARGO
0 – 19 min	Notificación del incidente por correo y asignación del ticket	Operador SOC
20 – 30 min	No se obtiene respuesta o solución. Escalar con ***Administrador de Red*** y copiar en el correo a ***Supervisor de SOC***	Administrador de Red - Supervisora de SOC
30 – 40 min	No se obtiene respuesta o solución. Escalar con ***Jefe de soporte nivel 2*** y copiar en el correo a ***Supervisor de ciberseguridad***	Jefe de soporte nivel 2 - Supervisor de ciberseguridad
40 – 60 min	No se obtiene respuesta o solución. Escalar con ***Gerente de Ingeniería*** y copiar en el correo a ***Gerente de CyberSOC y Ciberinteligencia***	Gerente de Ingeniería - Gerente de CyberSOC y Ciberinteligencia
60 – 70 min	No se obtiene respuesta. Escalar con ***Gerente General de SecureSoft***	Gerente General de SecureSoft

fuente: Autoría Propia

A continuación, se detalla la encuesta realizada a los operadores después de la implementación del Zabbix.

Tabla 13

Tiempo de detección de un incidente utilizando Zabbix

TIEMPO DE DETECCIÓN DE UN INCIDENTE UTILIZANDO ZABBIX	USUARIOS	PORCENTAJE (%)
5 - 19 min	6	100%
20-39 min	0	0%
41 - 59 min	0	0%
más de 60 min	0	0%

fuente: Autoría Propia

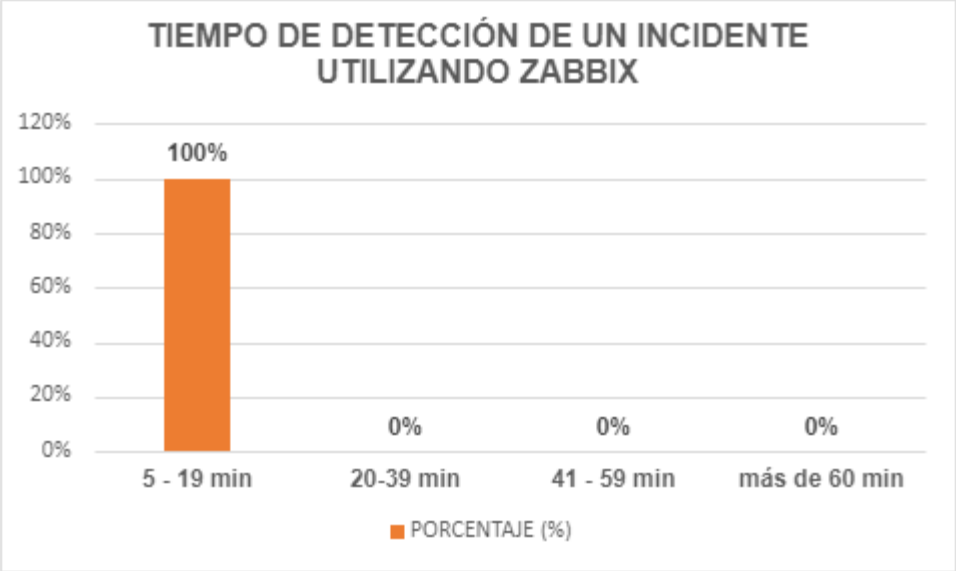

figura 19: *Tiempo de detección de un incidente utilizando Zabbix*

fuente: Autoría Propia

Interpretación:

El 100% de los encuestados opinan que después de la implantación del software Zabbix el tiempo de detección de un incidente se encuentra entre 5 a 19 min, llegando a la conclusión que se observa una mejora significativa en la detección de un incidente usando Zabbix.

Tabla 14

Calificación de que tan amigable es la interfaz de Zabbix

SIMPLICIDAD DE LA INTERFAZ DE ZABBIX	USUARIOS	PORCENTAJE (%)
Bajo	0	0%
Medio	3	50%
Alto	3	50%

Fuente: Autoría propia

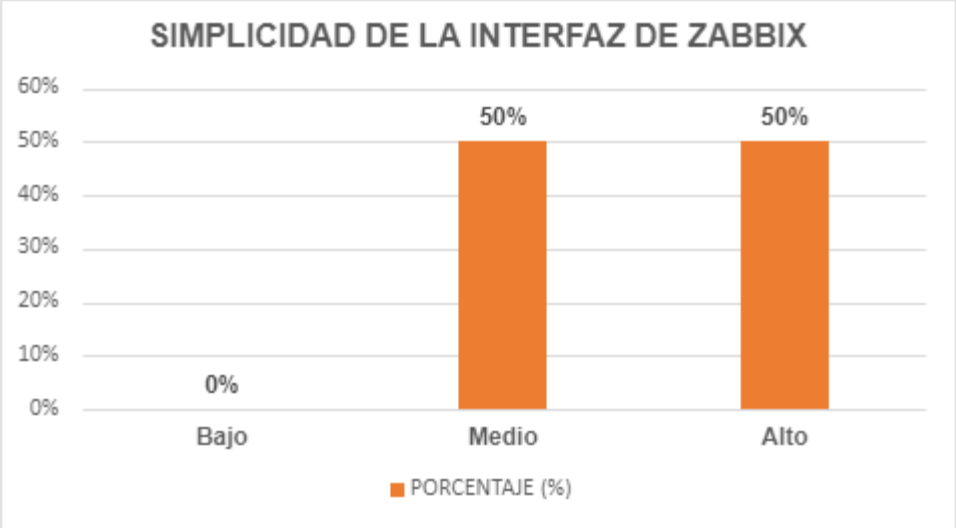

figura 20: Calificación de que tan amigable es la interfaz de Zabbix

Fuente: Autoría propia

Interpretación:

El 50% de los encuestados opinan que la interfaz del Zabbix es medianamente amigable, el 50% de los encuestados opinan que la interfaz del Zabbix es altamente amigable e intuitiva. En conclusión, la interfaz del Zabbix es mediano alto amigable e intuitivo.

Tabla 15

Dificultad para agregar nuevos usuarios al Zabbix

DIFICULTAD PARA AGREGAR NUEVOS USUARIOS	USUARIOS	PORCENTAJE (%)
Fácil	1	16.7%
Regular	4	66.7%
Difícil	1	16.7%

Fuente: Autoría propia

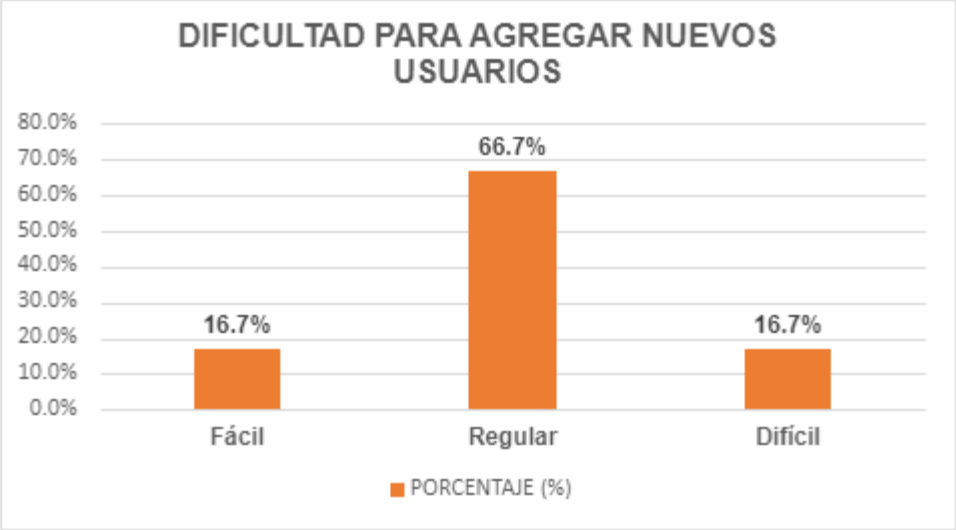

figura 21: Dificultad para agregar nuevos usuarios al Zabbix

Fuente: Autoría propia

Interpretación:

El 66.7% de los encuestados opinan que el agregar un nuevo usuario tiene una dificultad media, el 16.7% opina que agregar un nuevo usuario es fácil y el 16.7% opina que agregar un nuevo usuario es difícil. En conclusión, el agregar un nuevo usuario tiene una dificultad media.

Tabla 16

Solución de incidentes antes de ocurrir alguna falla

SOLUCIÓN DE INCIDENTES ANTES DE OCURRIR ALGUNA FALLA	USUARIOS	PORCENTAJE (%)
Si	4	66.7%
No	2	33.3%

Fuente: Autoría propia

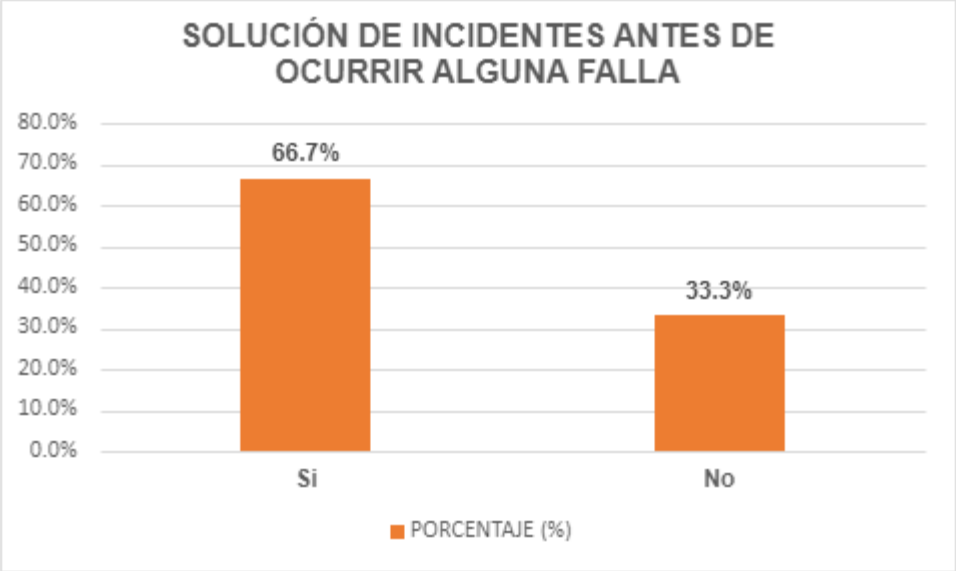

figura 22: Solución de incidentes antes de ocurrir alguna falla

Fuente: Autoría propia

Interpretación:

El 66.7% de los encuestados opinan que solucionaron un incidente antes de ocurrir alguna falla, el 33.3% de los encuestados opina que no se pudo prever el incidente y esto conllevo a que fallara. En conclusión, para la gran mayoría de los incidentes se pudo prever y solucionar antes de que ocurra alguna falla.

Tabla 17

Monitoreo con Zabbix cumple las funciones esperadas

MONITOREO CON ZABBIX CUMPLE LAS FUNCIONES ESPERADAS	USUARIOS	PORCENTAJE (%)
Si	6	100.0%
No	0	0.0%

Fuente: Autoría propia

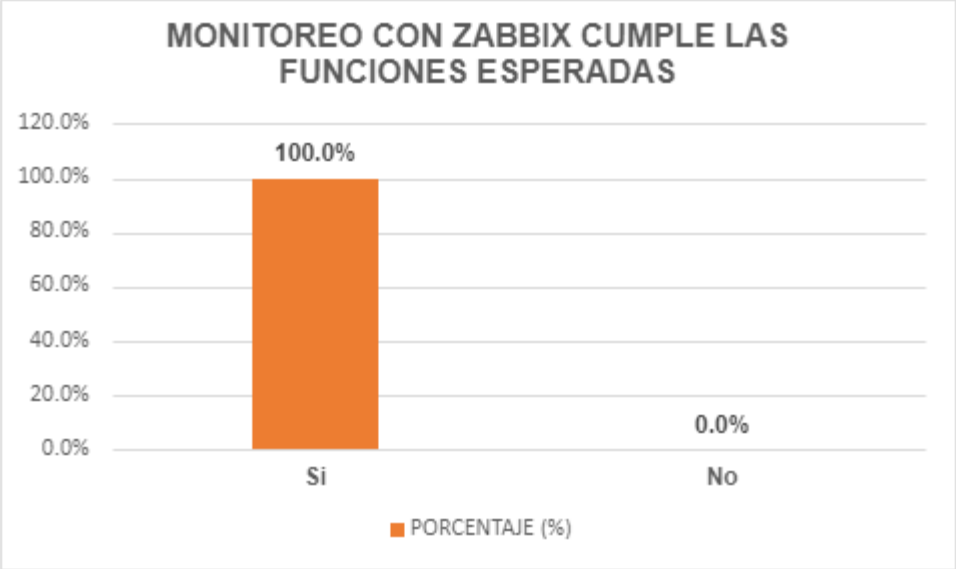

figura 23: Monitoreo con Zabbix cumple las funciones esperadas

Fuente: Autoría propia

Interpretación:

El 100% de los encuestados opinan que el monitoreo usando Zabbix cumple con las funciones esperadas.

Tabla 18

Diagrama de flujo y matriz de escalamiento para la gestión de incidentes

DIAGRAMA DE FLUJO Y MATRIZ DE ESCALAMIENTO AYUDA EN LA GESTION DE INCIDENTES	USUARIOS	PORCENTAJE (%)
Si	6	100.0%
No	0	0.0%

Fuente: Autoría propia

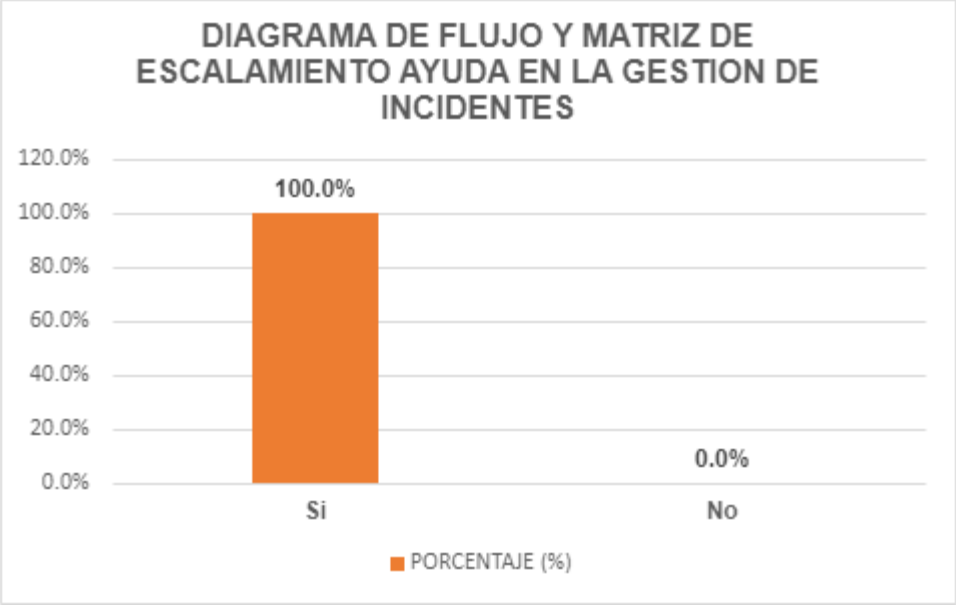

figura 24: Diagrama de flujo y matriz de escalamiento para la gestión de incidentes

Fuente: Autoría propia

Interpretación:

El 100% de los encuestados opinan que el diagrama de flujo y matriz de escalamiento ayuda en gran medida en la gestión de incidentes.

CONCLUSIONES

- Se realizó la configuración de un módulo en el Zabbix para el monitoreo de los recursos informáticos, mediante el cual se observa una disminución en el tiempo de detección de incidentes a un promedio de 5 a 19 min.
- Se utilizó el protocolo SNMP para el intercambio de datos y así poder realizar un monitoreo de los recursos informáticos.
- Se realizó el diseño de un modelo para la gestión de incidencias, para un mejor manejo y escalamiento frente a incidentes.

RECOMENDACIONES

- Se recomienda la utilización de software o herramientas de código abierto si se tiene un presupuesto de inversión limitada para la adquisición de software de monitoreo.
- Se recomienda evaluar las diferentes herramientas de software libre para el monitoreo ya que poseen un gran potencial para complementar el monitoreo.
- Se recomienda actualizar la versión del Zabbix ya que por cada versión se agrega mejoras y nuevas funcionalidades como el servicio Cloud.
- Finalmente, para los siguientes investigadores se recomienda implementar la notificación de alertas hacia el móvil mediante la aplicación Telegram.

BIBLIOGRAFÍA

Aguilar Prieto, G. (2017). *Estrategia de mejora para los servicios de gestion de incidencias y problemas ofrecidos por el Centro de Gestión Informática del Hospital San Vicente de Paúl.* (tesis maestria), Universidad Nacional Costa Rica, Heredia, Costa Rica.

Báez Cheza, J. E. (2017). *Diseño e implementación de un modelo de gestión de red para la red de área local del edificio central de la Universidad Técnica del Norte en base al Modelo de Géstion OSI con el Protocolo SNMP.* (tesis posgrado), Universidad Técnica del Norte, Ibarra, Ecuador.

Becerra Orrala, E. D. (2016). *Implimentacion de monitoreo de red utilizando los protocolos ICMP y SNMP.* (tesis posgrado), La Libertad, Ecuador.

F5. (31 de agosto de 2020). *f5 Glosario*. Obtenido de https://www.f5.com/es_es/services/resources/glossary

Guijarro Rodríguez, A. A., Molina Calderón, M. A., Galarza Soledispa, M. I., & Trejo Alarcón, J. E. (2020). *Principios Básicos de GNU/Linux CentOS 7.* Ecuador: Colloquium.

Lancheros Padilla, L. (2016). *Implementación de la Herramienta de Software Libre GLPI para Sistematizar la Mesa de Ayuda (Help Desk) del hospital Infantil Universitario de San José.* (tesis postgrado), Fundación Universitaria Los Libertadores, Bogotá, Colombia.

López Herrera, P. (2016). *Comparación del desempeño de los Sistemas Gestores de Bases de Datos MySQL y PostgreSQL.* (Tesis Postgrado), Universidad Autónoma del Estado de México, Texcoco, México.

Marín Santana, C. J. (2017). *Implementacion de un sistema de sensores, monitoreo y alertas de la tempreatura y humedad de un centro de datos.* (tesis postgrado), Universidad de Guayaquil, Guayaquil, Ecuador.

Monsalve Pulido, J. A. (2017). Web usage mining aplicado a servidores web apache. *PERSPECTIV@S, 14*(13), 25-30.

Naranjo Romero, J. (2016). *Estudio comparativo de factibilidad del uso de herramientas de Contro de Dispositivos y Servicios de Res de Datos mediante el Protocolo SNMP y Software Libre.* (tesis postgrado), Universidad de Guayaquil, Guayaquil, Ecuador.

Quispe Bustincio, J. W. (2018). *Implementación de un Sistema de Monitoreo y Control de Red, para un canal de Televisión, basado en herramientas Open Source y Software Libre, Lima - 2017.* (tesis postgrado), Universidad Nacional del Altiplano, Puno, Perú.

Ramirez Diaz, E. Y. (2019). *Alternativas de configuración con el uso de protocolos Syslog y SNMP para la gestion de Red de Redes Avanzadas.* (tesis postgrado), Universidad Nacional Agraria de la Selva, Tingo María, Perú.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes. Aplicaciones y Estándares* (Segunda ed.). Madrid, España: Pearson Educación, S.A.

Stallman, R. M. (2004). *Sofware libre para una sociedad libre.* Madrid, España: Traficantes de Sueños.

Zabbix. (29 de agosto de 2020). *Documentacion de zabbix 5.0*. Obtenido de https://www.zabbix.com/documentation/current/start

ANEXOS

ENCUESTA PARA ANALISTAS DEL SOC

Encuesta a analistas, para determinar la insatisfacción actual frente a cómo se maneja los incidentes.

1. En promedio, ¿cuánto tiempo te demoras en detectar un incidente?
    a. 05 min a 19 min
    b. 20 min a 39 min
    c. 40 min a 59 min
    d. 60 min a más
2. ¿Qué tan importante considera usted que es la prevención o anticipación de incidentes?
    a. Bajo
    b. Medio
    c. Alto
3. ¿Considera que es importante el mantenimiento planificado del hardware?
    a. Bajo
    b. Medio
    c. Alto
4. ¿Considera usted que la detección temprana de un incidente influye en el tiempo de solución?
    a. Si
    b. No
5. ¿Cómo califica el seguimiento realizado a su incidencia?
    a. Bajo
    b. Medio
    c. Alto

ENCUESTA PARA OPERADORES DEL SOC

Encuesta a usuarios operadores, para la validación del sistema de monitoreo, diagrama de flujo y matriz de escalamiento.

1. En promedio, ¿Cuánto tiempo te demoras en detectar un incidente usando Zabbix?
   a. 05 min a 19 min
   b. 20 min a 39 min
   c. 40 min a 59 min
   d. 60 min a más
2. ¿Qué tan amigable considera usted que es la interfaz de software Zabbix?
   a. Bajo
   b. Medio
   c. Alto
3. ¿Qué dificultad considera usted tiene el agregar nuevos equipos para el monitoreo?
   a. Fácil
   b. Regular
   c. Difícil
4. ¿Se solucionaron incidentes antes de ocurrir alguna falla?
   a. Si
   b. No
5. ¿El servicio de monitoreo cumple con las funciones esperadas?
   a. Si
   b. No
6. ¿Considera usted que el diagrama de flujo y la matriz de escalamiento ayudan a que la gestión de incidencia sea óptima?
   a. Si
   b. No