UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

IMPLEMENTACIÓN DE UNA ARQUITECTURA DE MONITOREO Y REGISTRO DE SEGURIDAD EN SERVIDORES DE LA UNIVERSIDAD PENÍNSULA DE SANTA ELENA BAJO LA NORMATIVA ISO 27000

AUTOR

Vera Tomala, Joel Javier

TRABAJO DE TITULACIÓN
Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Ing. Espinal Santana Albert Giovanny, PhD.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
ALBERT GIOVANNY ESPINAL SANTANA

Ing. Albert Giovanny Espinal, PhD
TUTOR

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Luis Zambrano, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
ANA EVA CHACON LUNA

Ing. Ana Eva Chacón, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIO GENERAL

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por VERA TOMALA JOEL JAVIER, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
ALBERT GIOVANNY ESPINAL SANTANA

Ing. Albert Giovanny Espinal Santana, PhD

Santa Elena, 15 de octubre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO
DECLARACIÓN DE RESPONSABILIDAD

Yo, **VERA TOMALA JOEL JAVIER**

DECLARO QUE:

El trabajo de Titulación, **Implementación de una arquitectura de monitoreo y registro de seguridad en servidores de la universidad península de Santa Elena bajo la normativa Iso 27000,** previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 15 de octubre de 2024

EL AUTOR

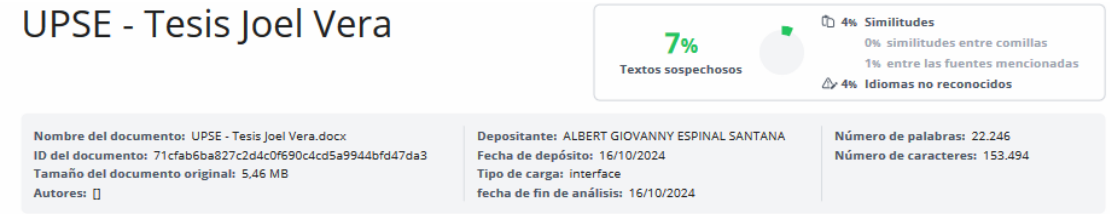
Firmado electrónicamente por:
JOEL JAVIER VERA TOMALA

JOEL JAVIER VERA TOMALA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Implementación de una arquitectura de monitoreo y registro de seguridad en servidores de la universidad península de Santa Elena bajo la normativa Iso 27000** , presentado por el estudiante, VERA TOMALA JOEL JAVIER fue enviado al Sistema Anti-plagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 7%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



TUTOR

Firmado electrónicamente por:
ALBERT GIOVANNY ESPINAL SANTANA

Ing. Albert Giovanny Espinal Santana, PhD.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **VERA TOMALA JOEL JAVIER**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo de propuestas metodológicas y tecnológicas avanzadas con fines de difusión pública, además apruebo la reproducción de este trabajo de propuestas metodológicas y tecnológicas avanzadas dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 15 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
JOEL JAVIER VERA TOMALA

VERA TOMALA JOEL JAVIER

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas las personas que me apoyaron a lo largo de este camino. A mis directores de tesis, quienes con su guía y conocimientos hicieron posible la realización de este trabajo, brindándome siempre el apoyo necesario para superar los obstáculos y aprender de cada etapa del proceso.

A mi familia, por su incondicional amor y apoyo, por ser mi pilar en los momentos difíciles y por siempre alentarme a seguir adelante. Sin su confianza y paciencia, este logro no habría sido posible.

A mis amigos y compañeros, quienes me acompañaron y motivaron durante este viaje académico. Su comprensión y compañía fueron invaluables en este trayecto.

Finalmente, agradezco a la Universidad Península de Santa Elena y a sus profesores por brindarme las herramientas académicas y el espacio para desarrollar este proyecto. Este trabajo es reflejo del compromiso y dedicación que nos inculcan como futuros profesionales.

VERA TOMALA JOEL JAVIER

DEDICATORIA

Dedico esta tesis a mi familia, quienes siempre han creído en mí, impulsándome a alcanzar mis sueños con amor y sabiduría. A mis padres, por ser ejemplo de esfuerzo y perseverancia, y a mis hermanos, por su apoyo incondicional.

A mis amigos, por estar presentes en los momentos de alegría y de dificultad, y por recordarme siempre la importancia del compañerismo y la amistad.

Y, especialmente, dedico este trabajo a todas las personas que, con su confianza en mi capacidad, me dieron la fuerza para seguir adelante y superar cada desafío que se presentó en el camino.

VERA TOMALA JOEL JAVIER

ÍNDICE GENERAL

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXO

RESUMEN

Este trabajo se centra en la implementación de estrategias de seguridad para los servidores de la Universidad Península de Santa Elena, utilizando la normativa ISO 27001 y metodologías de seguridad. Su objetivo es crear un sistema integral que proteja la integridad, confidencialidad y disponibilidad de la información institucional. La investigación combina métodos cuantitativos y cualitativos, empleando técnicas como la revisión documental, encuestas y análisis de datos, con una población de 21 miembros del departamento de TICs. Los resultados muestran avances significativos en la vigilancia y detección de incidentes de seguridad. Herramientas como Prometheus, Elasticsearch, Kibana y Grafana permitieron obtener métricas en tiempo real y registros históricos, facilitando la identificación de patrones de uso y vulnerabilidades. Un ejemplo es el servidor tomcat-auth1.local, que registró más de 2.5 millones de eventos en un solo día, optimizando los recursos y reduciendo riesgos de seguridad. Además, la implementación de alertas automáticas mejoró la respuesta ante incidentes, fortaleciendo la protección de la información.

Palabras claves: Seguridad de servidores, ISO 27001, Ciberseguridad.

ABSTRACT

This work focuses on the implementation of security strategies for the servers of the Santa Elena Peninsula University, using the ISO 27001 standard and security methodologies. Its objective is to create a comprehensive system that protects the integrity, confidentiality, and availability of institutional information. The research combines quantitative and qualitative methods, using techniques such as documentary review, surveys, and data analysis, with a population of 21 members of the ICT department. The results show significant advances in the surveillance and detection of security incidents. Tools such as Prometheus, Elasticsearch, Kibana and Grafana made it possible to obtain real-time metrics and historical records, facilitating the identification of usage patterns and vulnerabilities. An example is the tomcat-auth1.local server, which logged more than 2.5 million events in a single day, optimizing resources and reducing security risks. Additionally, the implementation of automatic alerts improved incident response, strengthening information protection.

.

Keywords: Server Security, ISO 27001, Cybersecurity.

INTRODUCCIÓN

La creciente exposición de información y sistemas a riesgos, derivada del aumento en el intercambio de datos y el uso extendido de redes abiertas, subraya la necesidad urgente de salvaguardar la seguridad de la información para proteger a las organizaciones de posibles daños (Santacruz Fernández, 2013). Esta situación ha generado la demanda de implementar medidas adecuadas de seguridad de la información, siendo la gestión sistematizada de la seguridad una iniciativa clave en la gestión de TI.

En este contexto, la norma ISO 27001 se ha consolidado como un referente crucial, proporcionando las mejores prácticas para administrar la seguridad de la información. Esta norma es esencial para desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) que asegure la continuidad y el mantenimiento de los procedimientos de seguridad en línea con los objetivos estratégicos de la organización.(ISO 27001 ,2005)

La Universidad Estatal Península de Santa Elena (UPSE), a través de su departamento de Tecnología de la Información (TIC), es responsable de proporcionar soporte administrativo y tecnológico a su comunidad. Sin embargo, a pesar del tiempo transcurrido desde la creación del departamento, las medidas de seguridad física, ambiental y de control de acceso en su centro de datos no cumplen con las mejores prácticas de un SGSI. Aunque en 2018 se aprobaron políticas de seguridad informática basadas en la norma ISO 27002, estas son generalizadas y no se han actualizado adecuadamente (UPSE ,2014).

El centro de datos del departamento de TIC carece de un control adecuado de acceso, lo que representa un riesgo significativo para la información almacenada en los servidores. Es imperativo garantizar que tanto los equipos físicos como el personal cumplan con normas de distanciamiento, ambientación y seguridad.

Por consiguiente, este proyecto se centra en la implementación de estrategias para el análisis de seguridad de servidores en la UPSE, abarcando desde la recolección de información hasta la remediación basada en normativas ISO 27001 y metodologías de seguridad reconocidas. El objetivo general es implementar un sistema integral de seguridad para los servidores de la UPSE, con el fin de proteger la integridad, confidencialidad y disponibilidad de la información institucional. Este objetivo se logrará a través de la evaluación del estado actual de seguridad, el diseño de estrategias basadas

en ISO 27001, la implementación de controles específicos, la capacitación del personal y el monitoreo continuo de las estrategias de seguridad.

Planteamiento de la investigación (Fundamentación de la investigación)

La UPSE maneja diversos sistemas que gestionan información vital para su comunidad universitaria. El departamento de Tecnologías de la Información y Comunicación (TIC) es responsable de asegurar que el procesamiento de esta información se ajuste a los principios fundamentales de integridad, confiabilidad y disponibilidad. La ausencia de un plan de seguridad específico para proteger estos activos expone a la universidad a vulnerabilidades significativas, ya que el personal del departamento carece de directrices claras para salvaguardar el Sistema de Gestión de Seguridad de la Información (SGSI).

Las áreas del departamento de TIC carecen de un adecuado nivel de control de acceso a los sistemas y áreas que manejan información crítica o sensible, lo que aumenta las amenazas tanto para la información como para la seguridad física. Es crucial que el centro de datos garantice un funcionamiento adecuado en términos de distanciamiento entre equipos informáticos, condiciones lumínicas, riesgos ambientales, software, entre otros aspectos.

La implementación de un plan de acción basado en las mejores prácticas de SGSI en la seguridad de servidores permitirá corregir deficiencias en el departamento y proteger los activos de información almacenados en los servidores de la universidad. Este proyecto no solo identificará las fallas actuales, sino que también seguirá las pautas establecidas en la norma ISO 27001, abarcando desde la recolección de información y análisis de riesgos y vulnerabilidades hasta la implementación de medidas correctivas y el monitoreo continuo, mejorando así la seguridad de los servidores de la UPSE.

Formulación del problema de investigación

¿Cómo se puede implementar un sistema integral de monitoreo y registro de seguridad en los servidores de la Universidad Península de Santa Elena, utilizando herramientas de código abierto y cumpliendo con los lineamientos de la normativa ISO 27001, que permita detectar actividades no autorizadas o eventos que puedan afectar la disponibilidad de los recursos?

Objetivo General:

Desarrollar un sistema de monitoreo de los registros de seguridad de los servidores de la Universidad Estatal Península de Santa Elena (UPSE) utilizando herramientas de código abierto, que permita detectar actividades no autorizadas o eventos que puedan afectar la disponibilidad de los recursos, conforme a la sección 12.4 de la norma ISO 27000.

Objetivos Específicos:

1. Evaluar el estado actual de la seguridad de los servidores de la UPSE, mediante la revisión exhaustiva de la infraestructura de TI y las políticas de seguridad existentes para el análisis de vulnerabilidades y brechas en la seguridad de los servidores.
2. Analizar los registros de seguridad de los servidores, conforme a la sección 12.4 de la normativa ISO 27000, que permita la identificación y, configuración de reglas de los eventos y su almacenamiento, de acuerdo con posibles incidentes de seguridad informática.
3. Implementar un sistema de monitoreo y registro de seguridad para la supervisión continua de los servidores en la UPSE, mediante un dashboard, que permita la visualización de todas las métricas relevantes para la detección de actividades o eventos sospechosos.

Planteamiento hipotético

La implementación de un sistema de monitoreo y registro basado en la sección 12.4 de la norma ISO 27000, permite mejorar la seguridad de los servidores de la Universidad Estatal Península de Santa Elena (UPSE), que permita detectar actividades no autorizadas o eventos que puedan afectar la disponibilidad de los recursos.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1 Revisión de Literatura

1.1.1 Introducción a la Revisión de Literatura

La revisión de literatura es un componente fundamental en cualquier investigación académica, ya que proporciona el marco teórico y contextual necesario para comprender el estado actual del conocimiento sobre un tema específico. Su importancia radica en varios aspectos clave que son esenciales para el éxito del presente proyecto.

En primer lugar, la revisión de literatura permite identificar y analizar estudios previos relevantes, lo que ayuda a construir una base sólida sobre la cual desarrollar nuevas ideas y enfoques. Al revisar trabajos anteriores, se puede comprender qué preguntas han sido abordadas, qué metodologías se han utilizado y cuáles son los resultados y conclusiones más destacados en el campo de estudio.

Además, la revisión de literatura facilita la identificación de lagunas en el conocimiento existente. Estas lagunas representan oportunidades para contribuir de manera significativa a la disciplina, abordando áreas que no han sido totalmente exploradas o proponiendo nuevas perspectivas sobre temas ya estudiados. De esta manera, la investigación no solo se apoya en lo que ya se conoce, sino que también busca expandir las fronteras del conocimiento.

Otro aspecto crucial es que la revisión de literatura ayuda a situar la investigación en un contexto más amplio. Al comprender cómo se ha desarrollado un campo de estudio a lo largo del tiempo y cuáles han sido las principales tendencias, teorías y debates, se puede situar el trabajo dentro de una narrativa más amplia, lo que enriquece la relevancia y el impacto potencial de sus hallazgos.

Finalmente, la revisión de literatura es esencial para garantizar la validez y rigor del proyecto. Al analizar críticamente los estudios anteriores, se puede identificar las fortalezas y debilidades de diferentes enfoques metodológicos, lo que le permite diseñar su propio estudio de manera más robusta y evitar errores comunes o sesgos que podrían comprometer los resultados.

Contexto de la seguridad de servidores y normativa ISO 27000.

La seguridad de servidores y la normativa ISO 27000 tiene como objetivo principal proporcionar una base sólida para la comprensión de los estándares y prácticas que aseguran la protección efectiva de la información en entornos tecnológicos. En primer

lugar, es fundamental identificar las mejores prácticas en la seguridad de servidores, ya que permiten implementar controles que mitiguen riesgos y vulnerabilidades. La información se ha convertido no sólo en un activo valioso, sino también estratégico en las organizaciones. La información puede ser protegida de muchas maneras. (Ramos Mamami et al., 2023)

Asimismo, se busca evaluar cómo la normativa ISO 27000 ha sido implementada en diferentes organizaciones, particularmente en el ámbito de la seguridad de servidores. La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. (Isabel Ladino et al., 2011)

En una organización con acceso a Internet es fundamental realizar una adecuada gestión de las trazas, principalmente las de navegación de los usuarios. Para lograr este objetivo deben contar con mecanismos de detección de violaciones de seguridad, que a su vez generen alarmas y reportes a los especialistas de seguridad. (Castillo, 2021) destaca que el seguimiento a eventos de seguridad de los sistemas de una empresa debe ser la manera en que se gestionan los incidentes de seguridad, permitiendo una respuesta más rápida y efectiva ante posibles ataques. Este enfoque emergente complementa las estrategias tradicionales de seguridad y refuerza la necesidad de estar al día con las innovaciones tecnológicas en el campo.

1.1.2 Normativas de Seguridad de la Información

Norma ISO 27000 y su Relevancia.

La familia de estándares ISO 27000, una serie de normas internacionales que proporcionan un marco para la gestión de la seguridad de la información dentro de las organizaciones. Esta norma en particular se centra en los requisitos básicos y el vocabulario de la gestión de la seguridad de la información, sirviendo como base para la implementación y comprensión de otros estándares de la serie, como la ISO 27001 e ISO 27002.

Hoy en día las amenazas tecnológicas son parte de nuestra cotidianeidad y más aún de la vida organizacional, las cuales van desde diversas formas de virus, pasando por los recientes ataques de ransomware hasta amenazas sofisticadas como los ataques día cero (en inglés, zero-day attack) lo cual requiere la implementación de controles que

puedan ser gestionados a través de un adecuado enfoque de seguridad de la información. (Valencia-Duque & Orozco-Alzate, 2017)

Las normas establecen el deber ser, y no la forma como se logra, de allí la importancia de establecer metodologías y procesos que permitan orientar a las organizaciones en la forma como se debe abordar este tipo de procesos, con el respaldo de las normas internacionales promulgadas para tal fin. (Valencia-Duque & Orozco-Alzate, 2017)

La importancia de la ISO 27000 radica en su papel como pilar fundamental para la creación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Al establecer un vocabulario común y requisitos claros, facilita la comunicación efectiva entre los profesionales de la seguridad de la información, auditores y partes interesadas. Esto es esencial para garantizar que todos los aspectos de la seguridad de la información sean comprendidos y abordados de manera coherente en toda la organización.

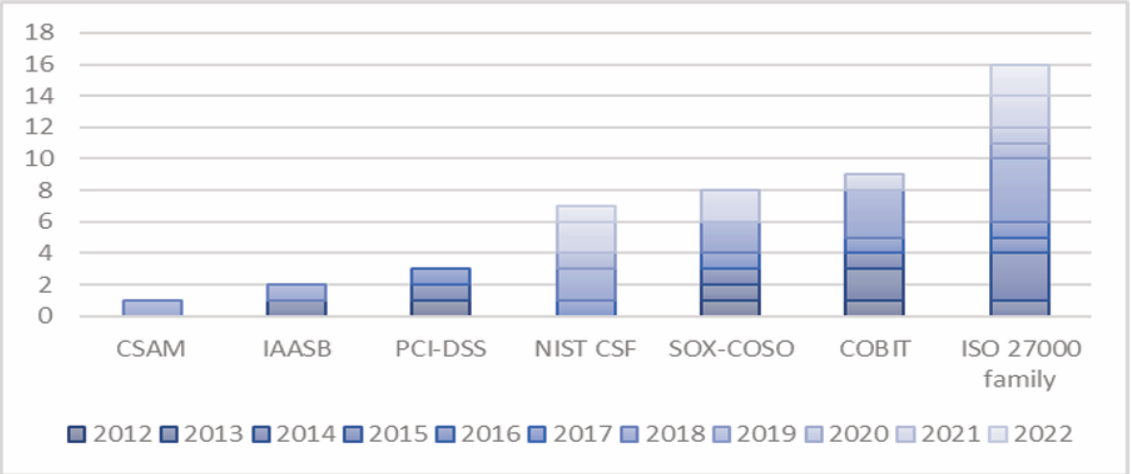
Comparativa con otras Normativas de Seguridad.

La ISO 27001, como marco de referencia global para la gestión de la seguridad de la información, ha cobrado una relevancia innegable en el panorama empresarial actual. Sin embargo, no es la única norma que aborda esta temática. Otras iniciativas como el NIST Cybersecurity Framework (NCF) y COBIT ofrecen enfoques complementarios y específicos para garantizar la protección de los activos de información.

(Sanchez-Garcia et al., s. f.) identifica siete guías utilizadas con mayor amplitud para las auditorías de riesgos de ciberseguridad: 1) la familia ISO 27000, 2) COBIT, 3) SOX COSO, 4) NIST CSF, 5) PCI-DSS, 6) IAASB y 7) CSAM. De las guías previamente identificadas, solo el NIST CSF y el CSAM fueron creadas explícitamente para el ámbito de la ciberseguridad como se aprecia en la Figura 1.

Figura **1**

Frecuencia de las guías de Auditoría de Ciberseguridad identificadas por año



Nota: Frecuencias de guías de Auditoria de Ciberseguridad desde el año 2012 hasta el 2022 (Sanchez-Garcia et al., 2024)

Tabla 1

Comparativa entre la norma ISO 27001, el NIST Cybersecurity Framework (NCF) y COBIT.

	ISO 27001	**NIST Cybersecurity Framework (NCF)**	**COBIT**
Enfoque principal	Seguridad de la información	Ciberseguridad en general	Gobernanza y gestión de TI
Alcance	Amplio conjunto de controles de seguridad para proteger la información	Marco más amplio que abarca diversos aspectos de la ciberseguridad	Marco general para la gestión de TI, incluyendo la seguridad
Estructura	Sistema de Gestión de la Seguridad de la Información (SGSI)	Funciones clave para mejorar la postura de ciberseguridad	Modelo de madurez para evaluar la capacidad de una organización
Ciclo de vida	Ciclo de mejora continua basado en Planificar-Hacer-Verificar-Actuar (PDCA)	Ciclo de mejora continua basado en identificar, proteger, detectar, responder y recuperar	Ciclo de mejora continua basado en un modelo de madurez
Flexibilidad	Permite una implementación personalizada	Ofrece flexibilidad para adaptarse a diferentes organizaciones	Permite una adaptación a las necesidades específicas de cada organización
Áreas de complementariedad	Puede utilizarse para implementar los controles específicos del NIST CSF	Puede proporcionar un marco general para la gobernanza y gestión de TI	Puede complementarse con la ISO 27001 para una gestión integral de la seguridad de la información

Nota: Detalles de características comparativas entre las normas.

En la tabla anterior se realizar la respectiva comparación, dentro de las normas comparadas la ISO 27001 profundiza en los controles de seguridad de la información, proporcionando un marco detallado para su gestión. NIST CSF ofrece un enfoque más amplio, abarcando la ciberseguridad en general y proporcionando un marco flexible para mejorar la postura de ciberseguridad de una organización y COBIT se centra en la gobernanza y gestión de TI, incluyendo la seguridad de la información como un aspecto clave.

Aplicaciones de la ISO 27000 en Entornos Educativos

Según estudio llevado a cabo por el gobierno de Reino Unido sobre ciberataques en el sector educativo se identificó que el 85% de las Universidades del país en mención han sido víctimas de ataques en el año 2023.

- El número de ataques a escuelas primarias fue de un 41%
- El 63% escuelas secundarias.
- Las escuelas de educación superior 82%.
- 85% de instituciones de educación superior están en la estadística de haber identificado infracciones o ataques durante el año 2023.

El estudio se realizó a 241 escuelas primarias; 217 escuelas secundarias; 44 colegios de educación superior; 52 instituciones de educación superior; 2.263 empresas del Reino Unido. (GOV.UK, 2023)

Datos recopilados a través de los informes de EcuCERT, ESET, y Check Point proporcionan un panorama claro sobre la situación de ciberseguridad en las universidades ecuatorianas. Estos resultados revelan una vulnerabilidad significativa frente a diversas amenazas cibernéticas, incluyendo phishing, ransomware, malware, y otras formas de ataques cibernéticos, lo que pone de relieve la necesidad urgente de mejorar la infraestructura y las medidas de seguridad en las instituciones educativas. (Derenzin-Martinez, 2024)

Todas las universidades ecuatorianas están enfrascadas en perfeccionar su sistema de gestión basado en una cultura de pensamiento estratégico. Las exigencias del ente evaluador externo a las universidades, el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES) también se enfoca

en el aseguramiento de un servicio educativo de calidad en todas las funciones sustantivas de la educación superior. (Becerra et al., 2019)

La norma ISO 27001, tradicionalmente asociada a grandes corporaciones, ha encontrado un nicho de aplicación cada vez más relevante en el sector educativo. Las instituciones educativas, desde escuelas hasta universidades, manejan una gran cantidad de información sensible, como datos personales de estudiantes, registros académicos, resultados de evaluaciones y propiedad intelectual. La protección de estos datos es fundamental para garantizar la privacidad, la integridad y la confidencialidad de la información, y es aquí donde la ISO 27001 juega un papel crucial.

Los sistemas de gestión de la seguridad de la información es uno de los puntos focales para el desarrollo de las instituciones educación superior; especialmente en el ámbito de la transferencia tecnológica y la investigación, donde la tecnología y la solidez de los sistemas informáticos frente a posibles amenazas es crucial para la integridad de la información depositada en dichos sistemas. (Guerra et al., 2021)

Entre las principales aplicaciones en las instituciones educativas primordialmente en las de Educación Superior la relevancia que toman estas medidas tiene que ver con:

Protección de datos personales: La normativa de protección de datos, como el RGPD en Europa, exige que las organizaciones manejen los datos personales de manera segura y responsable. La ISO 27001 proporciona un marco sólido para cumplir con estos requisitos legales.

Ciberseguridad: Las instituciones educativas son objetivos frecuentes de ciberataques, ya que almacenan una gran cantidad de información valiosa. La ISO 27001 ayuda a prevenir y mitigar los riesgos cibernéticos, protegiendo los sistemas y la infraestructura tecnológica.

Confianza y reputación: Al demostrar un compromiso con la seguridad de la información, las instituciones educativas ganan la confianza de estudiantes, padres, personal y socios.

Continuidad del negocio: En caso de un incidente de seguridad, un sistema de gestión de seguridad de la información (SGSI) basado en la ISO 27001 puede ayudar a minimizar el impacto y garantizar la continuidad de las operaciones.

Al implementar medidas alineadas con la ISO 27001, las instituciones educativas no solo cumplen con las normativas, sino que también fortalecen su seguridad informática, protegen la privacidad de sus estudiantes, personal, y optimizan sus procesos internos, contribuyendo a su posicionamiento como instituciones de excelencia.

1.1.3 Metodologías de Seguridad Informática

Open Web Application Security Project (OWASP), más que una organización; es una comunidad global de expertos en seguridad que trabaja para mejorar la postura de seguridad de las aplicaciones web en todo el mundo. A través de una amplia gama de recursos gratuitos y colaboraciones, OWASP se ha convertido en el referente indiscutible en el campo de la seguridad de aplicaciones web.

Está enfocada para realizar pruebas de penetración permiten descubrir las vulnerabilidades presentes en un sistema; y, entender los riesgos que representaría la explotación de alguna de ellas. (Coronel Suárez & Quirumbay Yagual, 2022)

La Guía de Pruebas de OWASP se evidenció como la más completa, siendo la metodología de ISSAF la que la siguió. Sin embargo, ninguna metodología evidenció su capacidad para proporcionar técnicas, herramientas o pruebas de seguridad que permitan identificar todas las vulnerabilidades comparadas de manera autónoma. (González & Montesino, 2018)

NIST Cybersecurity Framework

El Marco de Ciberseguridad del NIST se ha convertido en un referente global para las organizaciones que buscan fortalecer la postura de seguridad. Proporciona un lenguaje común y un enfoque estructurado para gestionar los riesgos cibernéticos, el NIST CSF permite a empresas de todos los tamaños y sectores evaluar sus capacidades actuales, identificar brechas y desarrollar un plan de acción personalizado. Este marco flexible y adaptable se ha posicionado como una herramienta invaluable para mejorar la resiliencia ante ciberataques, cumplir con los requisitos regulatorios y generar confianza en los clientes y socios comerciales. Su enfoque basado en funciones clave permite a las organizaciones priorizar sus esfuerzos y asignar recursos de manera eficiente, lo que se traduce en una mayor protección de sus activos más valiosos: la información y los sistemas.

El NIST (National Institute of Standards and Technology), lo describe como una "evaluación de seguridad donde los evaluadores simulan ataques de la vida real con el objetivo de descubrir métodos para eludir las características de seguridad de una aplicación, sistema o red de datos. Las evaluaciones de penetración exigen la realización de ataques reales en sistemas y datos reales, utilizando las mismas técnicas y herramientas empleadas por los atacantes presentes. (González & Montesino, 2018)

Metodologías de Análisis de Registro y Monitoreo de Seguridad

En el complejo panorama de las amenazas cibernéticas actuales, los datos de registros se han convertido en una herramienta indispensable para detectar y responder a incidentes de seguridad. El análisis de registros, combinado con un sólido sistema de monitoreo, permite a las organizaciones obtener una visibilidad profunda de sus sistemas, identificar anomalías y tomar medidas proactivas para proteger sus activos más valiosos.

El análisis de registros consiste en el examen sistemático de los registros generados por los sistemas informáticos, aplicaciones y dispositivos de red. Estos registros contienen información valiosa sobre eventos, errores, actividades de usuarios y otras acciones relevantes. Al analizar estos datos, es posible identificar patrones, detectar amenazas potenciales y reconstruir la secuencia de eventos que condujeron a un incidente de seguridad.

El estudio realizado por (Leguizamón-Páez et al., 2020) logró identificar diferentes patrones y formas de atacar, guiando la configuración de un script en el servidor IDS (Intrusion Detection System), permitiendo con los registros almacenados crear reglas e implementarlo en Iptables, ya que las IPs se identificaron como los datos de mayor connotación asociados a los diferentes ataques.

Metodologías de análisis de registros

Existen diversas metodologías para analizar registros, cada una con sus propias fortalezas y debilidades:

Análisis manual: Si bien es una tarea laboriosa, el análisis manual permite a los analistas de seguridad identificar patrones y correlacionar eventos que pueden pasar desapercibidos a los sistemas automatizados.

Análisis basado en reglas: Mediante la definición de reglas y alertas, los sistemas pueden identificar automáticamente eventos sospechosos, como intentos de acceso no autorizados o cambios en la configuración.

Análisis de comportamiento: Esta metodología se enfoca en identificar desviaciones de los patrones de comportamiento normales, lo que puede indicar la presencia de una amenaza.

Inteligencia artificial y machine learning: El uso de algoritmos de aprendizaje automático permite analizar grandes volúmenes de datos de registros y detectar anomalías de manera más precisa y eficiente.

1.1.4 Herramientas de Monitoreo y Análisis de registros

En el entorno de la ciberseguridad moderna, la gestión y análisis de registros se han convertido en componentes fundamentales para garantizar la integridad, disponibilidad y confidencialidad de la información en sistemas informáticos. Los registros, o registros de eventos, son archivos generados por sistemas operativos, aplicaciones y dispositivos de red, que documentan cada interacción y transacción que ocurre dentro de un entorno digital. Estos registros son esenciales para la detección de actividades inusuales, la identificación de brechas de seguridad, y la respuesta ante incidentes.

Las trazas generadas por los sistemas de hardware y software tienen una importancia fundamental en el proceso de gestión de la seguridad de la información. Dentro de los principales documentos está la guía de buenas prácticas de la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) ISO/IEC 27002 como parte de la norma certificable ISO/IEC 27001(Porven Rubier et al., 2015)

Con el aumento en la complejidad y volumen de los datos generados por las infraestructuras tecnológicas, las herramientas de monitoreo y análisis de registros han evolucionado significativamente. Estas herramientas no solo facilitan la recopilación y almacenamiento de datos, sino que también proporcionan capacidades avanzadas de búsqueda, visualización y correlación de eventos en tiempo real. Además, permiten automatizar alertas ante posibles amenazas y anomalías en el sistema, reduciendo el tiempo de respuesta ante incidentes de seguridad.

En un contexto donde las normativas y estándares de seguridad, como la ISO 27001, exigen un riguroso control y monitoreo continuo, las herramientas de análisis de registros son vitales para el cumplimiento regulatorio y la protección proactiva contra amenazas cibernéticas. A través del uso de soluciones como ELK Stack, Splunk, Graylog, Grafana y Prometheus las organizaciones pueden obtener una visión integral de sus operaciones y responder de manera efectiva a incidentes, minimizando el impacto de posibles ataques.

ELK Stack (Elasticsearch, Logstash, Kibana)

Se conoce como un motor de búsqueda y analítica de tipo código abierto, basado en Apache Lucene, considerado como RESTful (Basado en arquitectura REST, que es una interfaz para conectar varios sistemas basados en HTTP, y sirve para obtener y generar datos y operaciones) y con documentos JSON, diseñado para permitir una escalabilidad horizontal, fiabilidad y de fácil gestión. (Balseca-Chávez et al., 2021)

El ELK Stack se ha convertido en la columna vertebral de las operaciones de muchas organizaciones, proporcionando una plataforma de análisis de datos potente y flexible. Al combinar la capacidad de ingestión de datos de Logstash, el almacenamiento y búsqueda distribuida de Elasticsearch y las potentes capacidades de visualización de Kibana, el ELK Stack permite a las empresas recopilar, analizar y visualizar grandes volúmenes de datos de manera eficiente y efectiva. Esto a su vez facilita la detección temprana de amenazas, la optimización de procesos y la toma de decisiones basadas en datos, lo que contribuye a mejorar la seguridad, la eficiencia y la competitividad de las organizaciones.

Splunk y su Aplicación en la Gestión de Seguridad

Es una plataforma que ofrece una solución integral para la recopilación, indexación y análisis de grandes volúmenes de datos de seguridad. Su capacidad para recopilar datos de diversas fuentes, como firewalls, sistemas operativos, aplicaciones y dispositivos IoT, permite obtener una visibilidad completa de su entorno y detectar amenazas ocultas. Además, Splunk facilita la correlación de eventos de seguridad, permitiendo identificar patrones de ataque y responder de manera efectiva a incidentes. Posee grandes capacidades de búsqueda y visualización, permite tomar decisiones

basadas en datos y mejorar significativamente la capacidad de respuesta ante incidentes cibernéticos.

Splunk es una solución de almacenamiento y visualización de datos que utiliza índices y no base de datos para almacenar y acceder a todos los datos que se almacenen en la plataforma. (García Hidalgo & Moneo, 2023)

Plataforma de Big Data que simplifica la tarea de recopilar y administrar volúmenes masivos de datos generados por máquinas y buscar información dentro de ellos, siendo muy utilizado para análisis empresarial y web, gestión de aplicaciones, cumplimiento y seguridad (González de Juana, 2021)

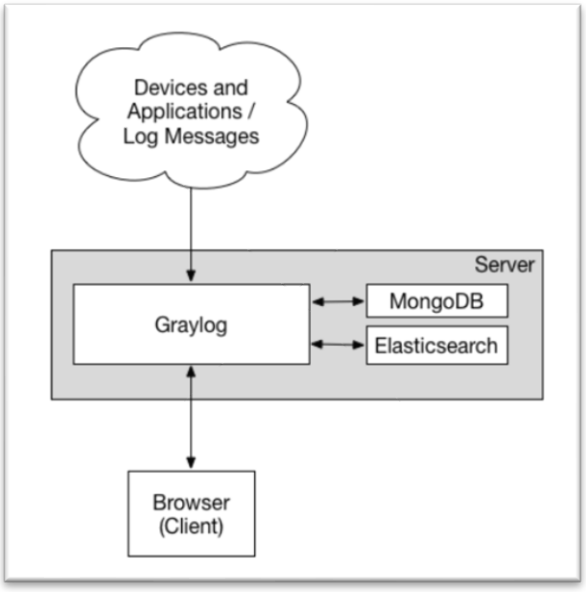
Graylog: Alternativas en la Gestión de registros

En el contexto de la ciberseguridad y la administración de infraestructuras tecnológicas, la correcta gestión de registros es un factor crítico para el análisis de incidentes y el monitoreo del comportamiento del sistema. Graylog es una herramienta ampliamente utilizada para la recolección, análisis y visualización de registros en tiempo real, destacándose por su capacidad de procesar grandes volúmenes de datos de manera eficiente y flexible. En este trabajo, se analizará Graylog como una opción para la gestión de registros, en comparación con otras herramientas como ELK Stack (ElasticSearch, Logstash, Kibana), Splunk entre otras, que ofrecen alternativas con diferentes niveles de escalabilidad, búsqueda avanzada y opciones de visualización.

Es una herramienta de análisis de eventos Open Source, con una versión Enterprise de pago que añade funcionalidades. Esta herramienta nos permitirá centralizar el análisis de eventos al ser posible recibir eventos de múltiples sistemas (Ruiz & Rodrigo, 2019).

Figura 2

Arquitectura básica de Graylog



Nota: Adaptado de *(Ruiz & Rodrigo, 2019)*

Grafana en el monitoreo de servidores.

En este trabajo también se ha empleado la herramienta Grafana, un software de libre disposición. Mediante esta herramienta se puede tanto consultar, visualizar y realizar un tratamiento de los datos recibidos de una fuente en los paneles de visualización. La gran utilidad de Grafana es que el tratamiento de los datos se puede realizar desde un único panel, juntando todas las gráficas, aunque provengan de varios destinos (Planes Martínez, 2022)

Sobre la base de investigaciones similares a las que se han explicado anteriormente, las soluciones ofrecidas para apoyar el proceso de monitoreo de recursos del servidor en este estudio utilizan aplicaciones Zabbix y Grafana porque es capaz de proporcionar información sobre el estado del componente del servidor en uso mediante el envío de Notificaciones por correo electrónico o telegrama a los administradores del servidor de forma fácil y atractiva (Yulvianda & Ismail, 2023)

En el ámbito del monitoreo y visualización de datos, Grafana ha surgido como una de las principales plataformas de código abierto, permitiendo a los administradores de sistemas y analistas de seguridad la creación de dashboards interactivos y altamente personalizables. Este trabajo se centrará en la implementación de Grafana como una

herramienta clave para la monitorización continua de la infraestructura de servidores en una IES, con el objetivo de optimizar la gestión y análisis de datos críticos, especialmente aquellos relacionados con la seguridad informática.

A través de la integración de Grafana con otras herramientas de monitoreo como Prometheus y la recolección centralizada de registros, el estudio explorará cómo se pueden visualizar métricas en tiempo real para detectar comportamientos anómalos, vulnerabilidades potenciales o indicios de ataques cibernéticos. El trabajo analizará la eficiencia de Grafana en la visualización de registros, su capacidad para generar alertas automatizadas ante eventos sospechosos, y su compatibilidad con normativas como la ISO 27001, que exige un control riguroso de los sistemas de información.

Prometheus en la Monitorización de registros para la Seguridad Informática.

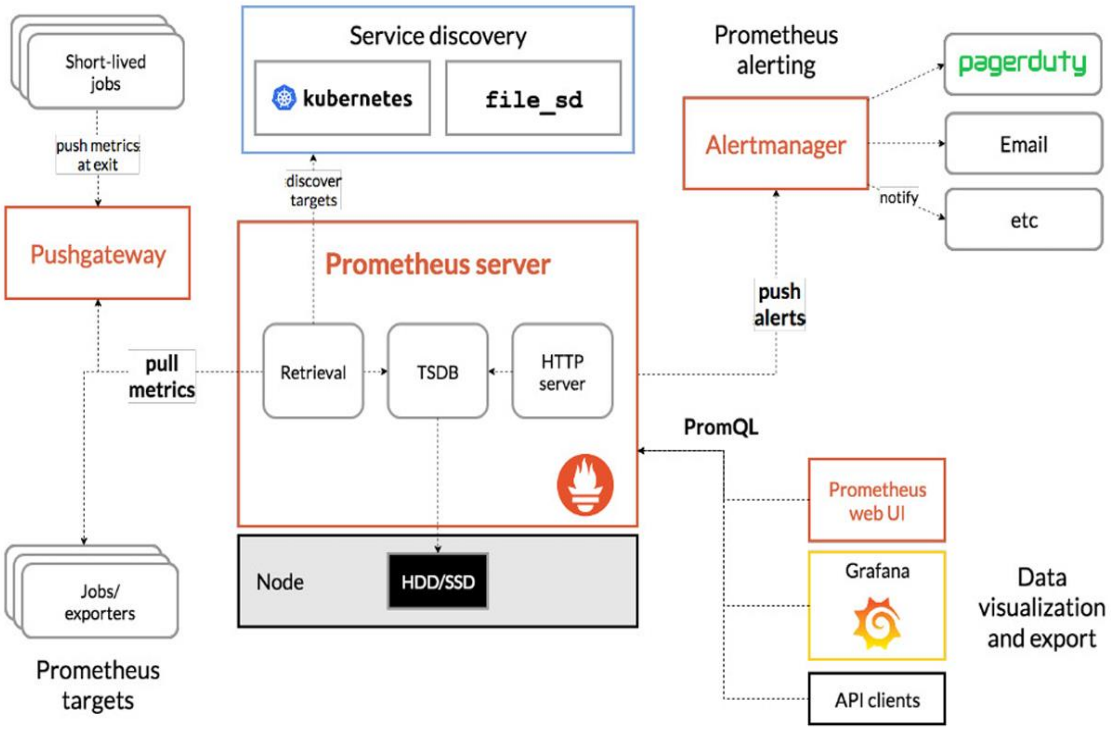
La correcta monitorización de servidores es un aspecto esencial en la gestión de infraestructuras tecnológicas, especialmente en el contexto de seguridad informática. En este trabajo se abordará el uso de Prometheus como herramienta principal para la monitorización de registros de servidores en una IES, con el objetivo de identificar comportamientos anómalos y posibles indicios de ataques cibernéticos.

Prometheus, se puede encontrar que esta ofrece la posibilidad de realizar consultas sobre el estado de diferentes métricas tales como: temperatura de GPU, potencia utilizada por cada una de las GPU, utilización de la capacidad de GPU expresada en porcentaje entre otras. (Pons Moro, 2021)

Prometheus, diseñado para la recopilación y almacenamiento de métricas, permite capturar datos detallados sobre el rendimiento y comportamiento de los servidores. A través de un sistema de series temporales, Prometheus es capaz de monitorear en tiempo real los registros generados por servidores tanto Linux como Windows, proporcionando alertas automáticas ante comportamientos sospechosos o degradaciones en el sistema. Este proyecto se centrará en la integración de Prometheus con otras herramientas de monitoreo como Grafana, la cual permitirá visualizar los datos recolectados de manera gráfica y comprensible, facilitando la toma de decisiones ante incidentes de seguridad.

Figura 3

Arquitectura de prometheus



Nota: Adaptado de *(Rahman et al., 2020)*

El análisis del presente estudio evaluará el impacto de la implementación de Prometheus en la seguridad informática de la universidad, en términos de detección temprana de vulnerabilidades y mejora en los tiempos de respuesta frente a ataques. Además, se abordarán los requisitos necesarios para cumplir con las normas ISO 27001, que exigen un monitoreo y auditoría continua de los sistemas críticos de la organización. La investigación comparará Prometheus con otras herramientas de monitoreo, destacando su flexibilidad, escalabilidad y facilidad de integración, lo que lo convierte en una opción viable para instituciones educativas con infraestructuras tecnológicas complejas.

Comparación de Herramientas: Capacidades y Limitaciones.

En el contexto de la implementación de un sistema de monitoreo y análisis de registros en servidores, es esencial comprender la relevancia y las capacidades de las herramientas que se van a utilizar. A continuación, se presenta un análisis ampliado con un enfoque en su integración y las implicaciones que tiene para la solución propuesta en este trabajo.

Tabla 2

Análisis de herramientas

Herramienta	Capacidades	Limitaciones	Licencias y Costos
Grafana	- Visualización avanzada mediante dashboards.	- No gestiona datos directamente, requiere integración con herramientas externas para la recolección de datos.	- **Open Source**: Gratis (características básicas).
	- Integración con múltiples fuentes de datos (Prometheus, ElasticSearch, etc.).	- Configuración inicial compleja.	- **Grafana Cloud**: Desde $49/mes (para 3 usuarios y hasta 50 GB de datos).
	- Alertas en tiempo real personalizables.		
Prometheus	- Recopila métricas en tiempo real a través de scraping.	- No recolecta registros, se enfoca principalmente en métricas.	- **Open Source**: Gratis.
	- Sistema de series temporales eficiente.	- Falta de soporte nativo para seguridad avanzada (autenticación/autorización).	- No hay versión paga directa, pero puede haber costos si se integra con servicios de terceros (e.g., Grafana Cloud).
	- Alertmanager para alertas personalizadas.		
	- Escalable y flexible.		
Graylog	- Recolección y análisis de registros en tiempo real.	- Alta demanda de recursos en grandes volúmenes de datos.	- **Open Source**: Gratis para uso básico.
	- Compatible con múltiples plataformas (Windows, Linux).	- Algunas funciones avanzadas requieren versiones comerciales.	- **Graylog Enterprise**: Desde $1,500/año (para características avanzadas como archivado, auditoría, etc.).
	- Búsqueda rápida de registros históricos.	- Menos intuitivo que Grafana en visualización.	
	- Alertas basadas en eventos.		
Splunk	- Análisis avanzado de registros en tiempo real.	- Alto costo de licencias, especialmente en grandes despliegues.	- **Splunk Enterprise**: Desde $200/GB/mes (licencias basadas en el volumen de datos procesados).
	- Búsqueda rápida y eficiente a gran escala.	- Alta curva de aprendizaje para usuarios sin experiencia en análisis de registros.	- **Splunk Cloud**: A partir de $120/GB/mes.
	- Funciones avanzadas de machine learning.	- Elevado consumo de recursos.	
	- Soporte comercial robusto.		

	- Paneles visuales interactivos.		
ELK Stack	- Elasticsearch permite búsquedas eficientes en grandes volúmenes de registros.	- Complejidad en la configuración inicial del stack.	- **Open Source**: Gratis.
	- Logstash recopila, procesa y transforma registros de múltiples fuentes.	- Escalabilidad limitada sin ajustes avanzados.	- **Elastic Cloud (SaaS)**: Desde $95/mes por 120 GB de almacenamiento y 2 GB de RAM (puede aumentar dependiendo del uso).
	- Kibana proporciona visualizaciones avanzadas y personalizables.	- Gestión y mantenimiento más laboriosa en comparación con otras soluciones.	
	- Integración flexible y gratuita (open source).		

Nota: Creación propia.

Grafana sigue siendo una opción ideal para la visualización de datos provenientes de registros y métricas en tiempo real. Sin embargo, su verdadera fortaleza radica en la capacidad de crear dashboards personalizados y altamente visuales que permiten analizar el estado de sistemas y servidores de manera intuitiva. A pesar de su versatilidad, Grafana no recopila datos por sí misma, lo que significa que requiere integrarse con herramientas especializadas en la recolección de métricas o registros, tales como Prometheus o Elasticsearch.

Prometheus es una de las principales herramientas que complementan a Grafana, enfocada en la recolección de métricas y series temporales. Su capacidad para realizar scraping en sistemas distribuidos y almacenar datos en una base de datos optimizada para series temporales lo convierte en una solución poderosa para el monitoreo de servidores. Sin embargo, Prometheus no está diseñado para gestionar registros, lo que limita su alcance en la detección de anomalías basadas en registros.

Para el análisis de registros, Elasticsearch, dentro del stack ELK (ElasticSearch, Logstash, Kibana), se convierte en un aliado esencial. Al integrarse con Grafana, Elasticsearch permite realizar búsquedas eficientes en grandes volúmenes de datos y analizar registros históricos para detectar comportamientos anómalos o posibles ataques de seguridad. Esta integración crea un entorno robusto para la gestión centralizada de registros y visualización de datos.

En el marco de este trabajo, la combinación de Grafana con herramientas de recolección como Prometheus para métricas y Elasticsearch para registros, representa una

solución completa y escalable para el monitoreo centralizado y análisis de logs en los servidores de la IES. Esto permite no solo la detección de fallos operacionales, sino también la identificación de amenazas de seguridad en tiempo real, proporcionando un enfoque proactivo para la gestión de la seguridad de los sistemas.

1.1.5 Estudios Previos y Casos de Éxito

Implementaciones de Seguridad en Entornos Académicos

La creciente dependencia de sistemas informáticos y la proliferación de datos sensibles exigen un enfoque proactivo para proteger la infraestructura tecnológica y la información confidencial de las instituciones educativas.

El Panorama de Amenazas 2024 de Kaspersky revela que la compañía bloqueó 1,185,242 ataques de ransomware en América Latina entre junio de 2023 y julio de 2024, lo que representa un aumento del 2.8% en el último año. En América Latina hubo 1.185.242 ataques, es decir, 3.247 al día. (Kaspersky, 2024)

Según el informe Estado de Ciberseguridad en Ecuador, elaborado por la firma Deloitte, que encuestó a cerca de 100 empresas a escala nacional: El 51% de las organizaciones tiene un responsable que cubre la seguridad física y digital. El 13% no cuenta con un experto entre su personal. Pero, además solo el 3% de las empresas aplican herramientas que amortiguan los riesgos cibernéticos de almacenamiento en la nube. (Sayago-Heredia, 2022)

Las instituciones estatales han fortalecido sus políticas de seguridad de la información como se encuentra estipulado en el acuerdo ministerial Nro. 166 de la Constitución del Ecuador en la que el gobierno ecuatoriano ha decretado la adopción de la norma ISO 27002 para la seguridad de la información (Chifla-Villón et al., 2020).

Pareciera una tarea sencilla el adquirir el hardware y software para la ciberseguridad, pero no es así, esto requiere de inversión, conocimiento en la configuración de las herramientas informáticas, y la capacidad de integrarlas a las plataformas empresariales. Sin dejar a un lado al usuario que labora en la organización, al cual se le debe capacitar en políticas institucionales para la prevención. (Cedeño Villacís, 2022)

Ecuador no cuenta con un instrumento legal que emita lineamientos para gestionarlos riesgos cibernéticos y proteger las infraestructuras críticas de manera integral

desde una perspectiva nacional, en colaboración y coordinación con los sectores público y privado, la academia y la sociedad civil. (Pico-Verdezoto et al., 2023)

Este trabajo se centra en una institución de educación superior IES como caso de estudio, dado la creciente complejidad de sus infraestructuras tecnológicas y la necesidad de proteger una amplia gama de datos sensibles, donde la proliferación de servidores sin un adecuado análisis de registros representa una vulnerabilidad significativa. A pesar de la presencia de firewalls perimetrales, la falta de un repositorio centralizado de registros impide una detección proactiva de amenazas y una respuesta efectiva a incidentes. Con el objetivo de abordar estas deficiencias, se propone una arquitectura de seguridad basada en tecnologías open source, que permitirán recolectar, almacenar y visualizar datos de registros de manera eficiente, facilitando la identificación de patrones anómalos y la detección temprana de incidentes de seguridad.

A nivel mundial se ha trabajado mucho en la centralización de los registros. Se han desarrollado muchas herramientas con gran potencia y velocidad de procesamiento, capaces de recoger los registros y además a partir de la información que contienen realizar reportes y gráficas de los datos recolectados, todo lo cual se hace en tiempo real. (López & García, 2008)

La extrema importancia de realizar una adecuada gestión de los registros en toda organización, la implementación de una solución debería ser el resultado de un proyecto que empiece por un análisis de las metas y requerimientos que exige cada escenario desde su particular situación y la identificación de los objetivos generales y específicos a conseguir mediante el análisis de la información recolectada. (Carrión, 2015)

1.2 Desarrollo Teórico y Conceptual

1.2.1 Conceptualización de la seguridad en servidores

Fundamentos de la seguridad en servidores

La seguridad de los servidores ha evolucionado de una postura reactiva a una proactiva. Hoy en día, las organizaciones más resilientes se anticipan a las amenazas, implementando medidas de seguridad en profundidad que van más allá de los firewalls tradicionales. La detección temprana de anomalías, el análisis conductual de usuarios y entidades, y la automatización de respuestas a incidentes son elementos clave para mantener los servidores a salvo en un panorama de amenazas en constante evolución.

Uno de los problemas de mayor envergadura a los que las empresas u organizaciones deben enfrentarse para alcanzar estos objetivos, y principalmente las pequeñas y medianas, es el que se relacionan con la capacidad del crecimiento, del uso del hardware y software para cubrir sus necesidades operativas y les obliga a tener que abordar de forma continua aquellos temas que se relacionan con los costos, versatilidad, escalabilidad y funcionabilidad de estos componentes. (Arévalo Cordovilla et al., 2021).

La relevancia de valorar la seguridad lógica de estos servidores reside en la relación entre la protección de la información, el análisis y la elección de normas que faciliten un alineamiento en los controles de seguridad y sus métodos de validación mediante herramientas confiables y pertinentes. (Chifla-Villón et al., 2020)

En Sudamérica se realizó un estudio enfocado a los problemas latentes de inseguridad informática y el robo de la información, vulnerabilidad, hackeo, phishing entre otras amenazas en organizaciones financieras y de otra índole. Esta investigación de acuerdo con el Índice Global de Ciberseguridad (IGC) en el Ecuador ocupa el puesto 79 de 127 países respecto a la seguridad en el ranking internacional relacionado a la vulnerabilidad y evaluación de riegos(Castillo Enríquez et al., 2022)

Riesgos y amenazas comunes en servidores.

Los servidores, independientemente de su función, se encuentran expuestos a una amplia gama de amenazas cibernéticas en constante evolución. Desde ataques tradicionales como la denegación de servicio (DoS) y los exploits de vulnerabilidades conocidas, hasta las sofisticadas campañas de ransomware y los ataques dirigidos, la seguridad de los servidores es un desafío constante. La creciente interconexión de sistemas, la proliferación de dispositivos IoT y la adopción de tecnologías en la nube expanden la superficie de ataque, haciendo que la protección perimetral sea insuficiente. Es fundamental adoptar una estrategia de seguridad proactiva que combine medidas preventivas, detectivas y correctivas, respaldada por una gestión de parches rigurosa y una capacitación continua del personal.

Los delitos informáticos representan un acto ilícito existente en las redes de información (web), que atenta contra la propiedad privada intelectual de la sociedad, las organizaciones y el Estado en general. (Acosta et al., 2020)

Tabla 3

Riesgos y amenazas en servidores

Riesgo/Amenaza	Descripción
Ataques a la capa de red	Intentos de comprometer la comunicación entre dispositivos de red, como escaneos de puertos, ataques de denegación de servicio (DoS/DDoS), y ataques de intermediario.
Explotación de vulnerabilidades	Aprovechamiento de fallas de software o configuración para obtener acceso no autorizado, ejecutar código malicioso o causar daños al sistema.
Malware	Software malicioso diseñado para infectar sistemas, robar datos, cifrar archivos (ransomware) o causar daños.
Phishing	Engaño a usuarios para que revelen información confidencial a través de correos electrónicos, mensajes o sitios web falsos.
Ingeniería social	Manipulación de personas para obtener información confidencial o acceso a sistemas.
Ataques de fuerza bruta	Intentos repetidos de adivinar contraseñas para obtener acceso no autorizado.
Ataques de diccionario	Uso de listas de palabras comunes o combinaciones de caracteres para adivinar contraseñas.
Ataques de inyección (SQL, XSS)	Introducción de código malicioso en entradas de usuario para manipular la ejecución de aplicaciones y bases de datos.
Acceso no autorizado	Acceso a sistemas o datos por parte de personas no autorizadas.
Pérdida o corrupción de datos	Pérdida accidental o intencional de datos debido a fallos del sistema, desastres naturales o ataques cibernéticos.
Robo de identidad	Suplantación de la identidad de una persona para cometer fraude.

Espionaje industrial	Robo de información confidencial de una empresa para obtener una ventaja competitiva.
Sabotage	Daño intencional a sistemas o datos para causar disrupción o pérdida de servicio.
Insiders threats	Amenazas internas, como empleados descontentos o socios comerciales deshonestos, que pueden comprometer la seguridad de la información.

Nota: Creación propia.

La tabla anterior nos da una mirada breve de los diferentes riesgos y amenazas a los que están expuestas las infraestructuras de servidores de las instituciones, pero además se pueden considerar otros riesgos como:

- **Configuración incorrecta:** Errores en la configuración de los servidores pueden exponerlos a vulnerabilidades.
- **Falta de parches:** No aplicar actualizaciones de seguridad puede dejar los servidores expuestos a exploits conocidos.
- **Contraseñas débiles:** Contraseñas fáciles de adivinar facilitan el acceso no autorizado.
- **Falta de segmentación de redes:** Una red mal segmentada permite que un ataque se propague rápidamente.
- **Falta de respaldo de datos:** La ausencia de copias de seguridad puede resultar en la pérdida permanente de datos en caso de un incidente de seguridad.

Es importante destacar que esta lista evoluciona y que las amenazas cibernéticas también y de forma constante. Para proteger eficazmente los servidores, es necesario implementar una estrategia de seguridad integral que incluya medidas preventivas, de detección y correctivas, así como una evaluación de riesgos continua.

Importancia del Monitoreo y Análisis de Registros

El monitoreo y análisis de registros se ha convertido en un pilar fundamental para la ciberseguridad moderna. Estos registros detallados de las actividades de un sistema ofrecen una valiosa pista para detectar anomalías, identificar amenazas emergentes y responder de manera proactiva a incidentes. Al correlacionar eventos de múltiples

fuentes, es posible reconstruir la cronología de un ataque, identificar a los atacantes y determinar el alcance del daño. Además, los registros permiten cumplir con los requisitos de cumplimiento normativo y auditoría, proporcionando evidencia de las actividades realizadas en el sistema.

Las trazas generadas por los sistemas de hardware y software tienen una importancia fundamental en el proceso de gestión de la seguridad de la información. Dentro de los principales documentos está la guía de buenas prácticas de la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) ISO/IEC 27002 como parte de la norma certificable ISO/IEC 27001. La sección 12, seguridad de las operaciones, se dedica al tratamiento de las trazas y la subsección 12.4, registro y monitoreo. (Porven Rubier et al., 2015).

Debido a que la información que se almacena en los registros puede ser utilizada como evidencia digital (por evidencia digital se entiende toda información obtenida a partir de una computadora o equipo electrónico que permite el esclarecimiento de algún hecho delictivo o ayuda a vincular al autor con el propio hecho), en la actualidad se les da mucha importancia, por lo que se han redefinido determinados criterios indispensables para tener en cuenta para ser usados en un posible caso judicial. (López & García, 2008)

El registro y análisis de registros es una práctica fundamental en la gestión de sistemas informáticos. Los registros son registros detallados de eventos que se han producido en el sistema, y su análisis puede proporcionar información valiosa sobre el rendimiento, la seguridad y la estabilidad del sistema.(Suárez, 2022)

1.2.2 Modelos y Principios de Seguridad

1.2.2.1 Confidencialidad, Integridad y Disponibilidad

La aparición de las Tecnologías de la Información y Comunicación (TIC) y su nivel de dependencia por parte de las organizaciones y el uso adecuado de la información, inició la necesidad de una adecuada implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita garantizar la adecuada protección de la información empresarial y mantener los niveles aceptables de riesgo. (Damian Vasquez, 2023)

La confidencialidad, integridad y disponibilidad (CIA) conforman la tríada de seguridad de la información, estableciendo los pilares fundamentales sobre los cuales se construye cualquier sistema de protección de datos. La confidencialidad garantiza que la

información sea accesible únicamente a aquellos usuarios autorizados, preservando así su privacidad y evitando fugas de datos sensibles. La integridad asegura que la información se mantenga precisa, completa y confiable, protegiéndola de alteraciones no autorizadas. Por último, la disponibilidad garantiza el acceso oportuno y continuo a la información por parte de los usuarios autorizados, minimizando las interrupciones en los servicios.

La confidencialidad de la información es clave para el crecimiento y sostenibilidad de la empresa, por ello se debe prevenir la divulgación no autorizada de la información empresarial. Sulay et al., s. f.).

La integridad de la información garantiza que los datos se mantengan precisos, completos y consistentes a lo largo de su ciclo de vida. Esto implica proteger los datos de cualquier modificación no autorizada, ya sea accidental o intencional. Al asegurar la integridad de la información, se previene la pérdida de confianza en los datos, se evitan decisiones erróneas basadas en información incorrecta y se cumple con los requisitos legales y normativos aplicables.

1.2.2.2 Autenticación, Autorización y Auditoría (AAA)

Autenticación: Este primer componente se encarga de verificar la identidad de los usuarios que intentan acceder a los sistemas. En el entorno de la UPSE, se utilizarán métodos robustos de autenticación, como la autenticación de dos factores (2FA) y la integración con servicios de identidad, para asegurar que solo usuarios autorizados tengan acceso a los servidores y aplicaciones críticas, como el SGA y Moodle.

Un sistema de autenticación para ser más concisos se refiere a "un conjunto de procedimientos y protocolos informáticos que se utilizan para verificar la identidad de un usuario y permitirle el acceso a un sistema o servicio" (Marmolejo Corona et al., 2023)

Autorización: Una vez que un usuario ha sido autenticado, es esencial determinar qué recursos y operaciones puede realizar. Para esto, se implementarán políticas de control de acceso que definirán roles y permisos específicos dentro del sistema. Por ejemplo, los administradores del sistema tendrán acceso total, mientras que los usuarios finales solo podrán acceder a las funcionalidades necesarias para su interacción diaria. Esta segmentación es clave para minimizar riesgos y asegurar que los datos sensibles se mantengan protegidos.

Auditoría: Finalmente, la auditoría proporciona un registro detallado de todas las actividades realizadas en el sistema. Esto incluye quién accedió a qué datos, cuándo y qué

acciones se llevaron a cabo. La recopilación de registros a través de herramientas como Elasticsearch y Prometheus permitirá realizar un seguimiento efectivo de eventos críticos, así como detectar y responder a posibles incidentes de seguridad. La auditoría no solo cumple con los requerimientos de la norma ISO 27001, sino que también fortalece la postura de seguridad al permitir la identificación de patrones de uso y posibles vulnerabilidades en el sistema.

La auditoría informática en el contexto del Cloud Computing implica evaluar la gestión de la información, la seguridad de los datos y los controles implementados en los proveedores de servicios en la nube. Es fundamental asegurarse de que se cumplan las normativas y regulaciones aplicables en cuanto a la protección de datos personales. (Pilamunga, 2023)

1.2.2.3 Modelos de Amenazas y Mitigación

A medida que se implementan las estrategias de Autenticación, Autorización y Auditoría (AAA), se debe considerar un enfoque proactivo en la identificación y mitigación de amenazas potenciales.

La gestión y el tratamiento de las amenazas informáticas, es uno de los aspectos más importantes a considerar por parte de las organizaciones modernas, dedicando los recursos necesarios para poder responder a cualquier incidente de seguridad que surja. (Balseca-Chávez et al., 2021)

Identificación de Amenazas: Las amenazas pueden clasificarse en varias categorías, incluyendo amenazas internas (como empleados descontentos o malintencionados) y amenazas externas (como ciberataques o malware). Es vital realizar un análisis exhaustivo de los activos y sus vulnerabilidades, identificando posibles vectores de ataque. Herramientas de análisis de riesgos, como la evaluación de vulnerabilidades, serán fundamentales para este proceso.

Modelos de Amenazas: Existen varios modelos de amenazas que pueden aplicarse en el entorno universitario. El Modelo STRIDE, por ejemplo, se enfoca en los diferentes tipos de amenazas: suplantación de identidad (Spoofing), manipulación de datos (Tampering), denegación de servicio (Repudiation), revelación de información (Information Disclosure), denegación de servicio (Denial of Service) y elevación de privilegios (Elevation of Privilege). Al aplicar este modelo, se pueden desarrollar estrategias

específicas para cada tipo de amenaza, asegurando así una mayor protección de los sistemas de la UPSE.

Spoofing: la pretensión de ser alguien que no se es o el acto de algún usuario malintencionado que pretende ser, por ejemplo, un sitio web de confianza; Manipulación: el cambio en el flujo de datos real entre dos nodos; Repudio: la capacidad del remitente de negar el hecho de que envió un paquete específico o firmó un documento específico; Divulgación de información: el acceso a información confidencial que uno no debería tener, como el valor TTL de un paquete o datos confidenciales como credenciales de banca en línea o cualquier otra credencial de inicio de sesión. (Al-Azzawi & Lencse, 2023)

Mitigación de Amenazas: La mitigación debe abordarse desde múltiples ángulos. Por un lado, se pueden implementar medidas técnicas, como la segmentación de redes, la implementación de firewalls, y el uso de sistemas de detección y prevención de intrusiones (IDS/IPS). Además, la capacitación continua del personal en buenas prácticas de ciberseguridad es esencial para minimizar el riesgo de amenazas internas.

1.2.3 Centralización de Registros como Estrategia de Seguridad

A nivel mundial se ha trabajado mucho en la centralización de los registros. Se han desarrollado muchas herramientas con gran potencia y velocidad de procesamiento, capaces de recoger los registros y además a partir de la información que contienen realizar reportes y gráficas de los datos recolectados, todo lo cual se hace en tiempo real. (López & García, 2008)

El registro y análisis de registros es una práctica fundamental en la gestión de sistemas informáticos. Los logs son registros detallados de eventos que se han producido en el sistema, y su análisis puede proporcionar información valiosa sobre el rendimiento, la seguridad y la estabilidad del sistema. (Suárez, 2022)

Dentro del ámbito de la seguridad informática, la centralización de registros se ha vuelto una práctica imprescindible para incrementar la eficiencia y efectividad en la administración de incidentes y la observancia de regulaciones. Específicamente, para entidades con infraestructuras de Tecnología de la Información complejas, como las Universidades, la unificación de los registros producidos por varios sistemas y aparatos facilita una mayor visibilidad y un control más exacto de las actividades en la red. Este

método centralizado no solo mejora la identificación de riesgos y la reacción a incidentes, sino que también promueve el acatamiento de normativas, como la requerida por la norma ISO 27001, y potencia la toma de decisiones fundamentada en información.

A continuación, se exponen los beneficios más destacados de la implementación de

Ventajas de la Centralización de Registros

La centralización de registros se ha convertido en una estrategia fundamental para mejorar la seguridad de la información en organizaciones como Instituciones de Educación Superior. Esta técnica implica la recopilación y almacenamiento de registros de eventos de diversos sistemas y dispositivos en un único repositorio. A continuación, se detallan algunas de las principales ventajas de esta práctica.

Mantener una buena práctica en la gestión de los registros aporta varios beneficios, tanto a nivel de funcionamiento de los sistemas como a nivel de gestión de las seguridades. (Reyes et al., 2023)

- ✓ **Visibilidad Integral:** La centralización de registros proporciona una visión holística de la actividad en toda la infraestructura de TI. Esto permite a los administradores monitorear en tiempo real el comportamiento de los sistemas, facilitando la identificación de patrones inusuales que podrían indicar actividades maliciosas o incidentes de seguridad.
- ✓ **Detección Temprana de Amenazas:** Al consolidar los registros en un solo lugar, las organizaciones pueden implementar soluciones avanzadas de análisis y correlación de datos. Estas herramientas utilizan algoritmos para identificar comportamientos anómalos y posibles amenazas, lo que permite una respuesta más rápida ante incidentes de seguridad.
- ✓ **Facilitación de Auditorías y Cumplimiento Normativo:** La centralización de registros simplifica la recopilación de datos necesarios para auditorías y el cumplimiento de normativas, como la ISO 27001. Con registros bien organizados y accesibles, las organizaciones pueden demostrar fácilmente que están cumpliendo con los requisitos de seguridad y privacidad.
- ✓ **Reducción del Tiempo de Respuesta**: La capacidad de acceder a registros centralizados acelera el proceso de investigación de incidentes. Los equipos de seguridad pueden analizar rápidamente los registros relevantes para identificar la

causa raíz de un problema, permitiendo así una mitigación más eficiente de riesgos.

- ✓ **Mejora en la Gestión de Recursos:** La centralización permite optimizar el uso de recursos al reducir la necesidad de gestionar múltiples sistemas de registro. Esto no solo ahorra tiempo y esfuerzo, sino que también puede disminuir los costos operativos relacionados con el mantenimiento de herramientas diversas.
- ✓ **Fortalecimiento de la Toma de Decisiones:** Con acceso a datos centralizados y bien organizados, los responsables de la toma de decisiones pueden basar sus estrategias de seguridad en información precisa y actualizada. Esto les permite ajustar las políticas y controles de seguridad según sea necesario, asegurando una postura proactiva frente a las amenazas.

1.2.3.1 Arquitectura de sistemas para la centralización de Registros

El análisis de grandes cantidades de datos en el área de la seguridad de la información es considerado como un área de trabajo reciente, y requiere de una amplia investigación, así como establecer una arquitectura tecnológica que ofrezca una alta capacidad de almacenamiento, flexibilidad técnica y con una inversión de capital menos costosa, para hacer frente a las amenazas informáticas, con el apoyo del análisis de datos con herramientas de Big Data. (Balseca-Chávez et al., 2021)

Las arquitecturas de centralización de registros están diseñadas para facilitar la recopilación, almacenamiento y análisis de registros de eventos generados por diferentes servidores y aplicaciones dentro de la infraestructura tecnológica de una institución. A continuación, se describen los elementos clave que componen esta arquitectura.

- ✓ **Componentes de Recopilación:** La arquitectura incluye agentes de recopilación de registros instalados en cada servidor, que se encargan de capturar eventos y métricas relevantes.
- ✓ **Servidor Central de** Registros**:** En el corazón de la arquitectura se encuentra un servidor dedicado a la centralización de registros, que recibe y almacena la información proveniente de los diferentes agentes. Este servidor puede estar basado en plataformas robustas como Elasticsearch, que permite el almacenamiento eficiente y la búsqueda rápida de registros.

  El cuadrante mágico de Garner incluye en el mes de febrero 2021 a Elastic, descrito en la figura 2, dentro de los principales quince proveedores de motor de

información que combina las capacidades de búsqueda con la inteligencia artificial, para ofrecer información procesable derivada del espectro completo de contenido y datos (Balseca-Chávez et al., 2021)

- ✓ **Sistema de Análisis y Correlación:** Integrado con el servidor central, se debe implementar un sistema de análisis y correlación que permita identificar patrones y comportamientos anómalos en los datos recopilados. Herramientas como Kibana o Grafana pueden ser utilizadas para visualizar los registros y facilitar la identificación de incidentes de seguridad.
- ✓ **Seguridad y Acceso Controlado:** La arquitectura debe incluir mecanismos de seguridad que protejan tanto la transmisión como el almacenamiento de registros. Esto puede lograrse mediante la implementación de protocolos de comunicación seguros (como TLS) y controles de acceso que garanticen que solo el personal autorizado tenga acceso a los datos sensibles.
- ✓ **Mecanismos de Alerta:** Para asegurar una respuesta proactiva ante incidentes, es fundamental incorporar un sistema de alertas que notifique al equipo de seguridad sobre eventos críticos. Estas alertas pueden configurarse para activarse en función de umbrales específicos o patrones identificados, permitiendo una intervención rápida.
- ✓ **Integración con Otras Herramientas de Seguridad:** La arquitectura también debe ser capaz de integrarse con otras herramientas de seguridad existentes, como sistemas de detección de intrusiones (IDS) y soluciones de gestión de eventos e información de seguridad (SIEM). Esta integración permitirá una gestión más efectiva de la seguridad en la infraestructura de TI.
- ✓ **Escalabilidad y Flexibilidad:** Finalmente, es importante que la arquitectura sea escalable y flexible para adaptarse a futuras expansiones o cambios en la infraestructura tecnológica de la universidad. Esto asegura que la centralización de registros continúe siendo efectiva a medida que se incorporen nuevos sistemas y aplicaciones.

Desafíos y Consideraciones Técnicas

La implementación de estrategias de seguridad para servidores presenta una serie de desafíos y consideraciones técnicas que deben abordarse para garantizar la efectividad del plan. A continuación, se describen algunos de estos aspectos críticos:

- ✓ **Complejidad de la Infraestructura:** La UPSE cuenta con una infraestructura compuesta por más de 100 servidores virtualizados, lo que aumenta la complejidad del monitoreo y la gestión de la seguridad. Esta diversidad de entornos puede dificultar la implementación de políticas uniformes de seguridad y la centralización de registros, ya que cada servidor puede tener configuraciones y aplicaciones distintas.
- ✓ **Integración de Herramientas:** La selección e integración de herramientas para la centralización de registros y el análisis de seguridad representan un desafío significativo. Es esencial que las herramientas elegidas sean compatibles entre sí y con los sistemas existentes en la universidad. La falta de integración puede llevar a silos de información, donde los datos no se comparten de manera efectiva entre diferentes plataformas.
- ✓ **Capacitación del Personal:** La efectividad de cualquier estrategia de seguridad depende en gran medida de la capacidad del personal para utilizar las herramientas y procesos implementados. Por lo tanto, es fundamental invertir en la capacitación continua del personal de TI, asegurando que comprendan no solo cómo utilizar las herramientas, sino también la importancia de las normativas de seguridad como ISO 27001.
- ✓ **Gestión de Cambios y Actualizaciones:** A medida que la tecnología avanza y se actualizan los sistemas, la gestión de cambios se convierte en una consideración crítica. Es fundamental establecer procedimientos claros para la actualización de sistemas y herramientas de seguridad, evitando que las brechas de seguridad se amplifiquen debido a configuraciones obsoletas o vulnerabilidades no atendidas.
- ✓ **Escalabilidad y Flexibilidad:** A medida que la universidad continúa creciendo y expandiendo su infraestructura tecnológica, es vital que las estrategias de seguridad sean escalables y flexibles. Esto implica la capacidad de adaptar las políticas y herramientas a nuevos entornos, sin comprometer la seguridad existente.
- ✓ **Cumplimiento Normativo y Legal:** Garantizar el cumplimiento de normativas de seguridad, como la ISO 27001, representa otro desafío significativo. La universidad debe estar atenta a las actualizaciones de estas normativas y asegurarse de que sus políticas y procedimientos se alineen con los requisitos

legales y de auditoría, lo que puede requerir revisiones regulares y auditorías externas.

- ✓ **Costos y Recursos:** Finalmente, la implementación de una estrategia de seguridad efectiva puede requerir inversiones significativas en herramientas, capacitación y recursos humanos. La UPSE debe equilibrar estos costos con su presupuesto disponible, buscando soluciones rentables que aún proporcionen la protección necesaria.

1.2.4 Normativas ISO 27000 y su Implementación

Uno de los requisitos para implementar un SGSI (Sistema de Gestión de Seguridad de la Información), en una organización es conocer los estándares, su estructura y la relación existente entre cada uno de ellos. Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), compuesta por aproximadamente 17 normas. (Damian Vasquez, 2023)

La familia de normas ISO 27000 proporciona un marco global para la gestión de la seguridad de la información, estableciendo directrices que ayudan a las organizaciones a proteger sus datos críticos. La ISO 27001, una de las normas más conocidas de esta serie, establece los requisitos para desarrollar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), que permite a las organizaciones gestionar sus riesgos de seguridad de manera eficaz. Mientras tanto, la ISO 27002 ofrece un conjunto de mejores prácticas y controles para fortalecer los procesos de seguridad.

Además, que los pilares principales de esta familia son las normas 27001 y la 27002. La principal diferencia entre estas dos normas es que 27001 se basa en una gestión de la seguridad de forma continua apoyada en la identificación de los riesgos de forma continuada en el tiempo. En cambio, 27002, es una mera guía de buenas prácticas que escribe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones. (Damian Vasquez, 2023)

Implementar la ISO 27000 implica un enfoque estructurado para gestionar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Esta implementación no solo requiere controles técnicos y procedimientos documentados, sino también la sensibilización de los empleados, para que la seguridad sea una responsabilidad compartida. Al adoptar estas normativas, las empresas pueden

cumplir con requisitos regulatorios y normativos, aumentar la confianza de los clientes y socios, y mejorar su resiliencia frente a amenazas de ciberseguridad.

Estructura y Requisitos de la ISO 27001

La norma ISO 27001 establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) eficaz, que permite a las organizaciones gestionar de manera adecuada los riesgos de seguridad. La estructura de esta norma sigue un enfoque basado en procesos y está diseñada para ser compatible con otras normas de gestión de la ISO.

La ISO 27001 establece directrices que se deben aplicar con el objetivo de asegurar la privacidad y la protección de la información. Además, en términos de integridad, es esencial resguardar la información para prevenir que se altere sin el permiso otorgado por la organización. ISO 27001 contribuye a establecer procesos para asegurar la integridad de los datos. (Sulay et al., 2020)

La ISO 27001 se estructura en varias secciones clave:

- Contexto de la organización: Aquí, se evalúan las circunstancias internas y externas que afectan a la seguridad de la información, definiendo claramente el alcance del SGSI.
- Liderazgo: Establece la responsabilidad de la alta dirección para el compromiso y apoyo en la gestión de la seguridad de la información, asegurando que los objetivos de seguridad estén alineados con la estrategia organizacional.
- Planificación: Implica la evaluación de riesgos y oportunidades, junto con la implementación de controles adecuados para mitigar esos riesgos de seguridad.
- Apoyo: Cubre los recursos, competencias, comunicación y documentación necesarias para gestionar el SGSI de manera eficiente.
- Operación: Detalla cómo deben gestionarse los procesos de seguridad de la información en el día a día, incluidos la identificación de riesgos y la implementación de los controles.
- Evaluación del desempeño: Se requiere una evaluación continua del sistema a través de auditorías internas y análisis para garantizar su eficacia.
- Mejora: La organización debe trabajar constantemente en la mejora continua del SGSI para corregir deficiencias y adaptarse a nuevas amenazas.

En el contexto de la centralización y análisis de registros, la ISO 27001 exige que las organizaciones implementen mecanismos para la monitorización continua de eventos y registros. Los registros proporcionan un registro detallado de las actividades del sistema, facilitando la detección de incidentes de seguridad. La correcta centralización de estos registros, seguida de un análisis proactivo, permite identificar comportamientos anómalos que podrían comprometer la seguridad.

Controles de Seguridad Relacionados con el Monitoreo de Servidores

En el marco de la implementación de la ISO 27001, uno de los aspectos cruciales es la aplicación de controles de seguridad efectivos para el monitoreo continuo de los servidores. Estos controles están orientados a proteger la información y a garantizar la disponibilidad y confiabilidad de los sistemas que soportan las operaciones críticas de una organización.

Los sistemas de seguridad han ido progresando a través del tiempo. En ese contexto los sistemas ISO han ido aportando elementos importantes a la seguridad desde la planificación de esta hasta el monitoreo permanente. La influencia existente permite establecer un horizonte seguro y confiable para los usuarios. (Sulay et al., 2020)

Los controles relacionados con el monitoreo de servidores incluyen la recolección y centralización de registros de eventos y actividades. Esta práctica permite analizar patrones de comportamiento que puedan indicar incidentes de seguridad, como accesos no autorizados o modificaciones sospechosas. Los servidores deben estar configurados para generar registros detallados que cubran tanto el acceso a recursos críticos como cambios en configuraciones del sistema.

El monitoreo y revisión es un proceso para medir la eficiencia y efectividad de los controles establecidos para la gestión del riesgo. (Fernández, 2021)

El monitoreo proactivo, permite identificar intentos de ataque y vulnerabilidades en tiempo real, brindando a los administradores de seguridad la capacidad de actuar antes de que se materialice una brecha. Además, la ISO 27001 enfatiza la importancia de integrar este monitoreo con un proceso de gestión de incidentes que garantice una respuesta adecuada y la documentación de las lecciones aprendidas para mejorar continuamente los controles de seguridad.

Integración de la ISO 27001 con Metodologías de Seguridad

La integración de la ISO 27001 con metodologías de seguridad resulta clave para mantener un entorno seguro y controlado, especialmente en la supervisión y análisis continuo de infraestructuras. Herramientas como Grafana, Prometheus y Elasticsearch juegan un papel importante en el monitoreo, aseguramiento y auditoría, alineándose con los principios de la ISO 27001 al facilitar un enfoque proactivo en la gestión de incidentes y riesgos.

La ISO 27001 establece la necesidad de implementar controles que aseguren la disponibilidad, confidencialidad e integridad de la información. En este contexto, Prometheus permite recolectar métricas de sistemas y aplicaciones, garantizando la observación en tiempo real de cualquier anomalía que pudiera comprometer la seguridad. Grafana, por su parte, visualiza esos datos de una manera comprensible y permite a los equipos de seguridad actuar rápidamente al detectar posibles vulnerabilidades o incumplimientos de políticas.

Además, Elasticsearch contribuye al cumplimiento de la norma al centralizar y analizar grandes volúmenes de registros, permitiendo correlacionar eventos y detectar patrones inusuales. Esta integración asegura una visión completa de la infraestructura tecnológica, clave para aplicar metodologías de seguridad como la gestión de incidentes y el monitoreo continuo de riesgos. Con estas herramientas, los controles recomendados por la ISO 27001 se fortalecen, facilitando la prevención de amenazas y la mejora continua de la postura de seguridad.

1.2.5 Desarrollo de una Estrategia de Seguridad Integral

Un Plan de Seguridad basado en la familia de normativas ISO 27000 implica establecer un conjunto de políticas, procedimientos y controles que aseguren la confidencialidad, integridad y disponibilidad de la información dentro de una organización. Esta serie de normativas ofrece un marco integral para gestionar la seguridad de la información y está estrechamente vinculada a la ISO 27001, que especifica los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

En este argumento, la implementación de herramientas de monitoreo como Grafana, Prometheus y Elasticsearch permite dar soporte a un Plan de Seguridad eficaz. Estas herramientas son clave para la recolección, visualización y análisis de datos,

proporcionando una plataforma robusta para identificar riesgos en tiempo real, detectar incidentes de seguridad, y realizar análisis forense en caso de violaciones.

Para superar este problema, el monitoreo de la red se puede realizar utilizando un sistema de monitoreo en tiempo real utilizando aplicaciones Prometheus y Grafana. Grafana puede proporcionar información sobre el estado de los componentes red en tiempo real enviando mensajes al administrador de la red vía Telegram. (Rahman et al., 2020)

El proceso de diseño comienza con la identificación de los activos críticos de información y la evaluación de los riesgos asociados en este caso. A partir de ahí, se definen controles basados en los lineamientos de la ISO 27001, como la supervisión continua de los sistemas, la gestión de incidentes y la evaluación de vulnerabilidades. Aquí es donde el monitoreo con Prometheus y la visualización con Grafana juegan un papel fundamental, ya que permiten a los equipos de seguridad tener una visión clara y en tiempo real del estado de los sistemas.

Prometheus es un software de alerta y monitoreo de sistemas que inicialmente es de código abierto creado en SoundCloud. Desde su inicio en 2012, muchas empresas y organizaciones lo han adoptado. Prometheus y tiene una comunidad de desarrolladores y usuarios muy activa. (Rahman et al., 2020)

Elasticsearch, por su parte, centraliza los registros y permite el análisis eficiente de grandes volúmenes de datos, facilitando la correlación de eventos de seguridad y proporcionando soporte para la toma de decisiones informadas. De esta forma, el plan de seguridad no solo se enfoca en la prevención, sino también en la respuesta rápida ante incidentes.

El Diseño de un Plan de Seguridad Basado en ISO 27000, apoyado por estas herramientas, asegura que los controles implementados sean dinámicos y que el monitoreo continuo facilite la mejora y adaptación constante frente a las amenazas emergentes.

Implementación de controles de seguridad.

La implementación de controles de seguridad enfocados en el monitoreo y la mejora continua es esencial para garantizar la protección constante de los activos de una organización. En el contexto de normativas como la ISO 27001, estos controles no solo

se aplican para detectar amenazas en tiempo real, sino también para asegurar que los sistemas estén en un proceso constante de evaluación y ajuste frente a riesgos emergentes.

Herramientas como Grafana, Prometheus y Elasticsearch desempeñan un rol crucial en la fase de monitoreo. Prometheus permite en el presente trabajo recopilar métricas detalladas del rendimiento y la seguridad de los sistemas, generando alertas ante comportamientos anómalos. Estas métricas son visualizadas en tiempo real a través de Grafana, lo que condesciende al equipo de seguridad identificar patrones y responder de manera proactiva ante posibles vulnerabilidades. Por otro lado, Elasticsearch facilita el análisis de grandes volúmenes de registros, permitiendo la correlación de eventos críticos y el análisis detallado de incidentes.

La mejora continua, como pilar de la ISO 27001, requiere que los datos recopilados sean utilizados para realizar evaluaciones periódicas de la eficacia de los controles implementados. Mediante el análisis de los registros centralizados y las métricas de monitoreo, las organizaciones pueden ajustar y optimizar sus estrategias de seguridad, garantizando que los controles sean adecuados frente a nuevas amenazas. Esto asegura que el ciclo de evaluación y adaptación sea una constante en la postura de seguridad de la organización, alineando las operaciones diarias con los objetivos estratégicos del sistema de gestión de seguridad de la información.

CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

La Universidad Estatal Península de Santa Elena (UPSE) es una institución de educación superior de carácter público, con autonomía en aspectos académicos, administrativos, financieros y orgánicos. Está financiada principalmente por el Estado ecuatoriano y pertenece al sistema de educación superior de Ecuador (UPSE, 2014). La universidad, como entidad pluralista y abierta a todas las formas de pensamiento universal, busca constantemente la mejora de sus procesos internos, particularmente en el área de tecnologías de la información y comunicación.

La investigación se desarrolló dentro del Departamento de Tecnologías de la Información y Comunicación (TIC) de la UPSE, localizado en el campus principal en La Libertad, provincia de Santa Elena, Ecuador. Este departamento es clave para el soporte académico y administrativo de la universidad, ya que administra los servidores y la infraestructura tecnológica que permite el funcionamiento eficiente de las diversas plataformas y servicios internos. Su infraestructura incluye una amplia gama de servidores y equipos de red que manejan el almacenamiento de información sensible y vital para la universidad.

Actualmente, en el Departamento de Tecnologías de la Información y Comunicación (TIC) de la Universidad Estatal Península de Santa Elena, no existe un sistema centralizado de monitoreo de registros que permita la gestión continua y eficiente de los eventos de seguridad. El manejo de los registros se realiza de manera manual, y únicamente se revisan los registros del servidor que presenta problemas específicos o fallos, lo que implica que no se lleva a cabo un monitoreo proactivo o constante.

Este enfoque reactivo genera varias limitaciones. Al no disponer de un sistema que centralice y automatice el análisis de registros, se corre el riesgo de que posibles incidentes de seguridad pasen desapercibidos. La falta de continuidad en la revisión de los registros puede ocasionar que ataques o vulnerabilidades queden sin detectar hasta que los daños sean significativos. Asimismo, el personal de TI se ve forzado a dedicar tiempo y recursos a la gestión de problemas ya avanzados, en lugar de anticiparse a posibles amenazas.

La implementación de un sistema centralizado y automatizado de gestión de registros, basado en herramientas como Grafana, Prometheus o Elasticsearch, resultaría

esencial para mejorar el monitoreo continuo, facilitando la detección temprana de anomalías, permitiendo la correlación de eventos y garantizando una mayor seguridad en los servidores.

La implementación de un sistema de análisis y monitoreo continúo basado en las normativas ISO 27000 tendría un impacto significativo en la organización. Estas normas establecen un marco integral de gestión de la seguridad de la información, asegurando que la organización pueda anticiparse a posibles amenazas, optimizar sus procesos de gestión de riesgos y mejorar la protección de sus activos digitales.

La ISO 27001, en particular, proporciona una estructura clara para establecer un Sistema de Gestión de Seguridad de la Información (SGSI), lo cual es esencial en un entorno universitario con datos sensibles. Aplicar estas normativas no solo mejora la seguridad, sino que también refuerza la reputación de la institución, asegura el cumplimiento regulatorio y ofrece un enfoque sistemático para la mejora continua en la protección de la información.

El Departamento de TIC ofreció un escenario propicio para implementar y analizar estrategias de seguridad en servidores, basadas en las normativas ISO 27001 y en metodologías especializadas en seguridad informática. A través de este entorno, fue posible llevar a cabo un estudio integral que abarcó desde la recolección de información, el monitoreo de registros, hasta la implementación de remediaciones efectivas. Esta investigación tiene como objetivo principal reforzar las políticas de seguridad de la universidad, contribuyendo al manejo de amenazas y a la mejora continua del sistema de gestión de seguridad de la información (SGSI).

2.2. Diseño y alcance de la investigación

El diseño de la presente investigación se basa en un enfoque analítico-explicativo, cuyo objetivo es estudiar y analizar el estado actual de la seguridad en los servidores de la Universidad Estatal Península de Santa Elena (UPSE) para proponer estrategias de mejora alineadas con la normativa ISO 27001. Dado que el análisis de la infraestructura y el monitoreo de los servidores forman el núcleo del proyecto, se emplearán métodos que permitan tanto la recopilación de datos cuantitativos (a través del análisis de registros y métricas) como cualitativos (por medio de encuestas y observación directa).

El **enfoque analítico** se justifica por la necesidad de descomponer el sistema de servidores en componentes específicos: servidores de aplicaciones, bases de datos, y

servicios críticos como Moodle y SGA. Cada uno será evaluado en términos de seguridad, disponibilidad, y eficiencia. El análisis de las vulnerabilidades detectadas en estas infraestructuras permitirá identificar las áreas de riesgo que requieren intervención.

Además, el **enfoque explicativo** se emplea para comprender las causas detrás de las vulnerabilidades y fallas en los sistemas de seguridad, así como los comportamientos observados en los servidores bajo estudio. Este enfoque busca no solo describir el estado actual de la seguridad, sino también ofrecer una explicación fundamentada de los problemas detectados y proponer soluciones basadas en las mejores prácticas internacionales.

Recopilación de Datos

Para la recopilación de información, se realizarán encuestas estructuradas dirigidas exclusivamente al director del departamento de TICs y al analista encargado de los servidores. Estas encuestas estarán orientadas a obtener información clave sobre el estado de la seguridad de los servidores, los procedimientos implementados, y el cumplimiento de los controles de la norma ISO 27001. Estas personas tienen un conocimiento profundo y directo de las operaciones del sistema, lo que garantiza que la información obtenida sea relevante y precisa.

Asimismo, se llevará a cabo observación directa y análisis del estado actual de los servidores, enfocándose en aspectos como la configuración de seguridad, el monitoreo de eventos, y la gestión de incidentes. Este proceso incluirá el análisis de registros obtenidos mediante herramientas especializadas, lo que permitirá recolectar datos cuantitativos sobre el comportamiento de los sistemas.

Justificación del Enfoque

El diseño **analítico-explicativo** es el más adecuado para el presente trabajo, ya que busca no solo identificar vulnerabilidades, sino también explicarlas a través del análisis de datos y de las encuestas al personal clave. La combinación de encuestas y observación directa proporcionará una visión detallada del estado de la infraestructura, mientras que el análisis de registros permitirá medir objetivamente la efectividad de las medidas de seguridad actuales.

2.3. Tipo y métodos de investigación

Para este proyecto, se implementará un enfoque mixto que integra métodos cuantitativos y cualitativos, aunque se priorizará un solo método para garantizar que los datos recopilados sean coherentes y alineados con los objetivos de la investigación.

Tipo de Investigación:

La investigación será aplicada y descriptiva, ya que se enfoca en la implementación de estrategias de seguridad en un entorno real, como lo es la infraestructura de servidores de la Universidad Estatal Península de Santa Elena (UPSE). Además, es explicativa, porque busca profundizar en las causas de las vulnerabilidades y brechas de seguridad detectadas, ofreciendo una explicación basada en el análisis de datos.

Métodos Cuantitativos:

Para la parte cuantitativa, se llevará a cabo un análisis de registros y métricas de seguridad recopiladas a través de herramientas especializadas como Elasticsearch y Prometheus. Estos datos permitirán obtener información precisa y objetiva sobre el comportamiento de los servidores, la frecuencia de incidentes de seguridad, y el nivel de cumplimiento con los controles de la norma ISO 27001. La recopilación de estos datos será continua y sistemática, proporcionando una base sólida para evaluar el estado actual de la seguridad.

Métodos Cualitativos:

El método cualitativo seleccionado será el de encuestas, aplicadas únicamente al personal del departamento de TICs y a los analistas de servidores. Las encuestas proporcionarán una perspectiva directa y profunda sobre las prácticas de seguridad actuales, las percepciones del personal sobre las fortalezas y debilidades del sistema, y las dificultades que enfrentan en la implementación de controles de seguridad. Estas encuestas permitirán complementar los datos cuantitativos obtenidos y proporcionar un contexto más amplio para la interpretación de los resultados.

Método Principal:

El método cualitativo será el principal, ya que las encuestas ofrecen información contextual y explicativa que no se puede obtener únicamente a través de los datos

cuantitativos. Al enfocarse en las experiencias y percepciones del personal responsable de la seguridad de los servidores, se podrá identificar con mayor claridad las áreas de mejora, así como las limitaciones operativas y técnicas que influyen en el cumplimiento de la norma ISO 27001.

La combinación de estos enfoques proporcionará un análisis integral de la seguridad en los servidores, permitiendo tanto la identificación de problemas técnicos a través de métricas, como la comprensión de las dinámicas organizativas que afectan la seguridad.

Relación de los Métodos con el Análisis de Logs, la ISO 27001 y los Controles de la ISO 27002.

El enfoque metodológico que combina métodos cuantitativos y cualitativos está estrechamente vinculado tanto con el análisis de registros como con el cumplimiento de las normas de seguridad, específicamente la ISO 27001 y la ISO 27002. Este enfoque no solo facilita la medición y gestión de riesgos, sino que también ayuda a verificar la correcta implementación de controles de seguridad establecidos por la ISO 27002, seleccionando las secciones más relevantes para la seguridad de los servidores.

Método Cuantitativo y Análisis de Registros

El análisis de registros es fundamental para evaluar la seguridad de los servidores y garantizar que los eventos críticos sean capturados y monitorizados. Para esto, el uso de herramientas como Elasticsearch, Prometheus y otros sistemas de recolección de registros permite obtener datos que cumplen con los controles de la ISO 27002, específicamente en las siguientes áreas:

Control 12.4: Registro y monitoreo: Esta sección de la ISO 27002 establece la necesidad de registrar actividades de los usuarios, eventos y fallos en los sistemas. Los métodos cuantitativos, como la recolección de registros, permiten analizar incidentes en tiempo real y cumplir con este control al asegurar que los registros de actividad de los servidores están completos y que los eventos críticos son monitoreados y almacenados de forma segura.

Control 12.6: Revisión de registros: El análisis de registros proporciona la capacidad de revisar regularmente los registros en busca de actividades sospechosas o comportamientos anómalos. Esto es esencial para la auditoría continua de seguridad y

garantiza que se cumpla con los requisitos de la ISO 27002 en términos de supervisión de los sistemas de información.

Control 13.1: Seguridad en las comunicaciones: El análisis de registros permite verificar la seguridad de las comunicaciones entre los servidores y otros sistemas críticos. Este control asegura que las conexiones entre servidores estén protegidas y que cualquier fallo o intento de intrusión sea detectado a través de la revisión de los registros.

Método Cualitativo y Gestión Organizativa

Las encuestas cualitativas realizadas al personal de TICs y a los analistas encargados de los servidores complementan la implementación de los controles de la ISO 27002, al proporcionar una visión operativa sobre cómo se ejecutan las políticas de seguridad y cómo se gestionan los riesgos asociados a la infraestructura tecnológica. Los controles cualitativos más importantes de la ISO 27002 relacionados con el aspecto organizacional son:

Control 5.1: Políticas de seguridad de la información: Las encuestas ayudan a evaluar si las políticas de seguridad están siendo adecuadamente implementadas y comprendidas por el personal. Este control es fundamental para asegurar que las estrategias de seguridad se ordenen con los objetivos de la organización y se lleven a cabo según los estándares.

Control 6.2: Gestión de riesgos de seguridad de la información: Al indagar en las percepciones del personal técnico sobre la gestión de riesgos, se puede determinar si los riesgos identificados a través del análisis de registros están siendo gestionados adecuadamente. Este enfoque cualitativo permite contrastar los resultados cuantitativos con la percepción y experiencia práctica del equipo de TI.

Control 16.1: Gestión de incidentes de seguridad de la información: Entender cómo el personal reacciona ante los incidentes detectados a través del análisis de registros es clave para evaluar la eficacia del plan de respuesta ante incidentes. Este control exige que haya procedimientos claros para gestionar y responder ante cualquier anomalía detectada en los servidores.

La combinación de métodos cuantitativos y cualitativos permite no solo la recolección de datos objetivos mediante registros, sino también la verificación de los controles administrativos y organizacionales que complementan la seguridad técnica. De esta manera, el análisis de registros se convierte en un componente crítico del ciclo de

gestión de riesgos, permitiendo que la organización cumpla tanto con los controles de la ISO 27001 como con los de la ISO 27002.

2.4. Población y muestra

Para el presente trabajo, la población objetivo se centrará en el personal clave del Departamento de Tecnologías de la Información y Comunicación (TICs). Este grupo es el encargado de gestionar la infraestructura tecnológica y garantizar la seguridad de los servidores en la institución.

Población

La población de este estudio está conformada por dos grupos específicos de profesionales dentro del departamento de TICs:

Director de TICs: persona responsable de la dirección estratégica y operativa del departamento. Su conocimiento es crucial para entender cómo se gestionan las políticas de seguridad y cómo se aplican los controles establecidos por la ISO 27001 e ISO 27002 en la universidad.

Analista encargado de servidores: responsable directo de la operación y monitoreo de los servidores de la universidad, incluyendo las actividades diarias de recolección y análisis de registros. Este rol es clave para evaluar el estado actual de los servidores y cómo se implementan las estrategias de seguridad basadas en la ISO.

Muestra

Dado el tamaño limitado de la población, se trabajará con una muestra no probabilística intencional, seleccionando directamente a los profesionales mencionados. No se aplicarán técnicas de muestreo aleatorio, ya que el objetivo es realizar un análisis profundo en base a las experiencias y conocimientos del personal especializado. Este enfoque asegura que la información recolectada sea directamente relevante y aplicable a los objetivos del estudio.

Tamaño de la Muestra

Para este estudio, se seleccionó una muestra de 7 personas del departamento de TICs de la Universidad Península de Santa Elena. La selección de la muestra se basa en la relevancia de los roles que los encuestados desempeñan en la gestión de la seguridad de servidores y en el monitoreo de registros. Dado que no todos los miembros del

departamento están directamente involucrados en estas funciones críticas, se decidió focalizar el estudio en aquellos con mayor responsabilidad en la implementación de medidas de seguridad y gestión de la infraestructura tecnológica. Esta muestra permite obtener datos valiosos y representativos de las personas clave que influyen en la seguridad de la universidad, garantizando la calidad y validez de los resultados del estudio.

Justificación del Tamaño

Este enfoque centrado en una muestra pequeña es adecuado debido a que el objetivo del estudio es analizar de manera profunda y detallada las prácticas de seguridad actuales. Al tratarse de un análisis especializado, donde se requiere información técnica específica y la aplicación de controles normativos, la recolección de datos cualitativos y cuantitativos de este grupo reducido es suficiente para cumplir con los objetivos de la investigación. Además, el tamaño de la muestra asegura que la investigación se concentre en la evaluación directa de los sistemas más críticos de la universidad.

2.5. Técnicas e instrumentos de recolección de datos

Para el proyecto, se emplearán una combinación de técnicas cualitativas y cuantitativas para asegurar una recolección exhaustiva y confiable de la información. El enfoque estará orientado a obtener datos específicos sobre la seguridad de los servidores y su alineación con las normativas ISO 27001 y ISO 27002.

Técnicas de Recolección de Datos

1. **Encuestas estructuradas:**

Se aplicarán encuestas dirigidas al director de TICs y al Analista encargado de servidores, con el objetivo de obtener información detallada sobre las políticas y procedimientos actuales en cuanto a la seguridad de los servidores y la gestión de registros.

Las preguntas estarán alineadas con los controles de la ISO 27002, específicamente en áreas como gestión de incidentes de seguridad, control de acceso y monitoreo de la infraestructura.

2. **Observación directa:**

Se realizará una observación directa de los sistemas y procedimientos de seguridad en los servidores críticos (por ejemplo, Moodle, SGA, servidores de bases de

datos como MariaDB) para analizar el estado actual y evaluar la implementación de los controles normativos.

La observación también permitirá analizar cómo se realiza la recolección, almacenamiento y monitoreo de registros en la infraestructura tecnológica de la universidad.

3. **Análisis de registros y métricas:**

Se utilizarán herramientas especializadas como Elasticsearch, Logstash, y Kibana (ELK) para la recolección y análisis de registros. Estas herramientas permitirán una evaluación cuantitativa del tráfico, incidentes y cualquier actividad sospechosa que pueda comprometer la seguridad de los servidores.

Los registros de seguridad serán correlacionados con los requisitos de la ISO 27001 para identificar brechas en los controles y posibles riesgos.

Instrumentos de Recolección

1. **Formularios de encuesta:**

Se diseñarán formularios con preguntas cerradas y escalas de valoración basadas en criterios específicos de seguridad. Estos formularios medirán aspectos clave como la eficacia de los controles de acceso, la gestión de incidentes, y el monitoreo de la actividad en los servidores.

Los cuestionarios serán distribuidos de forma electrónica, asegurando la anonimización de respuestas para fomentar la sinceridad en las percepciones sobre la seguridad actual.

2. **Plantillas de observación:**

Se utilizarán plantillas predefinidas para la observación de los sistemas de monitoreo, gestión de registros y análisis de incidentes. Estas plantillas estarán alineadas con los controles más relevantes de la ISO 27002 como los controles de acceso, auditoría, y la gestión de vulnerabilidades.

3. **Herramientas de análisis de seguridad:**

Adicionalmente, el uso de Prometheus y Grafana permitirá el monitoreo continuo de métricas de rendimiento y seguridad, proporcionando datos en tiempo real sobre la infraestructura tecnológica.

2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

Para asegurar la validez y confiabilidad de los instrumentos empleados en el levantamiento de información, se adoptarán estrategias rigurosas que permitan que los resultados obtenidos sean precisos, representativos y alineados con los estándares de seguridad establecidos por la ISO 27001 y la ISO 27002. En este contexto, las herramientas empleadas para la recolección de registros y el análisis de datos se evaluarán de manera constante para garantizar la calidad de los resultados.

Validez de los Instrumentos

La validez de los instrumentos empleados en la investigación se garantizará mediante la alineación directa de los datos obtenidos con los objetivos del estudio y los controles de seguridad especificados en la ISO 27001. Para ello, se aplicarán los siguientes criterios:

1. **Relevancia de los datos recopilados:**

Las herramientas seleccionadas para la recolección de registros, como Elasticsearch, Logstash y Kibana (ELK), son ampliamente reconocidas por su capacidad de manejar grandes volúmenes de datos y proporcionar análisis detallados de eventos y actividades. Estas herramientas permiten validar la calidad y relevancia de la información recopilada, asegurando que los registros capturen eventos significativos para la evaluación de la seguridad en los servidores.

2. **Adecuación de los instrumentos al contexto:**

Los instrumentos y técnicas de observación se diseñarán específicamente para adaptarse al entorno tecnológico de la Universidad Estatal Península de Santa Elena (UPSE), permitiendo que la recolección de datos refleje con precisión las características de la infraestructura y los sistemas de seguridad que están en uso.

3. **Alineación con los controles ISO 27002:**

Para asegurar que los instrumentos aplicados aborden todos los aspectos clave de la ISO 27001, se verificará que los registros y los procesos de monitoreo abarquen los controles más relevantes de la ISO 27002, como la gestión de incidentes, auditoría y el control de acceso. Esto garantizará que la información recopilada sea válida en términos de los estándares de seguridad requeridos.

Confiabilidad de los Instrumentos

La confiabilidad de los instrumentos se garantizará mediante la aplicación de procedimientos repetibles y el uso de herramientas tecnológicas confiables, lo que asegura que los datos obtenidos sean consistentes y reproducibles. Las siguientes estrategias se implementarán para aumentar la confiabilidad:

3.1 Pruebas piloto de los instrumentos:

Se realizarán pruebas piloto utilizando el stack ELK en un entorno de laboratorio, simulando las condiciones reales de operación de los servidores de la universidad. Estas pruebas permitirán identificar posibles ajustes en la configuración de las herramientas y evaluar su precisión antes de implementarlas en el entorno real de producción.

3.2 Correlación de datos entre herramientas:

Para aumentar la confiabilidad, los datos recopilados serán analizados mediante múltiples herramientas complementarias que se utilizan en el proceso de centralización de registros. La correlación de los registros provenientes de distintos servidores permitirá una mayor consistencia en la detección de patrones y la identificación de anomalías o incidentes de seguridad.

3.3 Documentación detallada de los procesos:

Cada paso del proceso de recolección de datos será documentado meticulosamente. Esto incluye configuraciones de herramientas, procedimientos de instalación y análisis de los resultados. Esta documentación detallada permitirá replicar los procedimientos en el futuro y verificar la confiabilidad de los datos obtenidos.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

En este capítulo, se describen detalladamente los pasos necesarios para la instalación de las herramientas y el servidor destinados a la recolección de métricas y registros. Además, se establece la estructura de los servidores que se consideran en esta propuesta.

3.1 Análisis de los resultados obtenidos mediante al departamento de Tics y su representación gráfica.

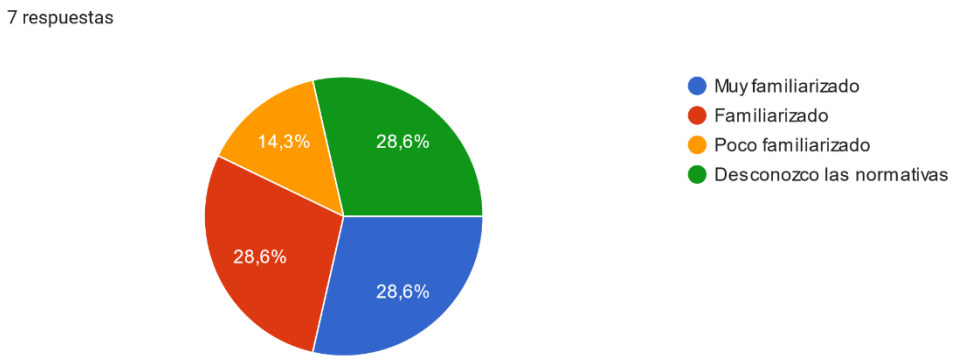
Para mantener la concentración del estudio en los elementos más esenciales de la seguridad y la centralización de registros en la infraestructura tecnológica de la Universidad Península de Santa Elena, se ha optado por incluir solo aquellos interrogantes del cuestionario que tienen una relevancia directa para los propósitos del estudio. Estas cuestiones tratan asuntos fundamentales como las políticas de seguridad establecidas, la situación actual del seguimiento de registros, y el nivel de acatamiento de las normas ISO 27001 e ISO 27002. Así, las respuestas recogidas ofrecerán un análisis detallado de las prácticas de seguridad y facilitarán la identificación de áreas fundamentales de mejora sin desviar la atención hacia elementos menos relevantes para la investigación.

3.1.1 Análisis de Preguntas de encuestas

1. **¿Nivel de familiaridad con las normativas ISO 27001 e ISO 27002?**

Figura 4

¿Nivel de familiaridad con las normativas ISO 27001 e ISO 27002?



El gráfico muestra los niveles de familiaridad del personal encuestado sobre las normas ISO 27001 e ISO 27002. De las 7 respuestas obtenidas, el 28.6% expresó tener un gran conocimiento de estas regulaciones, mientras que otro 28.6% declaró poseer un

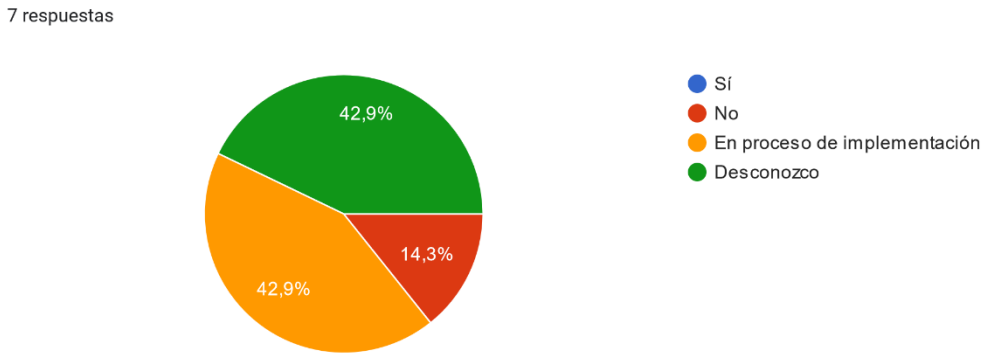
entendimiento general de ellas. Un 14.3% del personal se mostró poco familiarizado, mientras que el 28.6% restante admitió desconocer completamente las regulaciones.

Este escenario muestra una distribución balanceada entre los niveles de familiaridad, lo que indica que, aunque un segmento del equipo posee un sólido entendimiento de las regulaciones, aún hay un porcentaje significativo que podría aprovechar una mayor formación. Es esencial que todos los encargados de proteger los servidores y supervisar los registros posean el conocimiento apropiado sobre las regulaciones ISO.

2. **¿Existen políticas documentadas de seguridad específicas para la protección de los servidores en la universidad?**

Figura 5

¿Existen políticas documentadas de seguridad específicas para la protección de los servidores en la universidad?



El gráfico refleja las respuestas sobre la existencia de políticas documentadas de seguridad para la protección de los servidores en la universidad. Del total de encuestados, un 42.9% señaló que las políticas están en proceso de implementación, mientras que otro 42.9% desconoce si estas políticas existen o no. Solo un 14.3% respondió que no existen políticas documentadas en la actualidad.

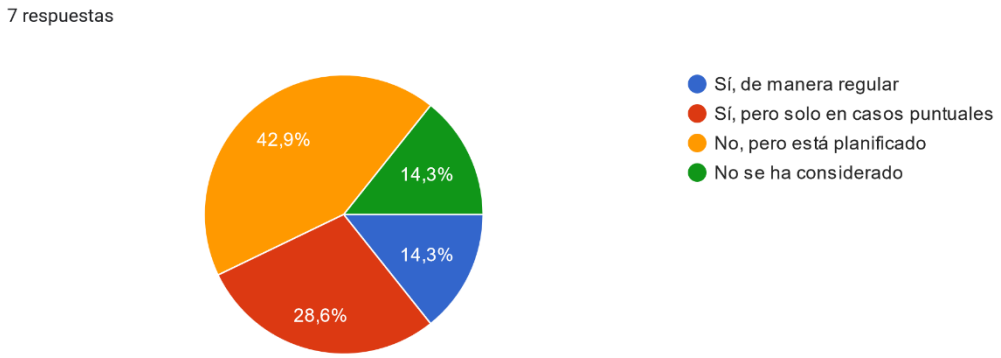
Este resultado pone de manifiesto una situación importante: aunque se están tomando medidas para implementar políticas de seguridad, casi la mitad del equipo no está al tanto de su existencia. Esto sugiere que, además de avanzar en la implementación de dichas políticas, es crucial mejorar la comunicación interna para asegurar que todos

los involucrados en la gestión de los servidores estén bien informados y puedan aplicar las medidas de seguridad de manera efectiva.

3. **¿El departamento de TICs ha realizado evaluaciones de riesgo para la infraestructura de servidores?**

Figura 6

¿El departamento de TICs ha realizado evaluaciones de riesgo para la infraestructura de servidores?



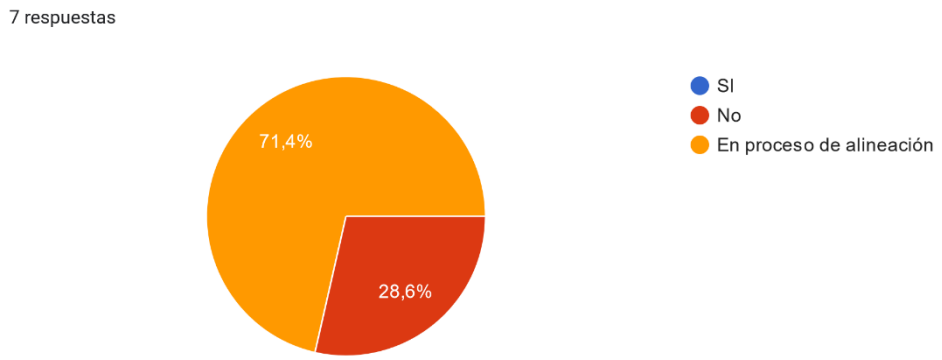
El gráfico refleja cómo se llevan a cabo las evaluaciones de riesgo en la infraestructura de servidores de la universidad. Un 42.9% de los encuestados indicó que, aunque **no** se realizan actualmente, estas evaluaciones **están planificadas**. Un 28.6% mencionó que solo se realizan en **casos puntuales**, mientras que el 14.3% aseguró que se llevan a cabo **de manera regular**. Finalmente, otro 14.3% indicó que **no se ha considerado** realizar evaluaciones de riesgo.

Este resultado muestra que, aunque la universidad tiene la intención de implementar evaluaciones de riesgo, su ejecución no es constante. Existe una oportunidad clara para mejorar y asegurar que estas evaluaciones se realicen de manera más frecuente, lo que fortalecería la seguridad de la infraestructura tecnológica.

4. **¿Considera que el sistema de monitoreo actual cumple con los controles de seguridad establecidos por la ISO 27001?**

Figura 7

¿Considera que el sistema de monitoreo actual cumple con los controles de seguridad establecidos por la ISO 27001?



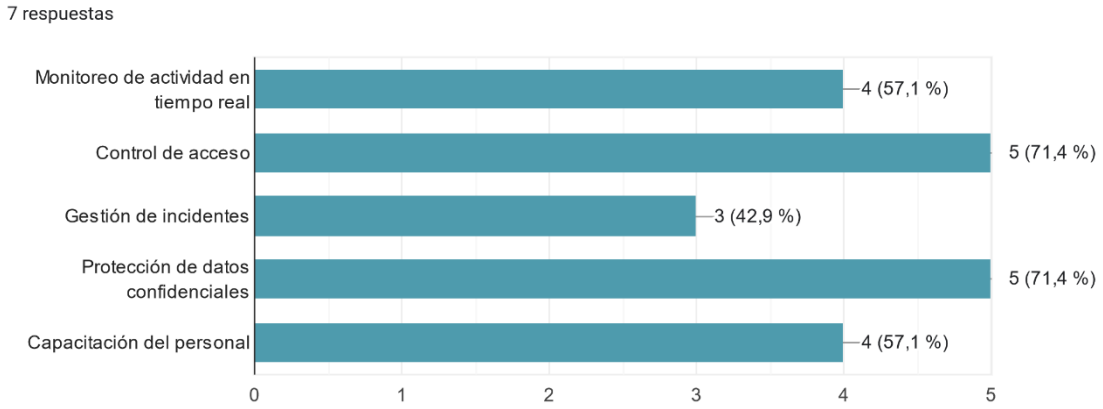
El gráfico muestra las respuestas sobre el cumplimiento del sistema de monitoreo con los controles de seguridad establecidos por la normativa ISO 27001. Un 71.4% de los encuestados indicó que el sistema se encuentra **en proceso de alineación** con la normativa, mientras que el 28.6% señaló que **aún no** se cumple con estos controles. Es importante destacar que ninguna respuesta afirmó un cumplimiento total en este momento.

Estos resultados indican que, aunque la universidad está tomando medidas para alinearse con la normativa ISO 27001, todavía queda trabajo por hacer para asegurar el cumplimiento completo. La implementación de procesos y ajustes en el sistema de monitoreo será clave para alcanzar los estándares establecidos y fortalecer la seguridad de los servidores.

5. **¿Qué áreas considera más críticas para mejorar la seguridad de los servidores?**

Figura **8**

¿Qué áreas considera más críticas para mejorar la seguridad de los servidores?



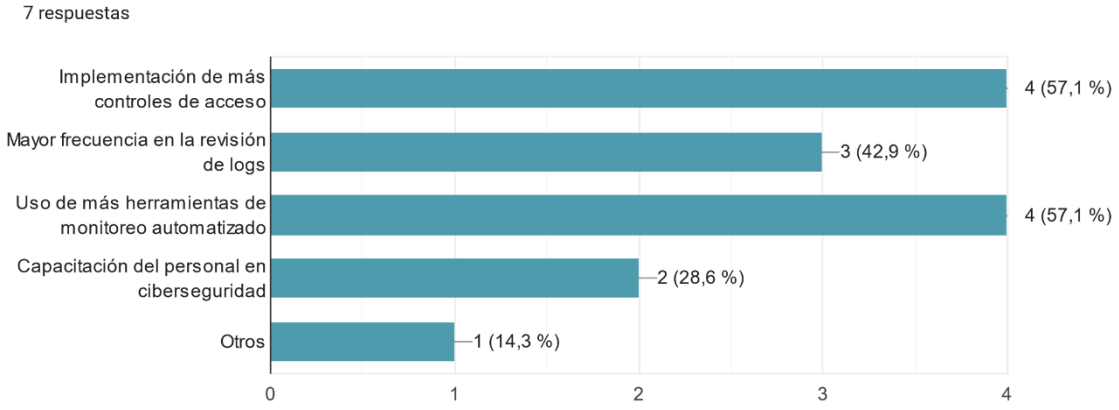
El gráfico muestra las áreas que los encuestados consideran más críticas para mejorar la seguridad de los servidores. El **control de acceso** y la **protección de datos confidenciales** son las áreas más mencionadas, con un 71.4% de los participantes que las señalan como prioritarias. Le siguen el **monitoreo de actividad en tiempo real** y la **capacitación del personal**, cada una con un 57.1% de respuestas. La **gestión de incidentes** fue señalada por un 42.9% de los encuestados.

Estos resultados indican que, si bien todas las áreas tienen importancia, el control de acceso y la protección de la información son vistas como los aspectos más urgentes a reforzar. Además, se destaca la necesidad de mejorar la formación del personal para garantizar que estén preparados ante posibles amenazas y situaciones de riesgo, así como de implementar sistemas más robustos de monitoreo en tiempo real para detectar anomalías de manera inmediata.

6. **¿Qué mejoras considera necesarias en la infraestructura actual de seguridad para cumplir con las normativas ISO 27001 e ISO 27002?**

Figura 9

Qué mejoras considera necesarias en la infraestructura actual de seguridad para cumplir con las normativas ISO 27001 e ISO 27002



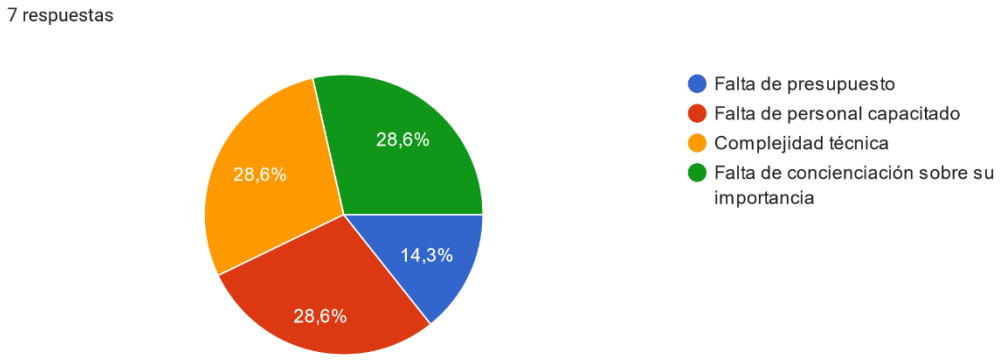
El gráfico muestra las mejoras que los encuestados consideran necesarias en la infraestructura de seguridad para cumplir con las normativas ISO 27001 e ISO 27002. Los resultados destacan que el **57.1%** de los participantes cree que es esencial implementar **más controles de acceso** y utilizar **más herramientas de monitoreo automatizado**. Además, un **42.9%** considera que es importante aumentar la **frecuencia en la revisión de registros**, mientras que un **28.6%** de los encuestados señala la **capacitación del personal en ciberseguridad** como un área clave de mejora. Solo un **14.3%** mencionó otras áreas no especificadas.

Estos resultados subrayan que el enfoque principal debe estar en fortalecer los controles de acceso y en la automatización del monitoreo, lo que permitiría una detección más rápida de incidentes. Sin embargo, también se observa una necesidad importante de mejorar las revisiones periódicas de los registros y asegurar que el personal esté adecuadamente capacitado en ciberseguridad, para garantizar una respuesta eficaz ante posibles amenazas.

7. **¿Cuál es el mayor obstáculo para implementar un sistema de centralización de registros?**

Figura 10

¿Cuál es el mayor obstáculo para implementar un sistema de centralización de registros?



El gráfico muestra las percepciones sobre los principales obstáculos para la implementación de un sistema de centralización de registros en la universidad. Las respuestas están bastante equilibradas: un **28.6%** de los encuestados considera que la **complejidad técnica** es el mayor desafío, mientras que otro **28.6%** menciona la **falta de concienciación sobre su importancia** como una barrera significativa. Un **28.6%** adicional destaca la **falta de personal capacitado**, y solo un **14.3%** indica que el principal obstáculo es la **falta de presupuesto**.

Este resultado refleja que, aunque el presupuesto es un factor, el desafío principal parece ser la combinación de la complejidad técnica, la falta de personal especializado y la necesidad de crear mayor conciencia sobre la importancia de la centralización de registros. Estos factores indican que, para avanzar en la implementación de este sistema, será clave invertir en formación técnica y en la concienciación sobre los beneficios que aporta a la seguridad de la infraestructura.

3.2 Definición de estructura para el análisis.

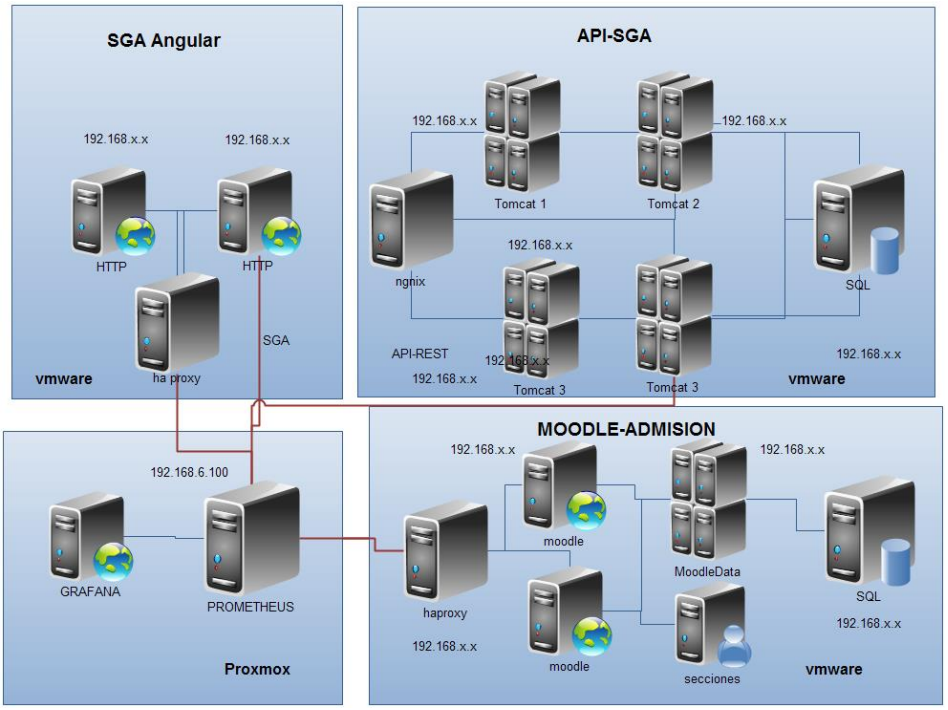
La Universidad Estatal Península de Santa Elena (UPSE) cuenta con más de 100 servidores virtualizados, los cuales proporcionan servicios a cada uno de los departamentos y áreas de la institución. Generalmente, los servidores que presentan una mayor demanda de recursos y disponibilidad son los correspondientes a las áreas estudiantiles, tales como el Sistema de Gestión Académica (SGA) y Moodle.

La estructura por analizar incluye los siguientes componentes: el servidor de aplicaciones, Moodle, SGA Angular y API-SGA. Estos elementos son cruciales para el funcionamiento efectivo de los servicios ofrecidos a los estudiantes y deben ser evaluados cuidadosamente en el contexto de la seguridad.

3.3 Estructura Grafana y Prometheus

Figura 11

Diagrama Grafana



En esta estructura, nos centraremos en la extracción de métricas de diversos servidores, tales como los servidores Tomcat, servidores Apache y bases de datos como MariaDB. Para facilitar esta comunicación entre los servidores, fue necesario habilitar ciertos puertos y VLANs, asegurando así un intercambio eficiente de información y métricas

críticas. Este enfoque permitirá una supervisión más efectiva del rendimiento y la seguridad de los sistemas involucrados.

Tabla 4

Puertos para Prometheus

Puerto	Servidor	VLAN
9100	Tomcat	400
9117	Apache	400
9104	MariaDB	400
9101	Haproxy	400
9090,9100,9117,9104,9101	MV Grafana y Prometheus	400,200

Esta arquitectura se sustenta en la implementación de agentes especializados en cada servidor, encargados de recolectar métricas sobre el rendimiento y estado del sistema. Estos agentes recopilan información clave, como el uso de recursos, actividad de servicios, y otros parámetros relevantes, y posteriormente envían estos datos a Prometheus. La transmisión de métricas se realiza a través de diversas configuraciones personalizadas en función de cada servicio o componente monitoreado, asegurando que Prometheus pueda centralizar y procesar eficientemente la información recolectada para su análisis.

Tabla 5

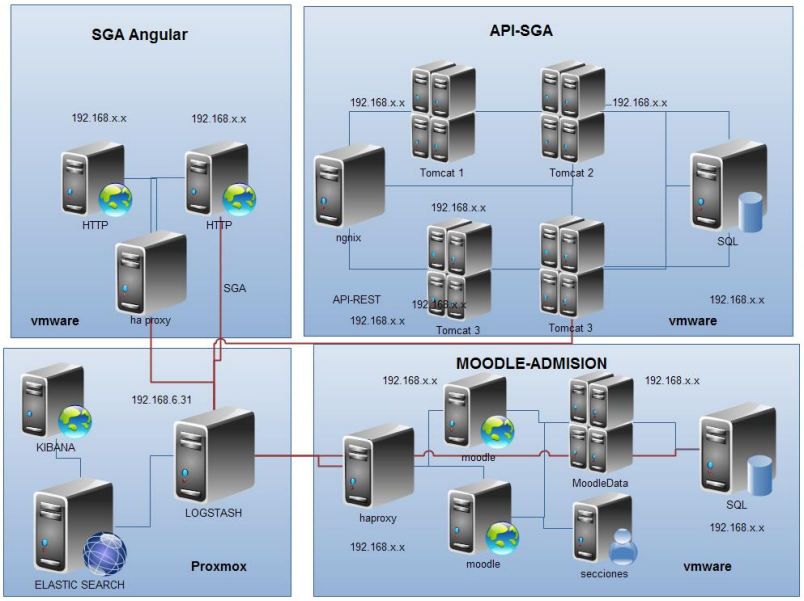
Exporte para Prometheus

Agente	Servidor
Node Exporter	Tomcat
Apache Exporter	Apache
MySQL Exporter	MariaDB
HAProxy Exporter	Haproxy

3.4 Estructura Kibana y Elastic search

Figura 12

Diagrama kibana y Elastic Search



En esta estructura nos enfocamos en la extracción de registros de diversos servidores, como Tomcat, Apache, bases de datos como MariaDB y servidores de balanceo de carga como HAProxy. Para lograr esto, se habilitaron los puertos y VLAN necesarios que permiten la comunicación fluida entre los servidores. Además, se realizaron ajustes en los servidores para garantizar la correcta generación de registros de log y el funcionamiento óptimo de cada servicio, asegurando que toda la información relevante se recopile de manera adecuada para su posterior análisis.

Tabla 6

Puertos kibana y elasticsearch

Puerto	servidor	Vlan
5044	Tomcat	400
5044	Apache	400
5044	Mariadb	400
5044	Haproxy	400
5601 , 9200, 5044	MV Kibana y ElasticSearch	400,200

La recolección de registros se llevó a cabo mediante el uso del agente Filebeat, que es un componente ligero diseñado para monitorear archivos de log en servidores y aplicaciones. Filebeat se encarga de recopilar datos de forma eficiente y enviar estos registros a Logstash, que actúa como el sistema de procesamiento central. Logstash se encarga de transformar y enriquecer los datos, aplicando filtros y manipulaciones necesarias para garantizar que la información sea relevante y esté en el formato adecuado. Finalmente, los datos procesados son enviados a Elasticsearch, donde se almacenan y pueden ser consultados y analizados en tiempo real.

Esta arquitectura permite un monitoreo efectivo y una visualización detallada de los registros, facilitando la detección de anomalías y la generación de informes

Instalación de Grafana y Prometeus

Paso 1 - Descargar Prometheus con los siguientes comandos

Wget

https://github.com/prometheus/prometheus/releases/download/v2.42.0/prometheus-2.42.0.linux-amd64.tar.gz

Paso 2 - Extraer el archivo descargado

tar -xvzf prometheus-2.42.0.linux-amd64.tar.gz

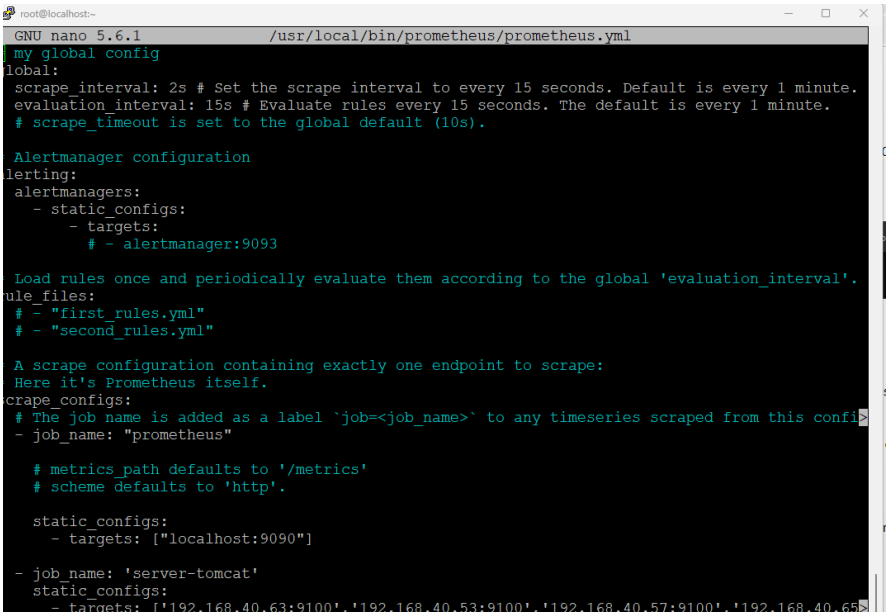
Paso 3 - Mover los archivos a un directorio adecuado

mv prometheus-2.42.0.linux-amd64 /usr/local/bin/prometheus

Paso 4 - Configurar Prometheus: Edita el archivo prometheus.yml para configurar tus targets y scrape configs.

Figura 13

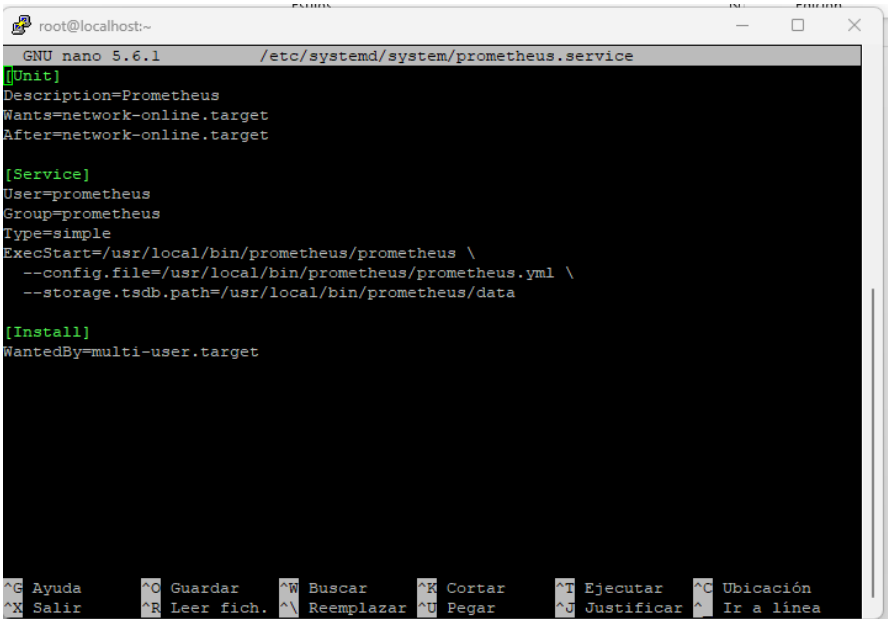
Prometheus.yml



Paso 5 - Crear un servicio de systemd para gestionar Prometheus de manera más convenient

Figura 14

Servicios Prometheus



Paso 6 - habilitamos los servicios con los siguientes comandos

Figura 15

Comandos Prometeus

```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

Paso 7 - Instalación de Grafana: agregamos la clave GPG para verificar los paquetes

Figura 16

Paquetes Grafana

```
sudo apt-get install -y software-properties-common wget
wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
```

Paso 8 - Agregar el repositorio APT de Grafana

Figura 17

Repositorio de Grafana

```
sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
```

Paso 9 - Instalamos Grafana con el siguiente comando.

- sudo apt-get install grafana

Paso 10 - Inicializamos y habilitamos Grafana con los siguientes comados

- sudo systemctl start grafana-server
- sudo systemctl enable grafana-server

Paso 11 - Configuración de Firewall

abrimos el puerto 3000 y 9090 para que Grafana y Prometheus se comuniquen entre si

Figura 18

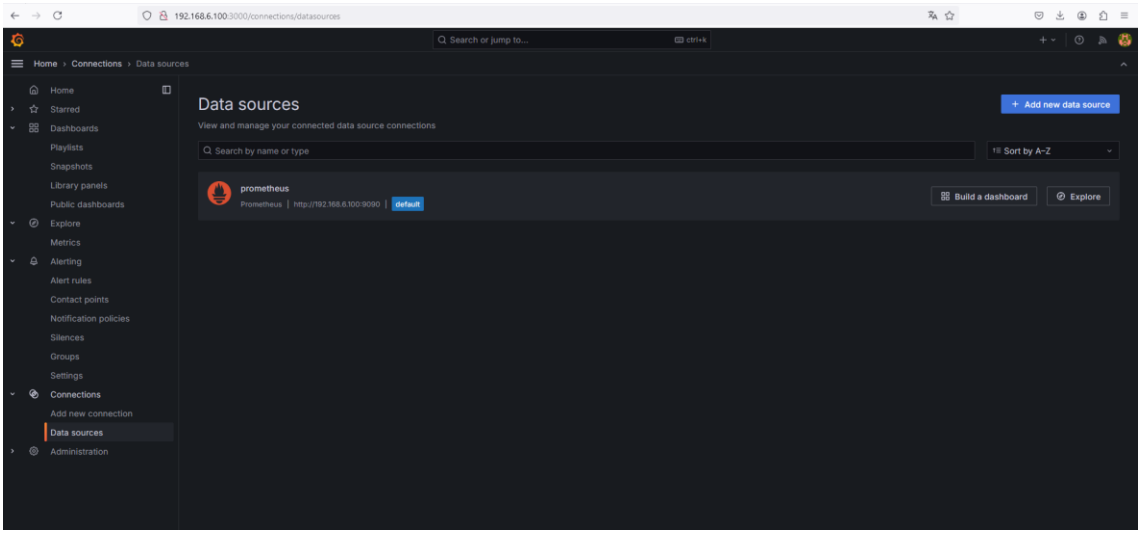
Puertos 3000 y 9090

```
68  firewall-cmd --zone=public --add-port=9090/tcp --permanent
69  firewall-cmd --reload
79  firewall-cmd --zone=public --add-port=3000/tcp --permanent
80  firewall-cmd --reload
```

Paso 12 - Creamos una nueva conexión para en Grafana

Figura 19

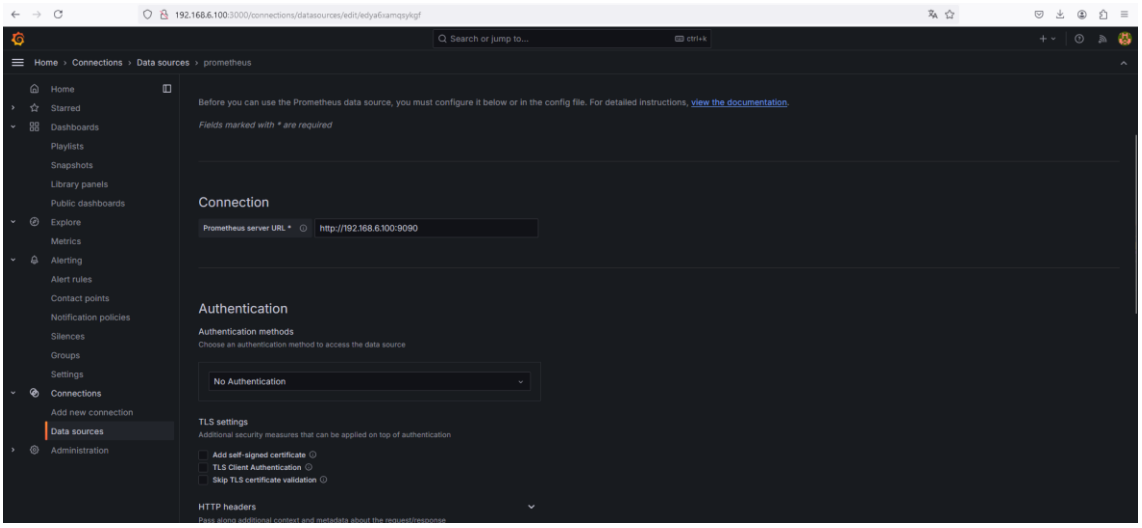
Conexión de Grafana



Apuntamos a nuestro servidor de Prometheus con el puerto especifico

Figura 20

Nueva conexión



1.3 Instalación de Agente Exporter Para los servidores de la Institución (UPSE)

Para esta instalación se analizó los servidores y sus servicios implementado versiones específicas para cada uno de ellos.

Paso 1 - Instalación de Node Exporte para servidores de aplicaciones

Descargamos la versión especifica que más se adapte a nuestro server .

https://github.com/prometheus/node_exporter/releases

Paso 2 - Extraer el archivo descargado en nuestra ruta

- tar -xvzf node_exporter-1.3.1.linux-amd64.tar.gz.
- sudo mv node_exporter-1.3.1.linux-amd64 /usr/local/bin/node_exporter

Paso 3 - Crear un usuario para Node Exporter

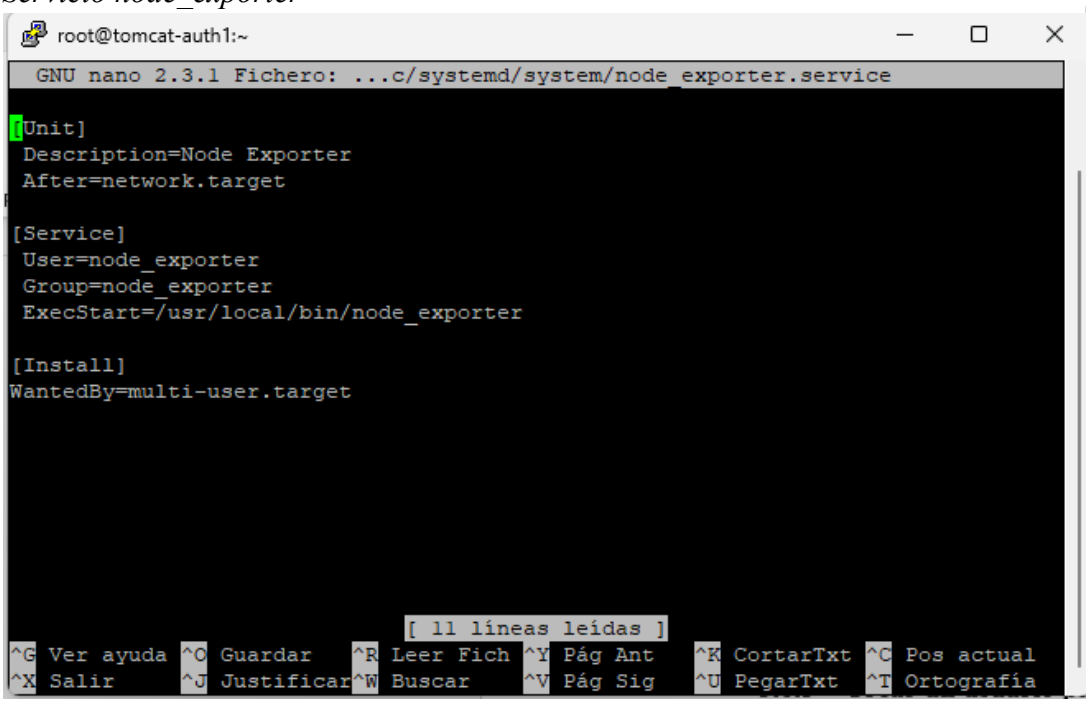
- sudo useradd --no-create-home --shell /bin/false node_exporter

Paso 4 - Crear un archivo de servicio systemd para Node Exporter

- sudo nano /etc/systemd/system/node_exporter.service

Figura 21

Servicio node_exporter



Paso 5 - Habilitamos Node Exporter

- sudo systemctl daemon-reload
- sudo systemctl start node_exporter
- sudo systemctl enable node_exporter

Paso 6 - Instalación de HAProxy Exporter

Primero, descarga el binario de HAProxy Exporter desde el repositorio oficial de Prometheus.

- wget https://github.com/prometheus/haproxy_exporter/releases/download/v0.13.0/haproxy_exporter-0.13.0.linux-amd64.tar.gz

Paso 8 - Mover el binario a un directorio adecuado

- sudo mv haproxy_exporter-0.13.0.linux-amd64/haproxy_exporter /usr/local/bin/

Paso 9 - Configurar el archivo haproxy.cfg para estadística

Para que HAProxy Exporter pueda recolectar métricas, es necesario que HAProxy esté configurado para generar estadísticas.

Figura 22

Configuración Haproxy

```
global
    stats socket /var/run/haproxy.sock mode 600 level admin

listen stats
    bind :8404
    stats enable
    stats uri /stats
    stats refresh 10s
```

Reinicia HAProxy después de realizar estos cambios:

- sudo systemctl restart haproxy

Paso 10 - Crear un servicio en systemd para HAProxy Exporter

Figura 23

HaProxy exporter service

```
[Unit]
Description=HAProxy Exporter
Wants=network-online.target
After=network-online.target

[Service]
User=root
ExecStart=/usr/local/bin/haproxy_exporter --haproxy.scrape-uri="unix:/var/run/haproxy.s

[Install]
WantedBy=multi-user.target
```

Paso 11 - Habilitación de servicio HAProxy Exporter

- sudo systemctl daemon-reload
- sudo systemctl enable haproxy_exporter
- sudo systemctl start haproxy_exporter

Paso 12 - Instalación de Apache Exporter

- wget https://github.com/Lusitaniae/apache_exporter/releases/download/v0.10.0/apache_exporter-0.10.0.linux-amd64.tar.gz

Paso 13 - Extraer y mover el binario

- tar xvf apache_exporter-0.10.0.linux-amd64.tar.gz
- sudo mv apache_exporter-0.10.0.linux-amd64/apache_exporter /usr/local/bin/

Paso 14 - Crear un archivo de servicio con systemd

Figura 24

Apache Exporter

```
[Unit]
Description=Apache Exporter
Wants=network-online.target
After=network-online.target

[Service]
User=root
ExecStart=/usr/local/bin/apache_exporter --scrape_uri=http://localhost/server-status?au

[Install]
WantedBy=multi-user.target
```

Paso 15 - Habilitar Apache Exporter

- sudo systemctl daemon-reload
- sudo systemctl enable apache_exporter
- sudo systemctl start apache_exporter

Paso 16 - Instalación del MariaDB Exporter

- wget https://github.com/prometheus/mysqld_exporter/releases/download/v0.14.0/mysqld_exporter-0.14.0.linux-amd64.tar.gz

Paso 17 - Extraer y mover el binario

- sudo mv mysqld_exporter-0.14.0.linux-amd64/mysqld_exporter /usr/local/bin/

Paso 18 - Crear usuario en MariaDB para el Exporter

Esta imagen es un ejemplo de configuración

Figura 25

Creación de Usuario exp

```
CREATE USER 'exporter'@'localhost' IDENTIFIED BY 'exporter_password';
GRANT PROCESS, REPLICATION CLIENT, SELECT ON *.* TO 'exporter'@'localhost';
FLUSH PRIVILEGES;
```

orter

Paso 19 - Establecemos los permisos adecuados para que solo el MariaDB Exporter pueda leer el archivo.

- sudo chown mysqld_exporter:mysqld_exporter /etc/.mysqld_exporter.cnf
- sudo chmod 600 /etc/.mysqld_exporter.cnf

Paso 20 - Crear un archivo de servicio systemd.

- sudo nano /etc/systemd/system/mysqld_exporter.service

Figura 26

Mysqlexporter

```
[Unit]
Description=Prometheus MySQL/MariaDB Exporter
After=network.target

[Service]
User=root
ExecStart=/usr/local/bin/mysqld_exporter --config.my-cnf=/etc/.mysqld_exporter.cnf
Restart=always

[Install]
WantedBy=multi-user.target
```

Paso 21 - Habilitar Mysql Exporter.

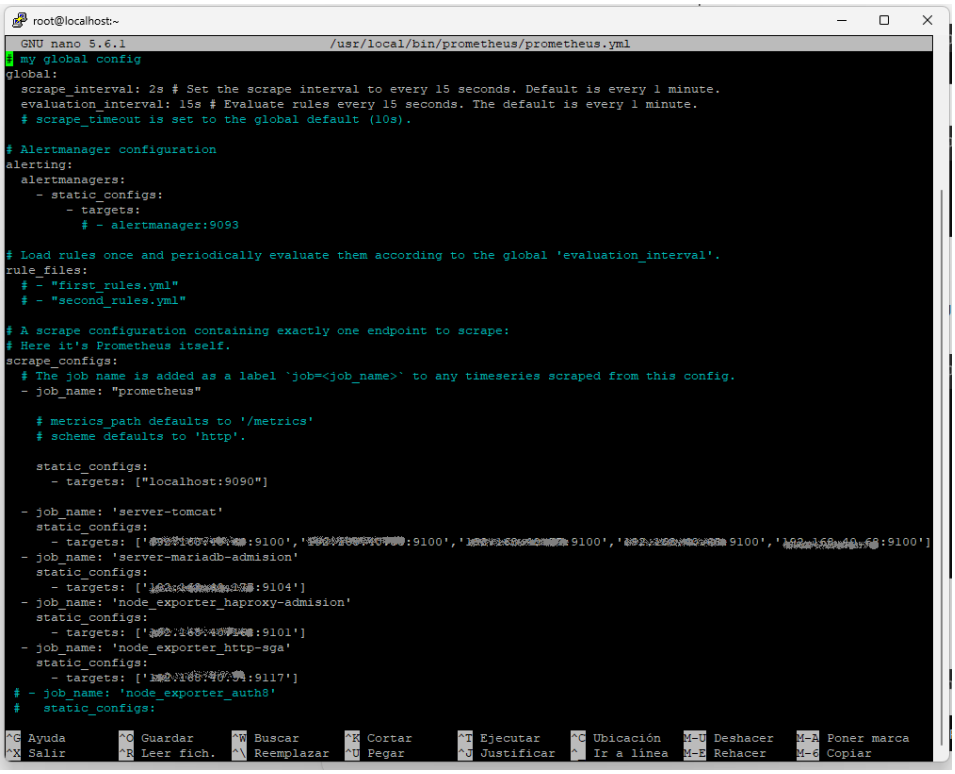
- sudo systemctl daemon-reload
- sudo systemctl enable mysqld_exporter
- sudo systemctl start mysqld_exporter

1.4 Configuración de Prometheus.

El archivo de configuración principal de Prometheus, prometheus.yml, especifica cómo recolectará métricas de varios servidores y servicios. Este archivo crea "trabajos", también conocidos como "Job", que indican a Prometheus de dónde debe extraer las métricas, especificando el nombre del trabajo y el puerto en el que opera cada exporter. Cada trabajo se refiere a un conjunto de puntos finales, generalmente exportadores, que Prometheus deberá vigilar. Aquí se le da a la tarea un nombre descriptivo y se le indica la dirección IP y el puerto específico a los que cada exporter está escuchando, lo que permite una recolección eficiente y organizada de métricas.

Figura 27

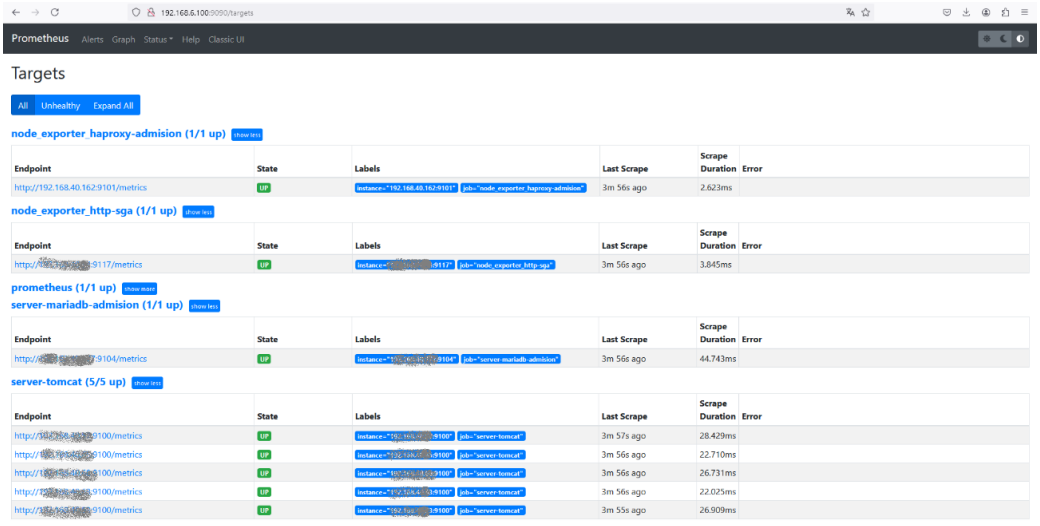
Configuraciones Prometheus



Con estas configuraciones podremos visualizar a través del puerto 9090 si nuestros targets se encuentran correctamente habilitados como podemos ver en la siguiente imagen.

Figura 28

Prometheus Estados

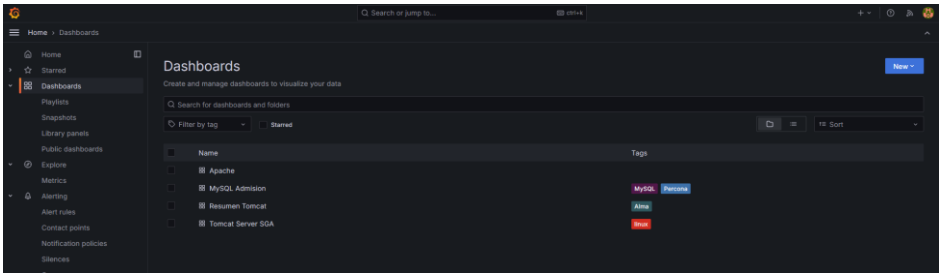


1.5 Creación e importación de dashboards para Grafana.

Se creo un dashboards para cada servidor registrado en prometheus

Figura 29

Dashboards Grafana



- Configuración de Registros de Query para cada Servicios

Figura 30

Query Grafana

- Dashboards de Aplicación resumen

Figura 31

Resumen Tomcat

- Dashboards de Tomcat Server SGA

Figura 32

Tomcat Server SGA

- Dashboards Mysql Admisión

Figura 33

Mysql Admisión

- Dashboards Apache

Figura 34

Dashboards Apache

1.6 Instalación de Elastic Stack.

La instalación de Elastic Stack (también conocido como ELK Stack) permite la recolección, el análisis y la visualización de datos de registros y métricas. La instalación de Elastic Stack en un sistema basado en Linux se detalla a continuación, utilizando Alma Linux.

Paso 1 - Importa la clave GPG

- sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

Figura 35

Repositorio ElasticSearch

```
cat <<EOF | sudo tee /etc/yum.repos.d/elasticsearch.repo
[elasticsearch-8.x]
name=Elasticsearch repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

Paso 2 - Comando de instalación de elasticsearch

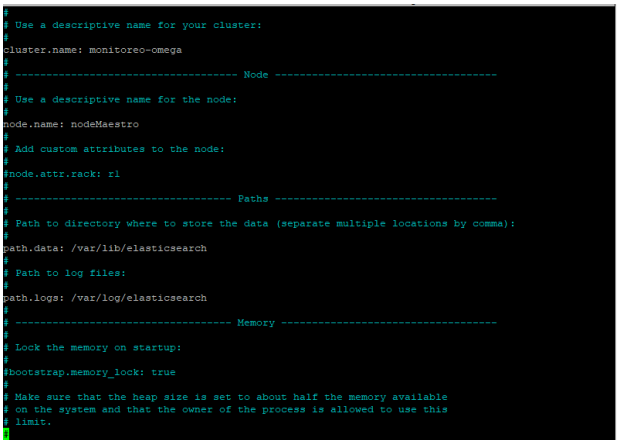
- sudo yum install elasticsearch
- sudo systemctl start elasticsearch
- sudo systemctl enable elasticsearch
- curl -X GET "localhost:9200/"

Paso 3 - Configuración de elasticsearch

- Se creo un clúster con el nombre de monitoreo-omega.
- Se lo asigno como nodo inicia

Figura 36

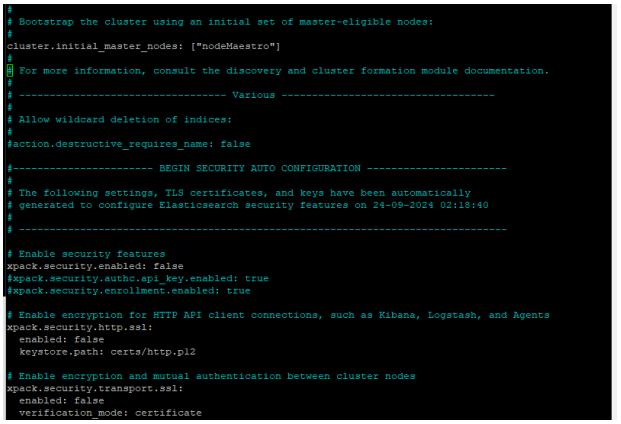
Configuración elasticsearch Parte 1



- habilito el acceso desde cualquier tipo de red

Figura 37

Configuración elasticsearch Parte 2



1.6.2 Instalación de Kibana

Figura 38

Repositorio Kibana

```
cat <<EOF | sudo tee /etc/yum.repos.d/kibana.repo
[kibana-8.x]
name=Kibana repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

Paso 1 - Comando de Instalación de Kibana

- sudo yum install kibana

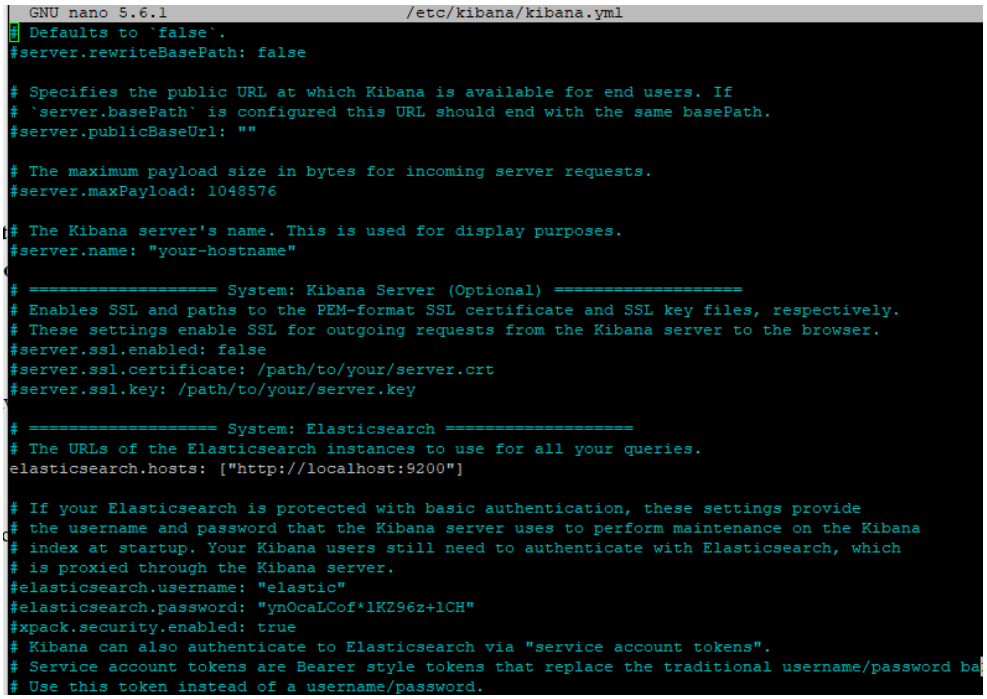
- sudo systemctl start kibana
- sudo systemctl enable kibana

Paso 2 - Configuración de Kibana

- Se agrego la conexión a elasticsearch

Figura 39

Configuración Kibana



1.6.3 Instalación de Logstash

Figura 40

Repositorio logstash

```
cat <<EOF | sudo tee /etc/yum.repos.d/logstash.repo
[logstash-8.x]
name=Elastic repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

Paso 1 - Comandos de Instalación

- sudo yum install logstash
- sudo systemctl start logstash

- sudo systemctl enable logstash

Paso 2 - Configuración de logstash

- Se creo un archivo de conexión para los agentes filebeat

Figura 41

Configuración de logstash

```
input {
  beats {
    port => 5044  # Asegúrate de que este puerto esté abierto en tu firewall
  }
}

filter {

 if "connection refused" in [message] or "failed to connect" in [message] {
    mutate { add_tag => ["connection_error"] }
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "upse-app"
 #   user => "elastic"
#    password => "ynOcaLCof*lKZ96z+lCH"
  }
}
```

1.6.4 Elastic Stack Estados

Verificamos que todos los servicios estén funcionando correctamente

- service logstash status

Figura 42

logstash status

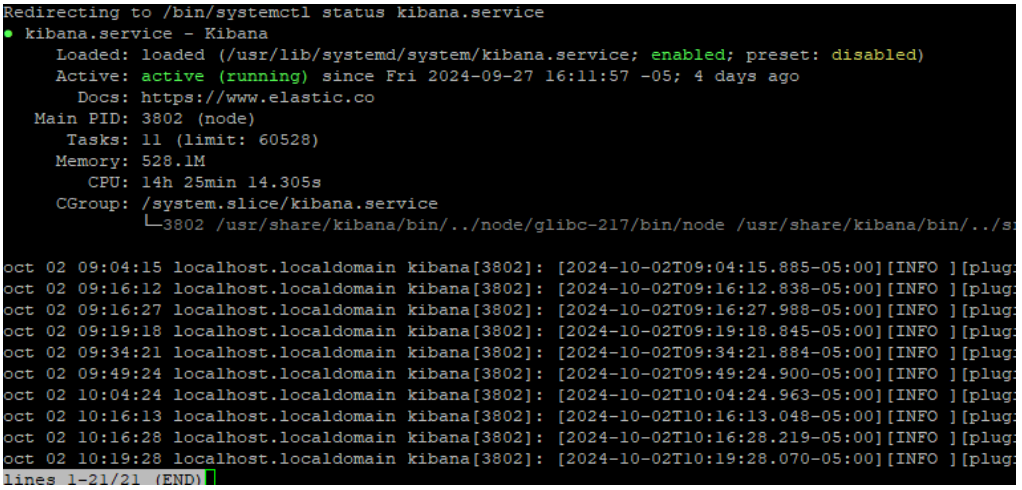
```
[root@localhost ~]# service logstash status
Redirecting to /bin/systemctl status logstash.service
● logstash.service - logstash
     Loaded: loaded (/usr/lib/systemd/system/logstash.service; disabled; preset: disabled)
     Active: active (running) since Mon 2024-09-30 12:27:49 -05; 1 day 21h ago
   Main PID: 13998 (java)
      Tasks: 61 (limit: 60528)
     Memory: 1.6G
        CPU: 6h 9min 24.542s
     CGroup: /system.slice/logstash.service
             └─13998 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfil>

sep 30 12:28:30 localhost.localdomain logstash[13998]: [2024-09-30T12:28:30,274][WARN ][logstash.o>
sep 30 12:28:30 localhost.localdomain logstash[13998]: [2024-09-30T12:28:30,306][INFO ][logstash.o>
sep 30 12:28:30 localhost.localdomain logstash[13998]: [2024-09-30T12:28:30,308][INFO ][logstash.o>
sep 30 12:28:30 localhost.localdomain logstash[13998]: [2024-09-30T12:28:30,329][INFO ][logstash.o>
sep 30 12:28:30 localhost.localdomain logstash[13998]: [2024-09-30T12:28:30,378][INFO ][logstash.j>
sep 30 12:28:32 localhost.localdomain logstash[13998]: [2024-09-30T12:28:32,145][INFO ][logstash.j>
sep 30 12:28:32 localhost.localdomain logstash[13998]: [2024-09-30T12:28:32,154][INFO ][logstash.i>
sep 30 12:28:32 localhost.localdomain logstash[13998]: [2024-09-30T12:28:32,210][INFO ][logstash.j>
sep 30 12:28:32 localhost.localdomain logstash[13998]: [2024-09-30T12:28:32,242][INFO ][logstash.a>
sep 30 12:28:32 localhost.localdomain logstash[13998]: [2024-09-30T12:28:32,415][INFO ][org.logsta>
```

- service kibana status

Figura 43

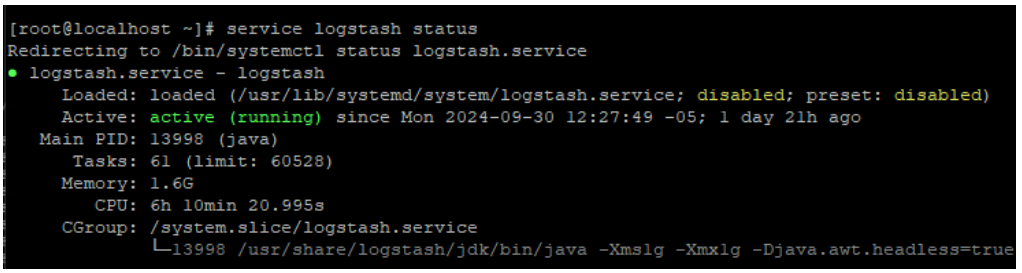
service kibana status



- **service logstash status**

Figura 44

service logstash status

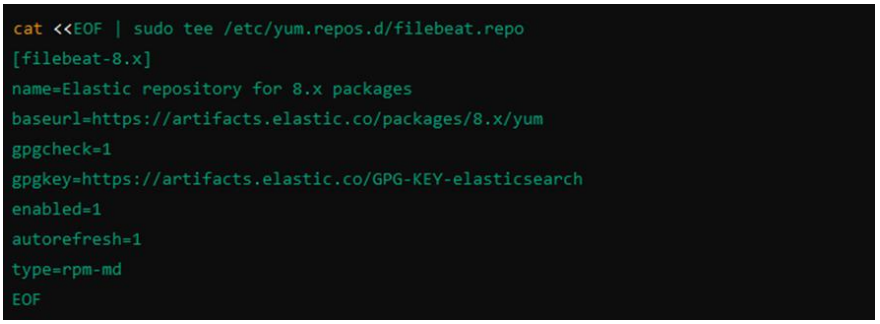


1.6.5 Instalación de filebeat.

Este proceso se realizó en la diferente estructura de los servidores de la universidad tomando en consideración la demanda de almacenamiento de log se escogió uno por estructura tales como: Httpd, tomcat, haproxy , mysql que nos servirán para realizar el monitoreo.

Figura 45

Repositorio filebeat



Paso 1 - Comandos filebeat.

- sudo yum install filebeat
- sudo filebeat modules enable system
- sudo systemctl start filebeat
- sudo systemctl enable filebeat

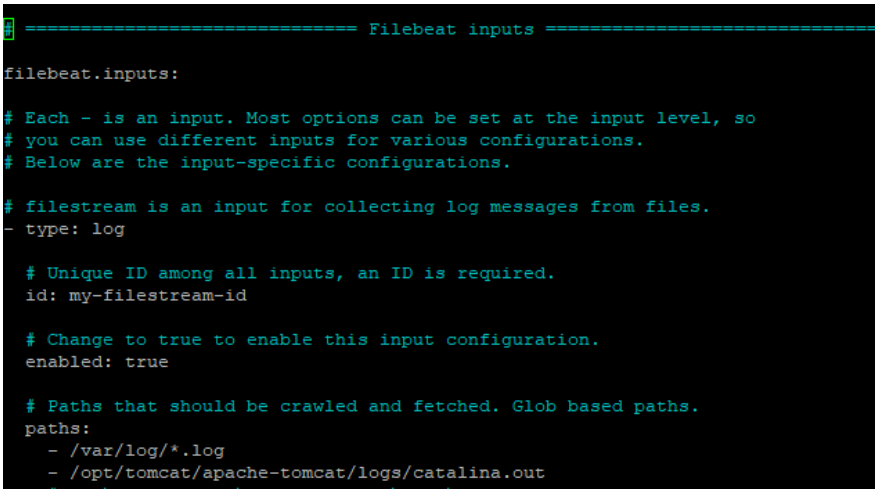
Paso 2 - Rutas de log para filebeat.

Para este proceso se prepararon los servidores en una ruta especifica dependiendo de cada servicio de tal modo que filebeat puedo obtener los registros de log y pueda enviárselo a logstash, además se agregaron alias para poder identificarlos y así la recolección de información sea más organizada.

- Ruta de log variada dependiendo de la configuración de los servicios que tengamos instalados en muestro servicios.

Figura 46

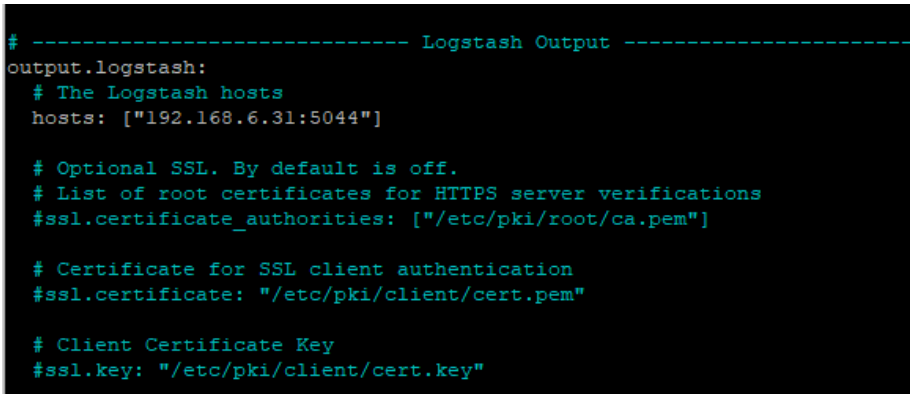
Rutas de log



- Conexión a logstash: Esta configuración permite que **Logstash** reciba datos de **Filebeat** en el puerto 5044 y luego los envíe a **Elasticsearch** en el puerto 9200

Figura 47

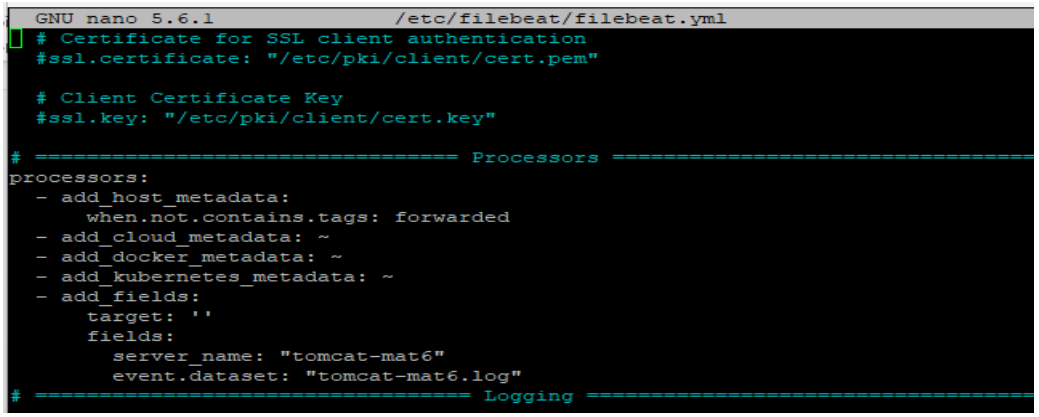
Conexión a logstash



- Los procesadores en **Filebeat** se usan para enriquecer, modificar o filtrar los eventos de log antes de enviarlos a su destino **Logstash**.

Figura 48

Procesadores Filebeat



1.7 Creación de Índex Para monitoreo de log en Kibana

1.7.2 Prueba de conexión a Elasticsearch

- Kibana nos ofrece mediante comandos hacer peticiones a Elasticsearch tales como "GET /

Figura 49

Repuesta Peticiones parte 1

El uso de herramientas de búsqueda estructurada, como Elasticsearch, refuerza la capacidad de monitorear y analizar eventos en tiempo real. Estas herramientas permiten realizar consultas específicas, como búsquedas por texto o patrones, lo que facilita la identificación de incidentes críticos y la correlación de eventos entre distintos sistemas.

1.7.3 Creación de índice

Mediante este esté Json creamos un índice para almacenaremos los logs envidos por las diferentes instancias de filebeat tal como se muestra en el anexo1.

Figura 50

Resumen json Upse-app

El uso de mapeos en Elasticsearch es una herramienta fundamental para estructurar y organizar datos provenientes de múltiples sistemas en un entorno centralizado. En este trabajo, el índice upse-app fue configurado para capturar eventos con un esquema

consistente, definiendo campos clave como @timestamp para consultas temporales y server_name para identificar el origen de los registros.

Debido a que solo tenemos un nodo el número de replicas deberá ser 0 para esto utilizamos este comando.

Figura 51

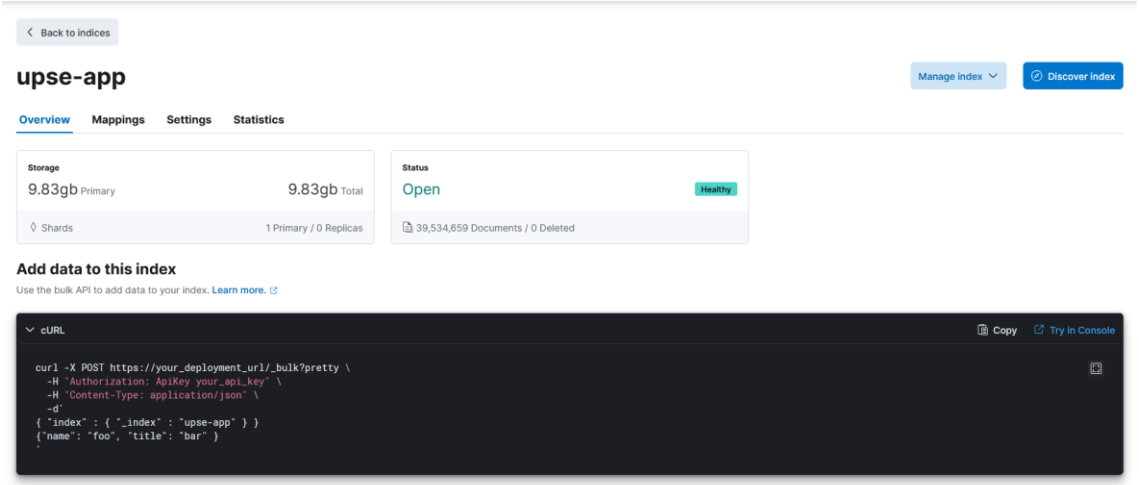
Numero replicas

```
PUT /upse-app/_settings
{
  "index": {
    "number_of_replicas": 0
  }
}
```

Verificamos que muestro índice este operativo

Figura 52

índice Open



1.7.4 Creación de data Views

Para poder analizar nuestra información creamos un nueva data view dentro de la sección de management, donde se escogerá el índice creado anteriormente.

Mostrándonos los key que nos servirán para el monitoreo de la información recolectada

Figura 53

Nueva data view

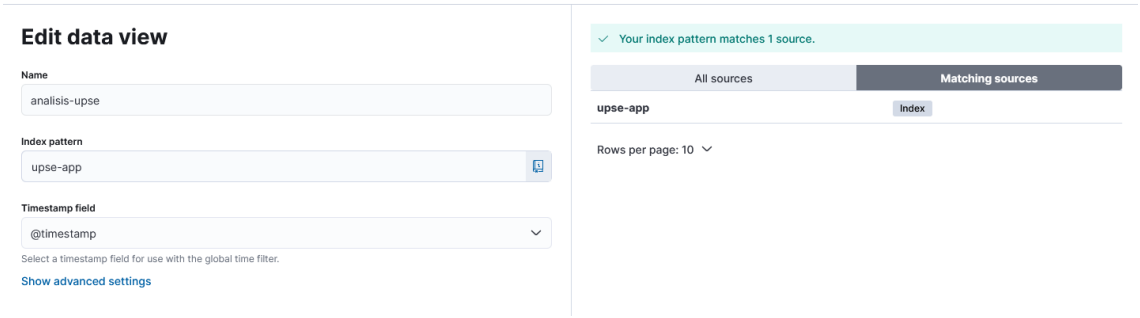
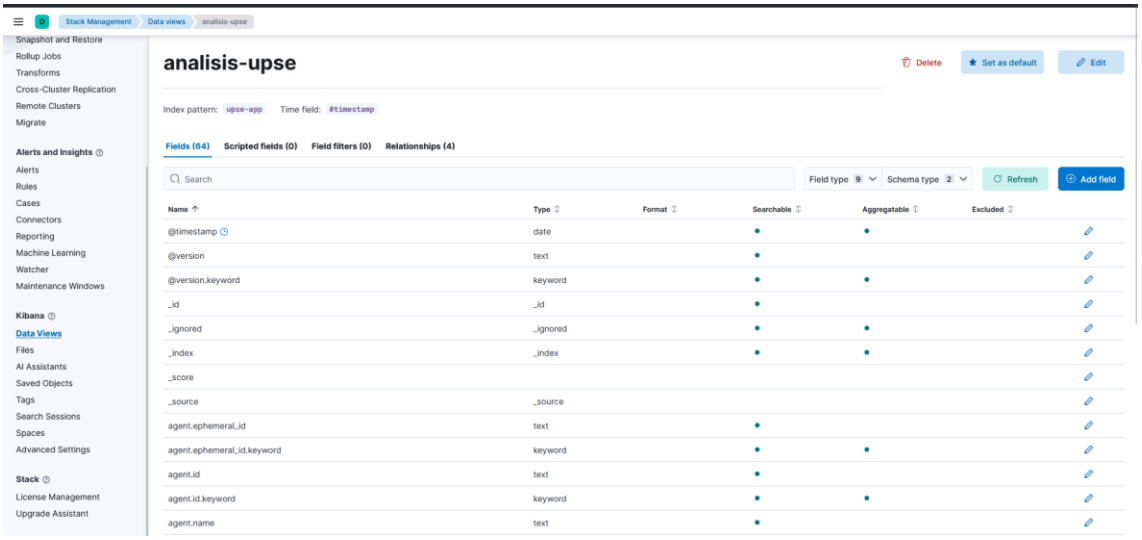


Figura 54

Claves



1.8 Resultados y Monitoreo de Grafana

1.8.2 Métricas Generales del Sistema

Estas métricas proporcionan una visión general del estado y la salud de la instancia:

mysql_up: Indica si MySQL está accesible y respondiendo (1 para arriba, 0 para abajo).

mysql_global_status_uptime_seconds: Tiempo total que MySQL ha estado en funcionamiento.

mysql_global_status_threads_connected: Número actual de conexiones activas.

mysql_global_status_threads_running: Número de hilos actualmente ejecutándose.

mysql_global_status_connections: Total de conexiones al servidor de MySQL desde su inicio.

node_cpu_seconds_total: Total de tiempo de CPU consumido desglosado por tipo (usuario, sistema, inactivo, etc.).

node_cpu_seconds_total{mode="user"}: Tiempo en modo usuario.

node_cpu_seconds_total{mode="system"}: Tiempo en modo sistema.

node_cpu_seconds_total{mode="idle"}: Tiempo en modo inactivo.

apache_scoreboard_Ready: Número de procesos que están listos para atender solicitudes.

apache_scoreboard_SendingReply: Número de procesos que están enviando una respuesta.

apache_scoreboard_Waiting: Número de procesos que están inactivos y esperando nuevas solicitudes.

apache_scoreboard_Busy: Número de procesos que están ocupados.

Métricas de Rendimiento de Consultas

Estas métricas nos permiten conocer el rendimiento de las consultas ejecutadas en la base de datos:

mysql_global_status_queries: Número total de consultas ejecutadas.

mysql_global_status_slow_queries: Número de consultas que han sido clasificadas como "lentas".

mysql_global_status_select_commands: Número de sentencias SELECT ejecutadas.

mysql_global_status_insert_commands: Número de sentencias INSERT ejecutadas.

mysql_global_status_update_commands: Número de sentencias UPDATE ejecutadas.

mysql_global_status_delete_commands: Número de sentencias DELETE ejecutadas.

apache_requests_total: Total de solicitudes atendidas por el servidor Apache.

apache_request_seconds: Tiempo total que ha tomado atender las solicitudes.

apache_connections_total: Total de conexiones al servidor Apache.

apache_bytes_sent_total: Total de bytes enviados a través del servidor.

Métricas de Memoria y Caché

Estas métricas ofrecen información sobre cómo se gestionan los recursos de memoria y la caché interna :

mysql_global_status_innodb_buffer_pool_size: Tamaño del pool de buffers de InnoDB (memoria usada para almacenar datos de tablas InnoDB).

mysql_global_status_innodb_buffer_pool_pages_data: Número de páginas de datos en el buffer pool.

mysql_global_status_innodb_buffer_pool_pages_dirty: Número de páginas sucias en el buffer pool (páginas modificadas pero aún no escritas al disco).

mysql_global_status_innodb_buffer_pool_pages_free: Número de páginas libres en el buffer pool.

mysql_global_status_innodb_buffer_pool_reads: Número de lecturas directamente desde el disco (cuando un dato no está en el buffer pool).

mysql_global_status_innodb_buffer_pool_read_requests: Número de lecturas desde el buffer pool (cuando un dato está en memoria).

node_memory_MemTotal_bytes: Total de memoria física disponible.

node_memory_MemAvailable_bytes: Memoria disponible para aplicaciones.

node_memory_MemFree_bytes: Memoria no utilizada.

node_memory_Buffers_bytes: Memoria utilizada como buffers.

node_memory_Cached_bytes: Memoria utilizada para caché.

node_memory_SwapTotal_bytes: Total de memoria swap.

node_memory_SwapFree_bytes: Memoria swap disponible

Métricas de Uso de Tablas y Almacenamiento

Estas métricas te permiten monitorear el uso de las tablas y la eficiencia del almacenamiento :

mysql_global_status_innodb_rows_read: Número de filas leídas por InnoDB.

mysql_global_status_innodb_rows_inserted: Número de filas insertadas en tablas InnoDB.

mysql_global_status_innodb_rows_updated: Número de filas actualizadas en tablas InnoDB.

mysql_global_status_innodb_rows_deleted: Número de filas eliminadas de tablas InnoDB.

mysql_global_status_innodb_data_reads: Número de operaciones de lectura desde el disco.

mysql_global_status_innodb_data_writes: Número de operaciones de escritura en el disco.

node_filesystem_size_bytes: Tamaño total del sistema de archivos.

node_filesystem_free_bytes: Espacio libre en el sistema de archivos.

node_filesystem_avail_bytes: Espacio disponible para usuarios no root.

node_disk_read_bytes_total: Total de bytes leídos desde el disco.

node_disk_written_bytes_total: Total de bytes escritos en el disco.

Métricas de Concurrencia y Bloqueos

Estas métricas ayudan a monitorear cómo las instancias gestionan la concurrencia y los bloqueos de las transacciones:

mysql_global_status_innodb_row_lock_waits: Número de veces que una transacción ha esperado por un bloqueo de fila.

mysql_global_status_innodb_row_lock_time_avg: Tiempo promedio que las transacciones pasan esperando por un bloqueo de fila.

mysql_global_status_table_locks_waited: Número de veces que se ha tenido que esperar por un bloqueo de tabla.

mysql_global_status_table_locks_immediate: Número de veces que se ha obtenido un bloqueo de tabla inmediatamente.

Replicación

_slave_status_seconds_behind_master: Cuántos segundos el servidor esclavo está detrás del maestro.

mysql_slave_status_slave_io_running: Estado del hilo de E/S en el servidor esclavo (1 para activo, 0 para inactivo).

mysql_slave_status_slave_sql_running: Estado del hilo SQL en el servidor esclavo.

Métricas de Red

Estas métricas proporcionan información sobre el tráfico de red en las instancias:

mysql_global_status_bytes_received: Total de bytes recibidos por MySQL.

mysql_global_status_bytes_sent: Total de bytes enviados por MySQL.

node_network_receive_bytes_total: Total de bytes recibidos en interfaces de red.

node_network_transmit_bytes_total: Total de bytes transmitidos en interfaces de red.

node_network_receive_packets_total: Total de paquetes recibidos.

node_network_transmit_packets_total: Total de paquetes transmitidos.

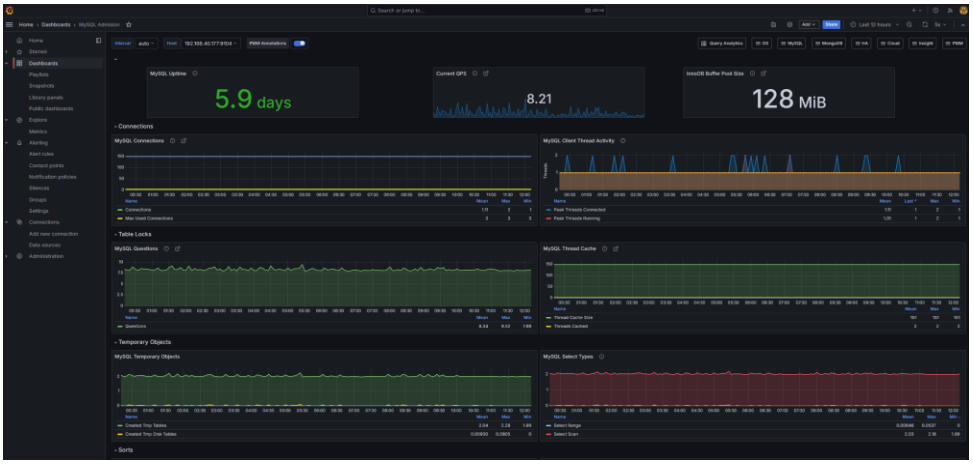
El sistema de monitoreo implementado en los servidores de la universidad se basa en **Prometheus** y **Grafana** para la recolección y visualización de métricas. Utilizando una variedad de exporters, como el **Apache Exporter**, **Node Exporter** y otros, se capturan métricas detalladas del rendimiento de diferentes servicios, como el servidor web Apache, bases de datos, y balanceadores de carga, entre otros. Estos datos se almacenan en **Prometheus**, permitiendo un análisis centralizado y detallado del estado de la infraestructura.

Grafana se encarga de visualizar estas métricas en paneles interactivos, lo que facilita la supervisión en tiempo real y la identificación de problemas potenciales. La integración de estas herramientas permite no solo almacenar el historial de métricas, sino también correlacionar datos de rendimiento con eventos de seguridad, lo que es crucial para cumplir con las normativas ISO 27000.

En resumen, la implementación de **Prometheus** y **Grafana** con diversos exporters ha permitido optimizar la administración de los servidores, ofreciendo a los administradores una visión clara y detallada del estado de los sistemas, lo que mejora la toma de decisiones y fortalece la seguridad operativa de la infraestructura de TI de la universidad.

Figura 55

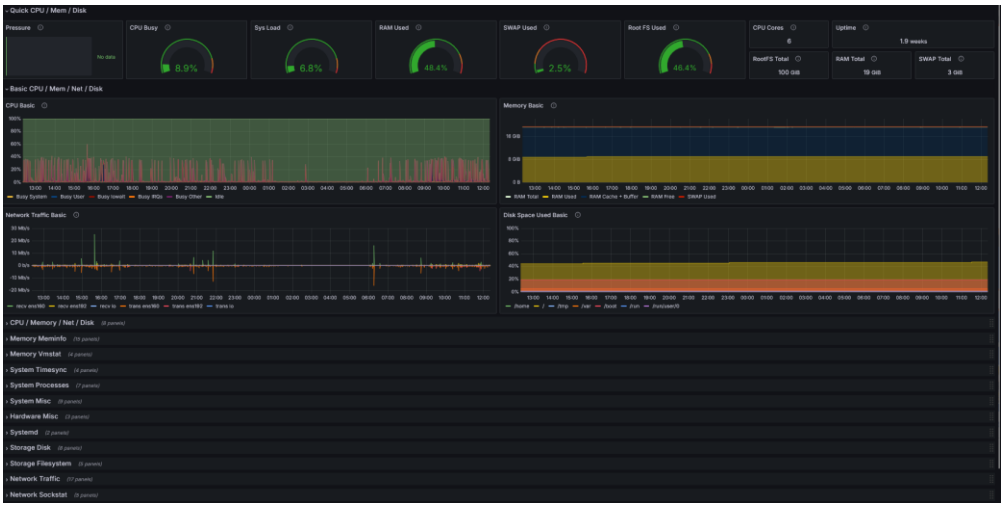
Dashboards Mysql



Esta figura presenta un dashboard diseñado para monitorear métricas clave del rendimiento y la disponibilidad de la base de datos MariaDB. Entre los indicadores destacados se encuentran el tiempo de actividad (5.9 días), el uso actual de CPU (8.21%), la memoria utilizada (128 MiB), las conexiones activas, y los objetos y threads gestionados por el sistema. Estas métricas son fundamentales para evaluar el estado de la base de datos y garantizar su operación continua, especialmente en contextos donde la alta disponibilidad y la confiabilidad son críticas.

Figura 56

Dashboards para los Tomcat



El monitoreo del servidor Tomcat mediante herramientas gráficas como Grafana proporciona una visión completa del rendimiento y el estado del sistema. El análisis de métricas como el uso de CPU, memoria, y transacciones por segundo es clave para garantizar la disponibilidad y la estabilidad de las aplicaciones. En este trabajo, el uso de dashboards como el mostrado ha permitido identificar patrones de uso, detectar posibles anomalías y optimizar la configuración del servidor, asegurando su alineación con los requerimientos establecidos en la ISO 27001, sección 12.4

Figura 57

Dashboards Apache

El monitoreo del servidor Apache mediante herramientas gráficas como Grafana proporciona una visión integral de su rendimiento y capacidad de gestión de solicitudes HTTP. El análisis de métricas clave, como el número total de solicitudes procesadas (391,772), las conexiones concurrentes, y el estado de las conexiones, permite identificar patrones de uso y optimizar el manejo de recursos. Estas métricas, combinadas con la estabilidad observada en el uso de CPU y disco, reflejan un sistema eficiente y estable, preparado para manejar cargas significativas.

Figura 58

Dashboards Resumen tomcat

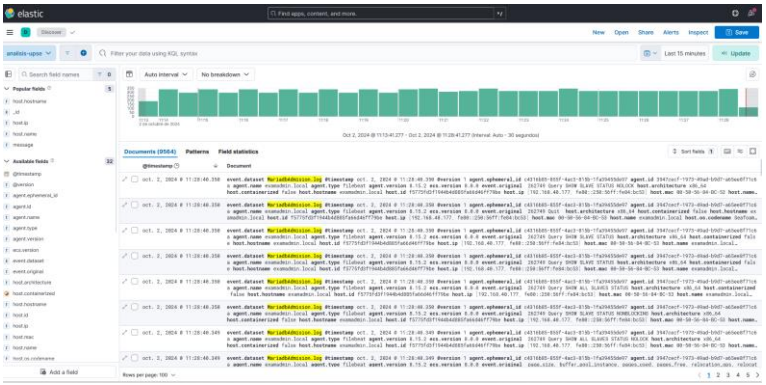
1.9 Resultados y Monitoreo Kibana.

1.9.2 Análisis de registros

Se diseño un dashboards interactivo utilizando consultas con sintaxis KQL en Kibana. Estas consultas permiten filtrar y analizar los registros generados por cada servidor, proporcionando una visión detallada de la actividad registrada en cada uno. Con estas consultas, se ha podido determinar la cantidad de registros generados por los diferentes servidores, segmentando los datos por períodos de tiempo, tipos de eventos y niveles de severidad. Esto ha facilitado la supervisión en tiempo real y ha permitido identificar patrones y posibles incidencias en los servicios, contribuyendo a una gestión más eficiente de la infraestructura.

Figura 59

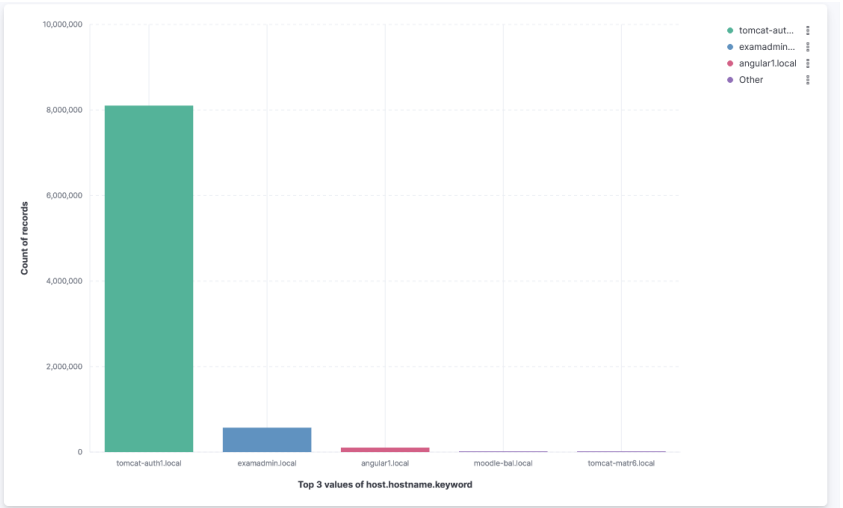
Registros de servidores



1.9.3 Análisis de Cantidad de Registros por servidor

Figura 60

Total de Registros



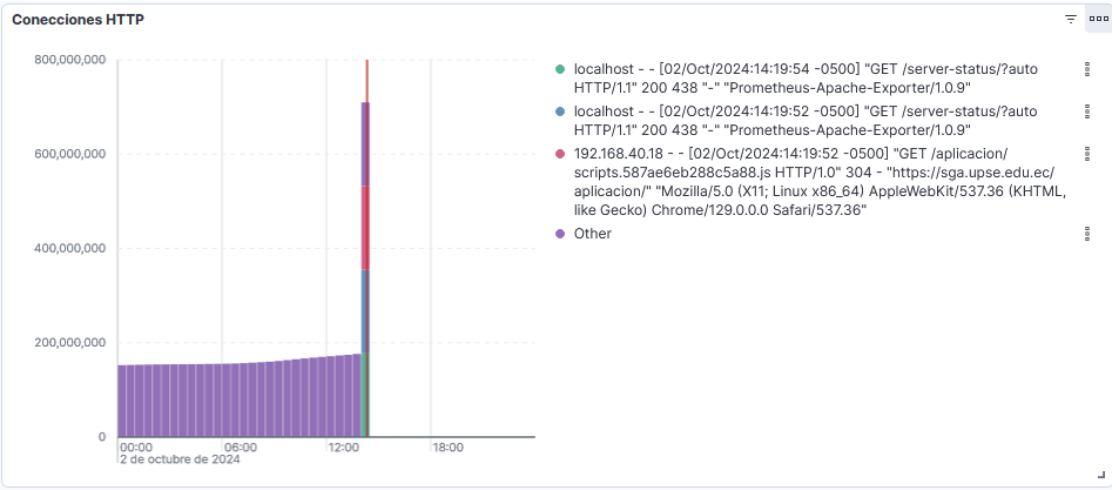
El análisis de registros mostrado en el gráfico revela que el servidor tomcat-auth1 es el que más registros genera, con más de 2.5 millones de entradas, lo cual sugiere una carga o actividad significativamente mayor en comparación con los demás servidores. Esto podría deberse a varios factores, como un volumen elevado de tráfico, más servicios ejecutándose, o posibles eventos de seguridad o errores que estén ocurriendo con mayor frecuencia.

Por otro lado, los servidores examadmin.local, angular1.local, y moodle-bal.local muestran una cantidad de registros mucho menor, lo que podría indicar que tienen menos carga o están siendo utilizados de manera más eficiente.

1.9.4 Análisis de conexiones HAProxy.

Figura 61

Análisis de conexiones Haproxy

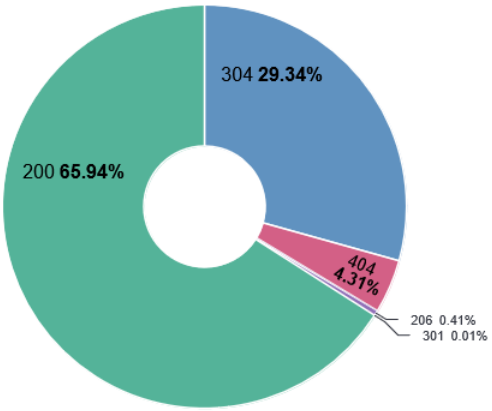


- El mayor número de conexiones ocurre después de las 12:00 horas, donde se observa un crecimiento acelerado en las solicitudes, con un pico cercano a los **800 millones de conexiones**.
- Las conexiones provienen de varias fuentes. Entre ellas:
  - ✓ **localhost** muestra solicitudes GET realizadas por el **Prometheus-Apache Exporter** para el endpoint /server-status/, que monitorea el estado del servidor Apache.
  - ✓ También hay solicitudes GET desde la dirección IP **192.168.x.x**, que accede a un script en la ruta /aplicacion/scripts, probablemente desde un navegador web con el agente de usuario "Mozilla/5.0 (X11; Linux x86_64)...".

1.9.5 Análisis peticiones http

Figura 62

Análisis peticiones http



La distribución de los códigos HTTP obtenida del análisis refleja que el servidor maneja las solicitudes de manera eficiente, con un **65.94%** de respuestas exitosas (200). Este resultado indica que la mayoría de los recursos solicitados por los usuarios están disponibles y se sirven correctamente. Sin embargo, un **4.31%** de los registros corresponden a errores 404, lo que implica solicitudes realizadas a recursos inexistentes o no localizables en el servidor. Esto puede ser un indicativo de enlaces rotos, recursos eliminados o mal configurados, o incluso intentos de acceso no autorizados. Para mitigar estos problemas, es esencial implementar redirecciones permanentes (301) o revisar los registros de acceso para identificar patrones de solicitudes fallidas y realizar las correcciones necesarias.

Además, un **29.34%** de las solicitudes generaron respuestas 304, lo que indica que el recurso solicitado no ha sido modificado desde la última vez que fue accedido, permitiendo al cliente reutilizar una copia almacenada en caché. Esto es un indicio positivo, ya que contribuye a reducir la carga en el servidor al evitar la retransmisión de contenido estático innecesario. Sin embargo, se recomienda evaluar las configuraciones de control de caché para maximizar aún más la eficiencia.

Por otro lado, los códigos restantes (206 y 301) constituyen menos del **1%** de las respuestas, lo que refleja escenarios puntuales de redirecciones o descargas parciales. Aunque representan un impacto mínimo en el comportamiento general del sistema, es importante monitorearlos para garantizar que no se conviertan en un problema recurrente en el futuro.

En resumen, este análisis proporciona información clave para identificar fortalezas y áreas de mejora en la administración de solicitudes del servidor HTTPD, y destaca la necesidad de un monitoreo continuo para garantizar la disponibilidad y el desempeño óptimo de los recursos

Análisis de anomalías

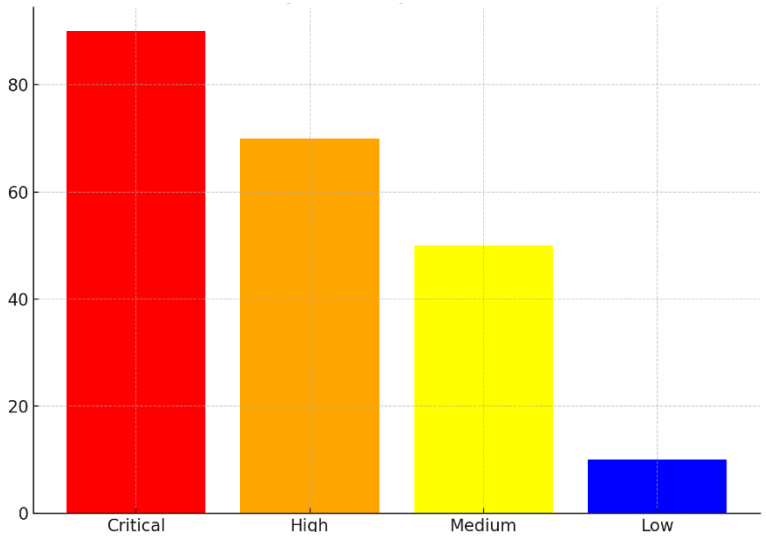
El análisis de anomalías en un sistema de monitoreo como Kibana consiste en identificar patrones fuera de lo común que pueden indicar problemas en el funcionamiento del sistema. El objetivo es detectar irregularidades en los datos que puedan representar riesgos de seguridad o afectaciones al rendimiento. A continuación, te doy un resumen de cómo se realiza este análisis

Las anomalías se clasifican según su impacto potencial en el sistema. Kibana usa una escala de colores para reflejar la gravedad:

- **Rojo (Crítico):** Representa una severidad **crítica**, Requiere atención inmediata, ya que representa un fallo grave.
- **Naranja (Alto):** Representa una severidad **alta**, Indica problemas serios que podrían convertirse en críticos.
- **Amarillo (Moderado):** Representa una severidad **alta**, Sugiere advertencias que deben ser monitoreadas, pero que no requieren intervención inmediata.
- **Azul (Bajo):** Representa una severidad **baja,** Anomalías leves que pueden no ser problemáticas, pero deben ser observadas.

Figura 63

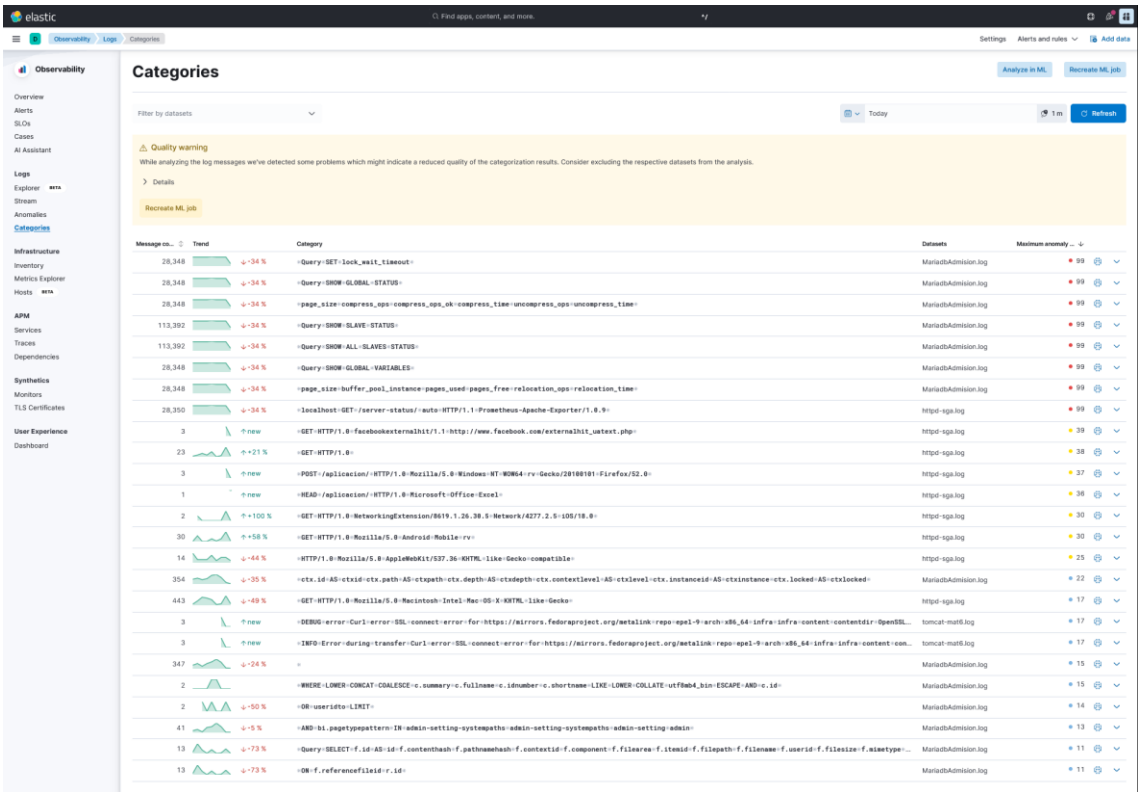
Nivel de anomalías



1.9.6 Análisis de anomalías por severidad

Figura 64

Anomalías por severidad



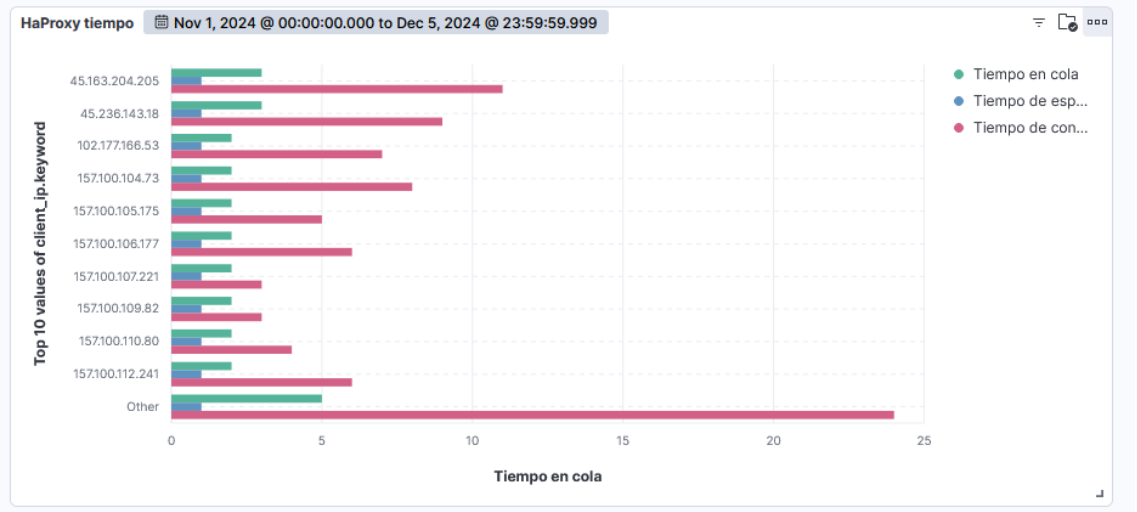
Durante el análisis de los datos de registro del archivo MariadbAdmision.log y httpd-sga.log, se identificaron varias anomalías significativas en diferentes categorías de mensajes. En particular, se observó una disminución del 34% en los registros de consultas SQL críticas como SHOW SLAVE STATUS y SET lock_wait_timeout. Estas anomalías, con una severidad crítica de 99, sugieren que el sistema está generando menos registros de lo esperado en estas categorías, lo que podría indicar problemas en la recolección de datos o cambios en la configuración de la base de datos.

Además, se detectaron anomalías moderadas en los registros HTTP (httpd-sga.log), con nuevas solicitudes desde diferentes fuentes, como navegadores y redes, mostrando incrementos de hasta un 100% en algunas categorías. Estas anomalías, con severidades que varían entre 25 y 38, deben ser monitoreadas, ya que podrían estar relacionadas con un aumento en el tráfico o comportamientos inesperados en el sistema.

- Haproxy

Figura 65

Haproxy Análisis



El análisis del balanceador de carga HAProxy permitió identificar patrones de comportamiento que impactan directamente en la disponibilidad y el rendimiento de los servicios balanceados. Entre los hallazgos más relevantes, se observó que ciertas IPs generan volúmenes significativos de solicitudes como se muestra en la figura . Este tráfico elevado podría indicar un uso descontrolado o, potencialmente, tráfico malicioso que debe ser analizado y mitigado mediante la implementación de límites de solicitudes por IP y reglas de seguridad.

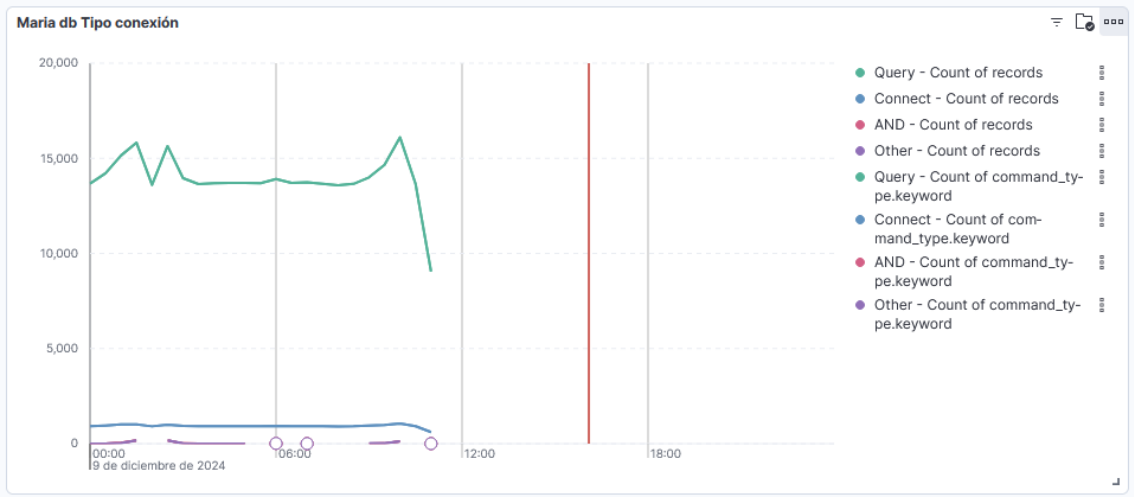
Asimismo, los tiempos en cola registrados para algunas IPs, como 45.163.204.205, alcanzaron niveles críticos cercanos a los 25 segundos, lo que afecta directamente la experiencia del usuario final. Estos tiempos elevados pueden estar asociados a cuellos de botella en el backend o configuraciones ineficientes en el balanceador, lo que resalta la necesidad de optimizar la infraestructura y los parámetros de HAProxy.

Por otro lado, la distribución de la carga entre los backends mostró un uso desproporcionado de los recursos, con el backend moodlepregrado gestionando la mayor parte del tráfico. Este desequilibrio podría ser mitigado mediante estrategias de balanceo más equitativas y la incorporación de un escalado dinámico para manejar picos de tráfico.

- MariaDB

Figura 66

Mariadb Query



El análisis de las métricas de MariaDB proporciona una visión detallada de la actividad en la base de datos y su impacto en el rendimiento del sistema:

1. **Tipos de conexión y operaciones:**
    - Las consultas (Query) son la operación predominante, con un volumen constante entre 10,000 y 15,000 registros durante la mayor parte del tiempo, y un descenso notable hacia el mediodía como se muestra en la Imagen().
    - Las conexiones nuevas (Connect) son significativamente menos frecuentes, lo que indica un manejo eficiente de las sesiones persistentes en el sistema.
2. **Operaciones por servidor:**
    - El volumen total de operaciones se mantiene estable durante gran parte del tiempo, con un incremento hacia las 12:00 horas, seguido de una caída significativa. Esto podría estar relacionado con eventos programados o fluctuaciones en la interacción de los usuarios.
3. **Consultas específicas:**
    - Las consultas comunes incluyen SHOW GLOBAL VARIABLES y SHOW STATUS, que reflejan solicitudes relacionadas con la configuración y el estado del servidor.

- Las consultas clasificadas como "Other" representan un alto porcentaje del total, lo que sugiere la presencia de operaciones personalizadas o específicas de las aplicaciones que requieren un análisis más detallado.

Todas las anomalías identificadas están relacionadas con la categoría FROM information_schema.innodb_cmp, lo que sugiere que el origen de estos picos está relacionado con operaciones de compresión de tablas en el motor InnoDB de MariaDB. Estos aumentos en las entradas de registros podrían estar vinculados a procesos intensivos de carga o consulta en la base de datos, lo cual deberá ser investigado más a fondo para determinar la causa raíz.

CONCLUSIONES

La implementación de estrategias para el monitoreo y registro de seguridad en los servidores de la Universidad Península de Santa Elena, siguiendo las normativas ISO 27001 y específicamente la sección 12.4 'Logging and Monitoring', ha demostrado ser eficaz para la detección de irregularidades críticas y la generación de evidencia clave para la gestión de la seguridad de la información. Durante el proyecto, las herramientas de observabilidad como Kibana facilitaron la recolección y análisis de registros provenientes de diversos componentes, incluyendo bases de datos (MariaDB), servidores web (HTTPD) y el balanceador de carga HAProxy, permitiendo identificar y evaluar patrones de comportamiento anómalos.

El análisis de los registros del servidor HTTPD reveló problemas relacionados con la latencia en la ingesta de datos, lo que resultó en un aumento considerable de solicitudes fallidas (404) y tiempos de respuesta superiores a los 400 ms en periodos críticos. Estas fallas evidenciaron la necesidad de optimizar los procesos de ingesta para manejar eficientemente las solicitudes fallidas y reducir la latencia, asegurando un registro en tiempo real que permita prevenir pérdidas críticas de información. Esto refuerza la importancia de alinear los procesos de monitoreo con los principios de gestión eficiente descritos en la normativa ISO 27001.

En el caso del servidor Tomcat, se identificaron picos de actividad intensiva que generaron saturación de hilos y tiempos de respuesta elevados en clases específicas como o.h.l.Loader y o-8080-exec-104. Estos resultados mostraron cómo las operaciones intensivas durante horarios pico pueden comprometer el rendimiento general del sistema. La detección temprana de estas anomalías destaca la relevancia de implementar estrategias proactivas, como la redistribución dinámica de cargas de trabajo y el ajuste de configuraciones del servidor, para garantizar la estabilidad del sistema y prevenir riesgos mayores.

Los registros de MariaDB también evidenciaron un alto nivel de interacción durante ciertos periodos, como los picos de consultas al mediodía. Aunque la gestión de conexiones fue eficiente, las consultas categorizadas como "Otros" representaron un alto porcentaje del total, lo que subraya la importancia de un monitoreo más detallado para identificar y optimizar estas operaciones. Esto es fundamental para evitar posibles impactos en el rendimiento de la base de datos y asegurar la continuidad operativa.

El análisis del balanceador de carga HAProxy destacó la necesidad de optimizar la distribución de solicitudes y recursos. Los resultados indicaron una carga desproporcionada generada por ciertas direcciones IP, así como tiempos elevados en cola y una distribución desigual entre los backends. Este comportamiento resalta la importancia de implementar límites por IP, mejorar las configuraciones del balanceador y escalar dinámicamente los recursos en función de la demanda, asegurando así la disponibilidad del sistema y una gestión más eficiente de los recursos.

Los resultados de la encuesta **Anexo 7** reflejan que la implementación del sistema de monitoreo y centralización de logs ha tenido un impacto positivo en la gestión de la seguridad de los servidores. La mayoría de los encuestados (71.4%) considera que el sistema facilita la gestión de eventos de seguridad gracias a la centralización de los logs y lo perciben como una herramienta intuitiva y útil para sus tareas diarias. Además, el 85.7% afirmó que las herramientas implementadas han contribuido a reducir el tiempo de respuesta ante incidentes, lo que respalda la efectividad del sistema en situaciones críticas.

RECOMENDACIONES

Se recomienda continuar fortaleciendo los procesos de monitoreo mediante la optimización de la configuración de las herramientas utilizadas, como Kibana, Prometheus y Grafana, para garantizar la recolección y análisis en tiempo real de eventos críticos en los servidores. Esto permitirá una mayor eficiencia en la detección de anomalías y en la respuesta a incidentes.

Fortalecimiento de las políticas de seguridad de acceso: Las anomalías detectadas en las solicitudes HTTP, que muestran incrementos en peticiones provenientes de fuentes externas, subrayan la necesidad de reforzar los controles de acceso. Es fundamental implementar políticas de seguridad más estrictas para prevenir accesos no autorizados o tráfico no deseado.

Mejora en el monitoreo y la detección de anomalías: Es recomendable ajustar los algoritmos de aprendizaje automático utilizados en el sistema de monitoreo para aumentar la precisión en la detección de anomalías. Además, resulta esencial conectar estas herramientas de monitoreo con sistemas de respuesta a incidentes para actuar rápidamente en caso de detectar problemas críticos.

Se sugiere realizar un monitoreo continuo de la carga y el rendimiento del servidor Tomcat, priorizando la redistribución de operaciones intensivas en horarios menos concurridos. Asimismo, es fundamental optimizar la configuración de los hilos y ajustar los parámetros de ejecución para minimizar la saturación y los tiempos de respuesta elevados observados.

REFERENCIAS

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, *89*(89). https://doi.org/10.37960/revista.v25i89.31534

Al-Azzawi, A., & Lencse, G. (2023). Analysis of the Security Challenges Facing the DS-Lite IPv6 Transition Technology. *Electronics (Switzerland)*, *12*(10). https://doi.org/10.3390/electronics12102335

Arévalo Cordovilla, F., Arévalo Cordovilla, B., Castillo Salvatierra, L., & Cortez Lara, A. (2021). Gestión de Seguridad en Virtualización de Servidores. *Ecuadorian Science Journal*, *5*(4), 150-163. https://doi.org/10.46480/ESJ.5.4.178

Balseca-Chávez, F., Colina-Vargas, A. M., & Espinoza-Mina, M. A. (2021). Identificación de amenazas informáticas aplicando arquitecturas de Big Data. *INNOVA Research Journal*, *6*(3.2). https://doi.org/10.33890/innova.v6.n3.2.2021.1860

Becerra, F. Á., Adrián, L., & Orbe, M. A. (2019). *Sistema de gestión de la calidad para el proceso de investigación: Universidad de Otavalo, Ecuador*. 1-32. https://doi.org/10.15517/aie.v19i1.35235

Carrión, B. (2015). *Diseño e implementación de una solución de gestión centralizada de logs de aplicaciones, sistemas y dispositivos basada en logstash*.

Castillo Enríquez, Á. S., Hidalgo Guijarro, J. V., & Guano Cárdenas, C. A. (2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi, 2021. *SATHIRI*, *17*(2). https://doi.org/10.32645/13906925.1138

Castillo, Y. E. (2021). Arquitectura para la detección violaciones a políticas de seguridad Architecture for the detection of security policy violations. *Revista Cubana de Ciencias Informáticas*, *15*. http://rcci.uci.cuPág.265-280Editorial"EdicionesFuturo"https://orcid.org/0000-0001-6163-2819MónicaPeñaCasanova1https://orcid.org/0000-0003-2500-4510BárbaraLaborídelaNuez1https://orcid.org/0000-0001-8114-0969

Cedeño Villacís, R. P. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista Tecnológica Ciencia y Educación Edwards Deming*. https://doi.org/10.37957/rfd.v6i1.88

Chifla-Villón, M., Puma- Aucapiña, L., & Villacís-Real, K. (2020). Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del Ecuador. *CIENCIA UNEMI*, *13*(34). https://doi.org/10.29076/issn.2528-7737vol13iss34.2020pp127-143p

Coronel Suárez, I., & Quirumbay Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*, *9*(2), 97-108. https://doi.org/10.26423/RCTU.V9I2.672

Damian Vasquez, J. (2023). *ISO/IEC 27000*. https://doi.org/10.46363

Derenzin-Martinez, F. (2024). ¿Están los institutos universitarios en Ecuador preparados para los ciberataques? *593 Digital Publisher CEIT*, *9*(6), 1220-1232. https://doi.org/10.33386/593dp.2024.6.2864

Estructura orgánico funcional de la Universidad Estatal Península de Santa Elena. (2014).

Fernández, G. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.* Universidad de las Fuerza Armadas ESPE.

García Hidalgo, T., & Moneo, J. (2023). *Implementación de Security Data Lake con Splunk*. Universitat Obertade Catalunya.

González de Juana, O. (2021). *Generación de ciberinteligencia con Splunk*. https://riunet.upv.es:443/handle/10251/174443

González, H., & Montesino, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades. *Revista Cubana de Ciencias Informáticas*, *12*(4).

GOV.UK. (2023). *Encuesta sobre violaciones de la ciberseguridad 2023: anexo sobre instituciones educativas - GOV.UK*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

Guerra, E., Neira, H., Díaz, J. L., Patiño, J., Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Development of an information security management system based on analysis methodology and risk identification in university libraries. *Información tecnológica*, *32*(5), 145-156. https://doi.org/10.4067/S0718-07642021000500145

Isabel Ladino, M. A., Andrea Villa, P. S., & María López, A. E. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et Technica Año XVII*, *47*. www.iso27000.es

Kaspersky. (2024). *América Latina registra un aumento del 2.8% en los intentos de ataque de ransomware*. https://latam.kaspersky.com/about/press-releases/america-latina-registra-un-aumento-del-28-en-los-intentos-de-ataque-de-ransomware

Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., León-Cuervo, C. A., Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Análisis de ataques informáticos mediante Honeypots en la Universidad Distrital Francisco José de Caldas. *Ingeniería y competitividad*, *22*(2), 1-13. https://doi.org/10.25100/IYC.V22I2.8483

López, O., & García, A. (2008). *Propuesta para la recolección centralizada de Logs*. Universidad de las Ciencias Informáticas.

Marmolejo Corona, I. V., Serrano Manzano, G. A., Bautista Aguilar, F. A., & Santiago Gonzalez, Y. F. (2023). Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación. *XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan*, *11*(22). https://doi.org/10.29057/xikua.v11i22.10802

Pico-Verdezoto, D. V., Bohorquez-Rizzo, C. E., Delgado-Jiménez, S. A., & Katherine-Tatiana, T. T. (2023). Cibercrimen y ciberseguridad: protegiendo el futuro digital, Babahoyo, Ecuador. *IUSTITIA SOCIALIS*, *8*(3). https://doi.org/10.35381/racji.v8i3.3116

Pilamunga, J. (2023). Estrategias de auditoría de seguridad informática en cloud. *Technology Rain Journal*, *2*(2). https://doi.org/10.55204/trj.v2i2.e16

Planes Martínez, A. (2022). *Sensores inalámbricos en entornos industriales mediante SDN*. https://riunet.upv.es:443/handle/10251/187865

Pons Moro, D. (2021). *Diseño, desarrollo e implementación de un protocolo automático para la gestión inteligente de tareas en una infraestructura de inteligencia artificial*. https://riunet.upv.es:443/handle/10251/174400

Porven Rubier, J., Montesino Perurena, R., & Autor, *. (2015). Framework for centralized security logs management using open source tools. *Revista Cubana de Ciencias Informáticas*, *9*(3). http://rcci.uci.cuPág.18-32

¿Qué es la norma ISO 27001 y para qué sirve? | GSS. (s. f.). Recuperado 22 de julio de 2024, de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Rahman, D., Amnur, H., & Rahmayuni, I. (2020). Monitoring Server dengan Prometheus dan Grafana serta Notifikasi Telegram. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(4). https://doi.org/10.30630/jitsi.1.4.19

Ramos Mamami, R. G., Cahuaya Ancco, R., & Llanqui Argollo, R. R. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Innovación y Software*, *4*(1). https://doi.org/10.48168/innosoft.s11.a57

Reyes, W., Alvarez, A., & Barrera, J. (2023). *Estrategia de detección temprana de eventos de seguridad utilizando un SIEM open source para los servicios digitales de banca web*.

Ruiz, A., & Rodrigo, P. (2019). *CENTRALIZACIÓN Y ANÁLISIS DE EVENTOS DE SEGURIDAD CON GRAYLOG*.

Sanchez-Garcia, I., Rea-Guaman, A., & San Feliu, T. (2024). *Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación*. *53*. https://doi.org/10.17013/risti.53.69-87

Santacruz Fernández, A. (2013). *Plan de seguridad informática y los riesgos operativos en el Municipio Descentralizado de Quevedo, Provincia de los Ríos*. https://dspace.uniandes.edu.ec/handle/123456789/3037

Sayago-Heredia, J. (2022). Ciberseguridad en Ecuador y Latinoamérica. *Killkana Técnica*, *5*(1). https://doi.org/10.26871/killkanatecnica.v5i1.957

Suárez, A. (2022). *Monitorización y análisis de logs y métricas en tiempo real utilizando Elk Stack, Metricbeat y Filebeat*.

Sulay, L., Baca, R., Francisco, C., Puente De La Vega, C., Corredor, C. M., Alberto, M., Diaz, A., & Corredor, M. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana Application of ISO 27001 and its influence on the information security of a Peruvian private company*. *8*, 786. https://doi.org/10.20511/pyr2020.v8n3.786

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Las normas de reciente publicación de ISO incorporan dos elementos comunes. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73-88. https://doi.org/10.17013/risti.22.73

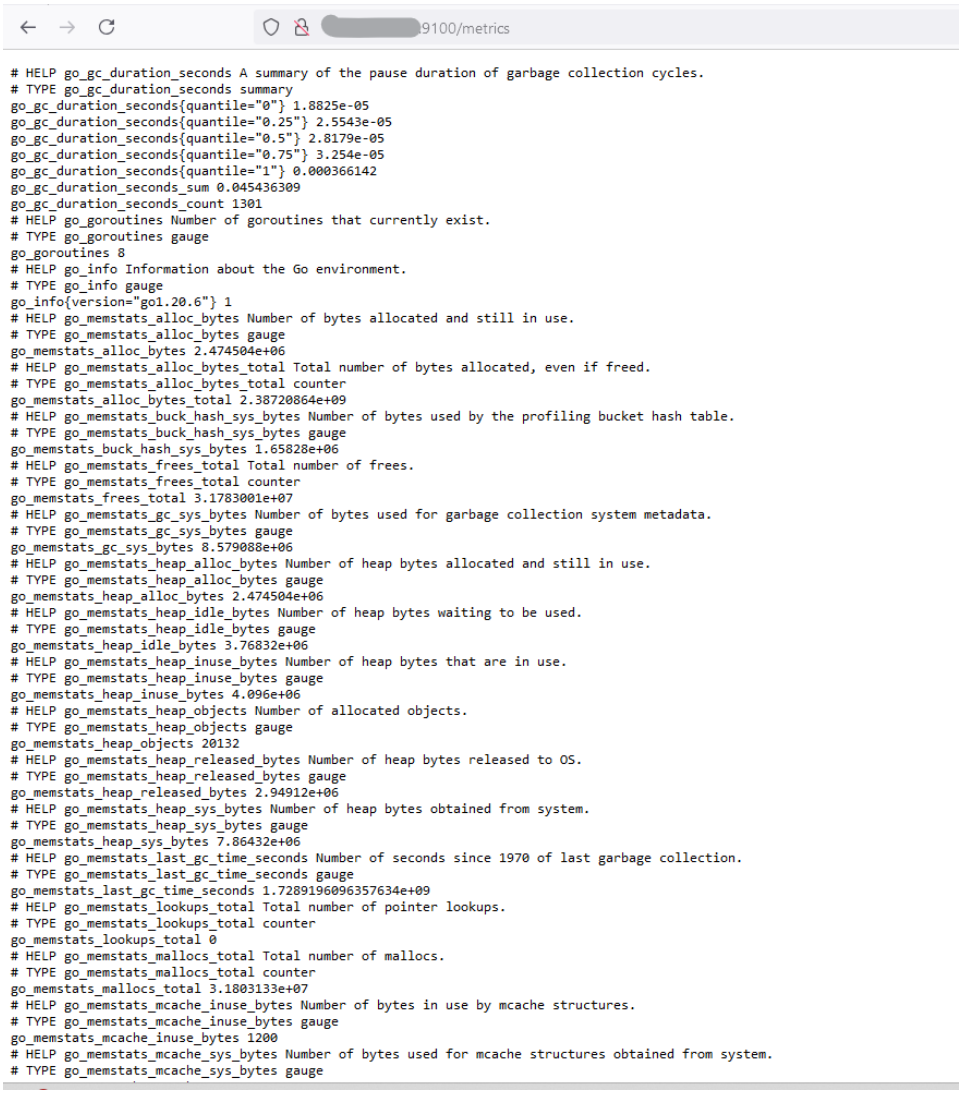
Yulvianda, R., & Ismail, M. (2023). Desain dan Implementasi Sistem Monitoring Sumber Daya Server Menggunakan Zabbix dan Grafana. *Jurnal Informatika Dan Rekayasa Komputer(JAKAKOM)*, *3*(1). https://doi.org/10.33998/jakakom.2023.3.1.712

ANEXOS.

Anexo 1 Exporter

A través de las capturas obtenidas de diferentes servidores y servicios, se evidencia la implementación de un monitoreo integral y centralizado que abarca componentes clave como Apache, Tomcat, MariaDB, y aplicaciones. Este enfoque asegura la recolección de métricas relevantes que permiten evaluar el estado y el rendimiento del sistema, identificar anomalías, y garantizar la continuidad operativa.

Figura 67 *Exporter servidor Tomcat 1*



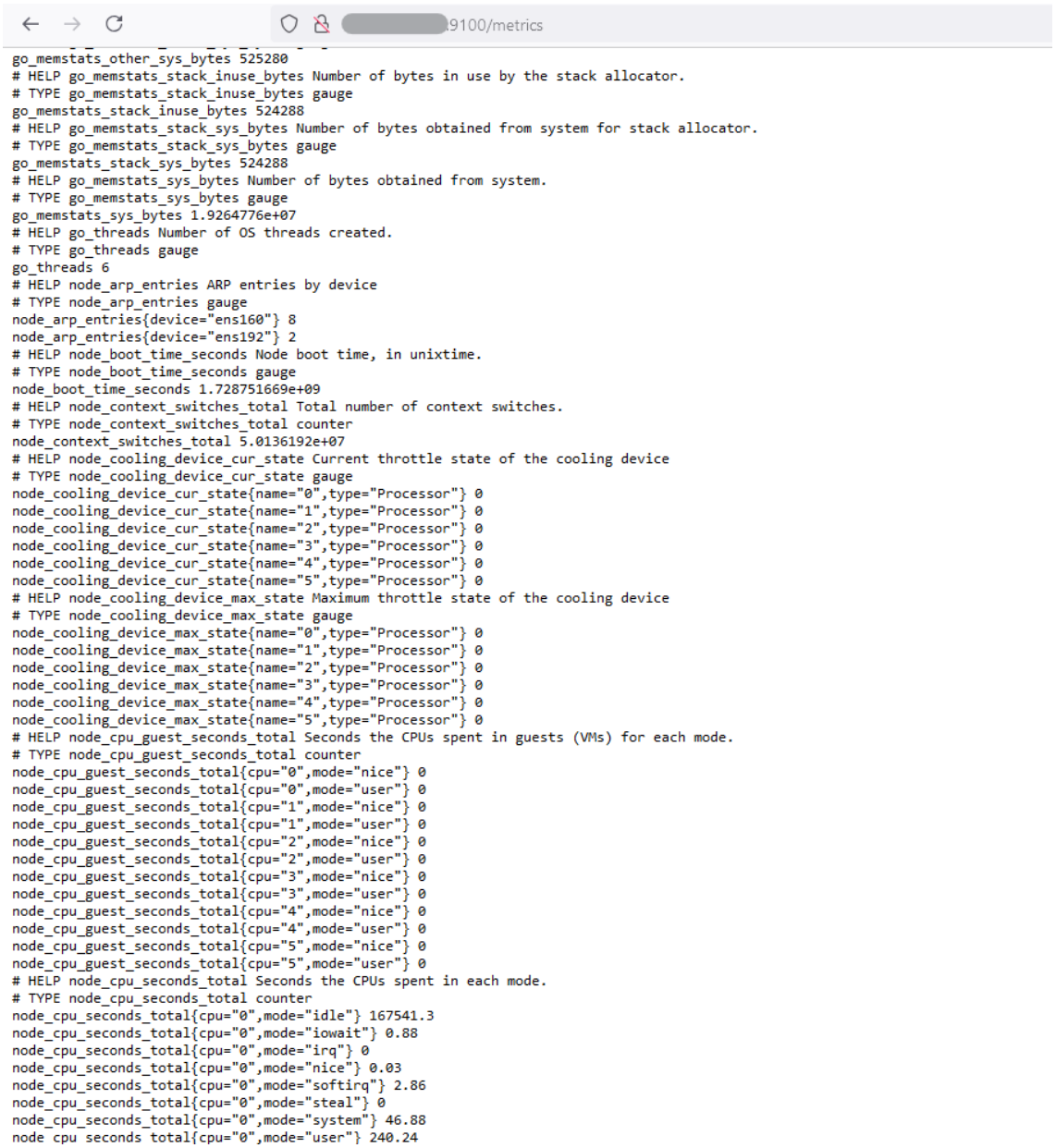


Figura 68 *Exporter servidor Tomcat 2*

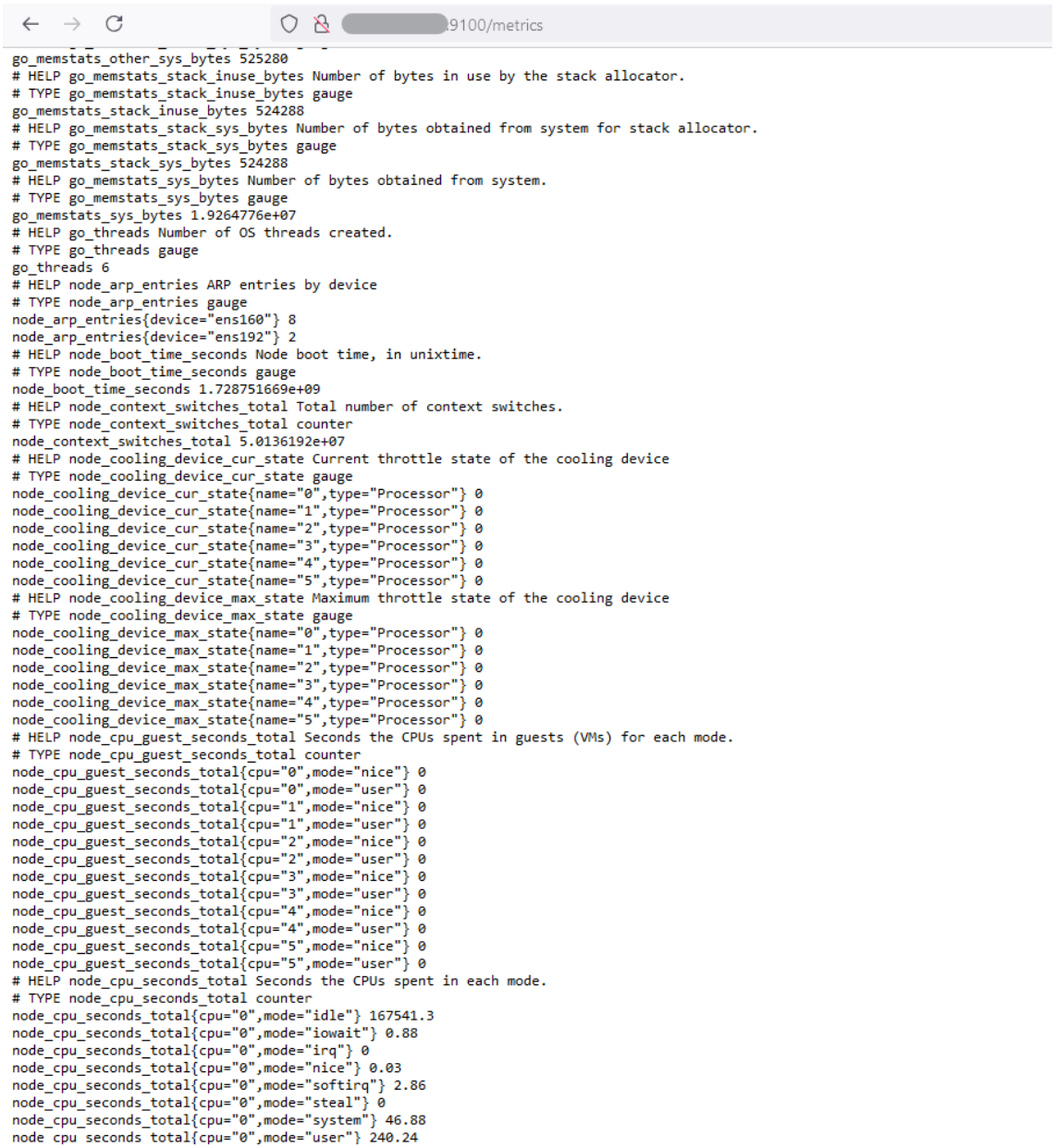


Figura 69 *Exporter servidor Tomcat 3*

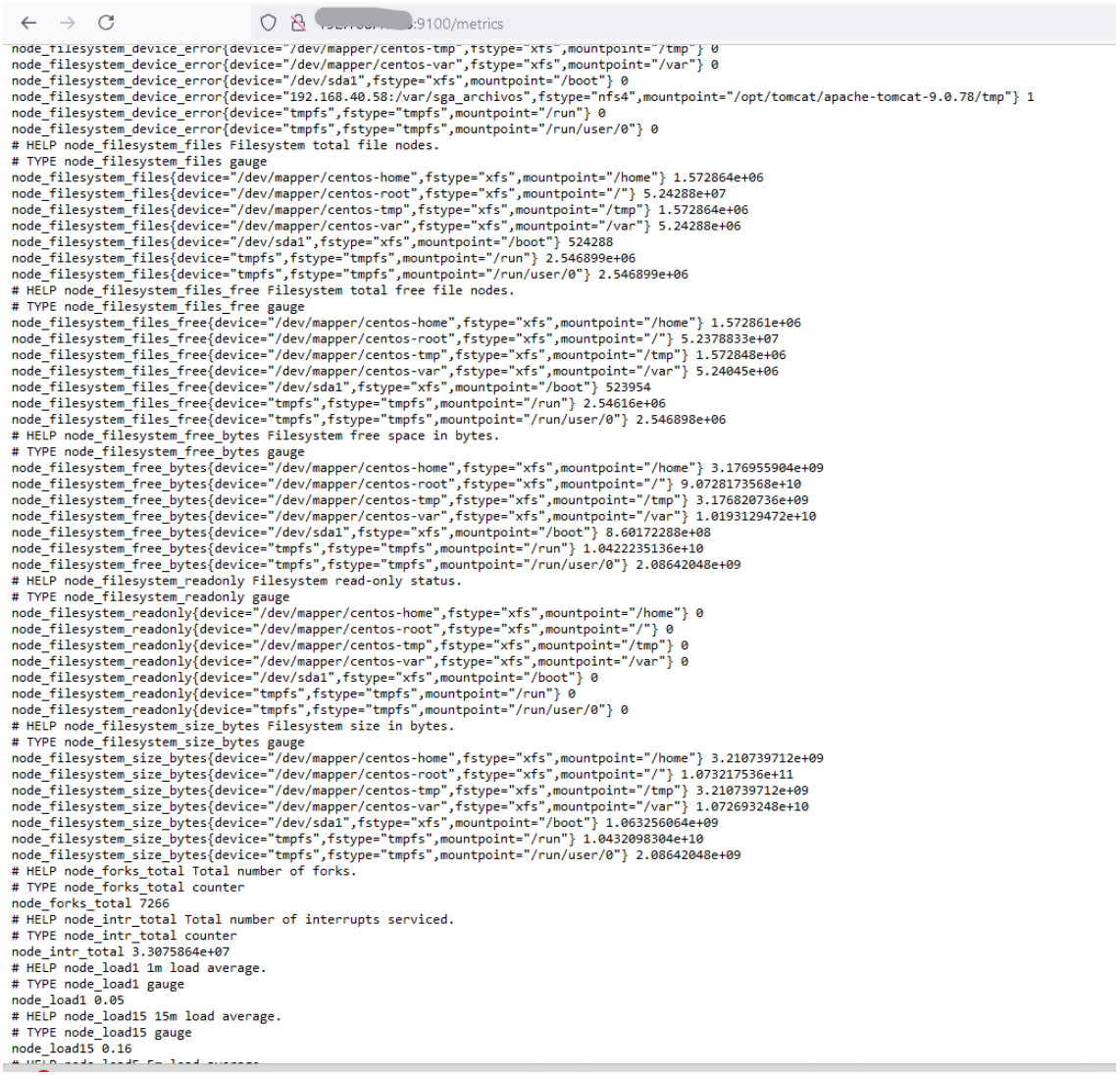


Figura 70 *Exporter servidor Tomcat 4*

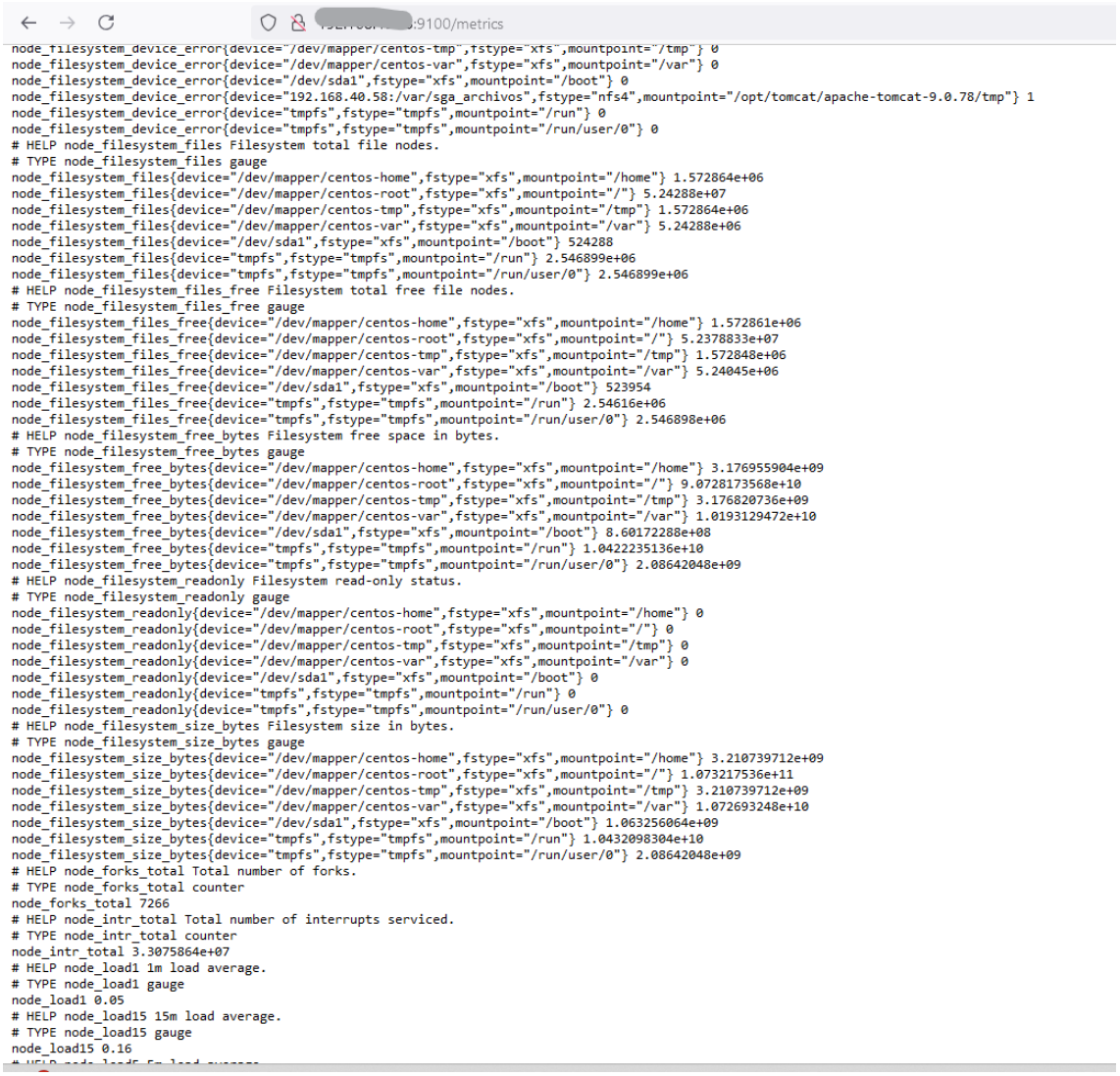


Figura 71 *Mysql Exporter*

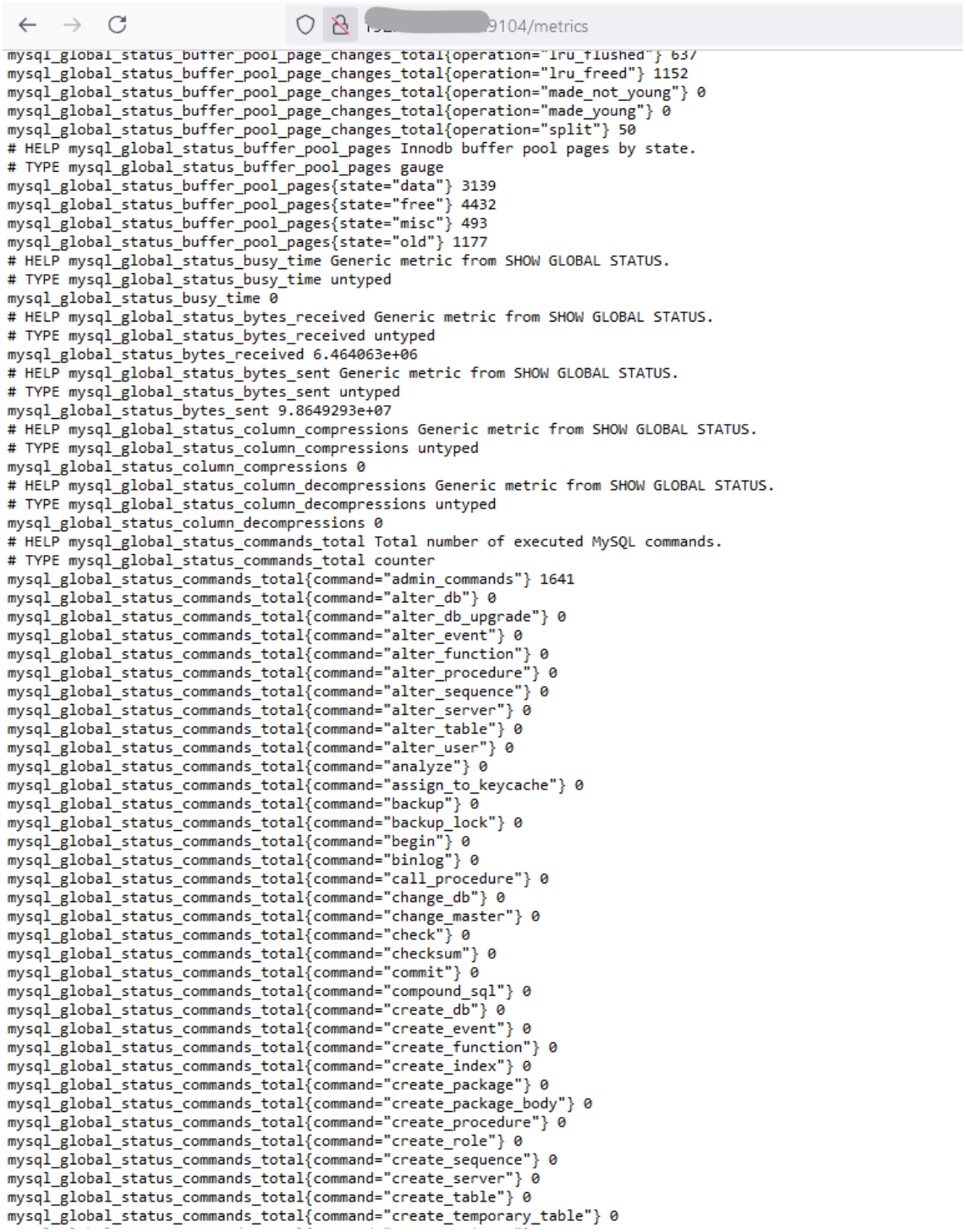


Figura 72 *Apache Exporter*

Figura 73 *Ha Proxy*

Anexo 2 *Dashboard Tomcat*

Figura 74 *Monitoreo cpu Tomcat*

Figura 75 *Monitoreo memoria ram*

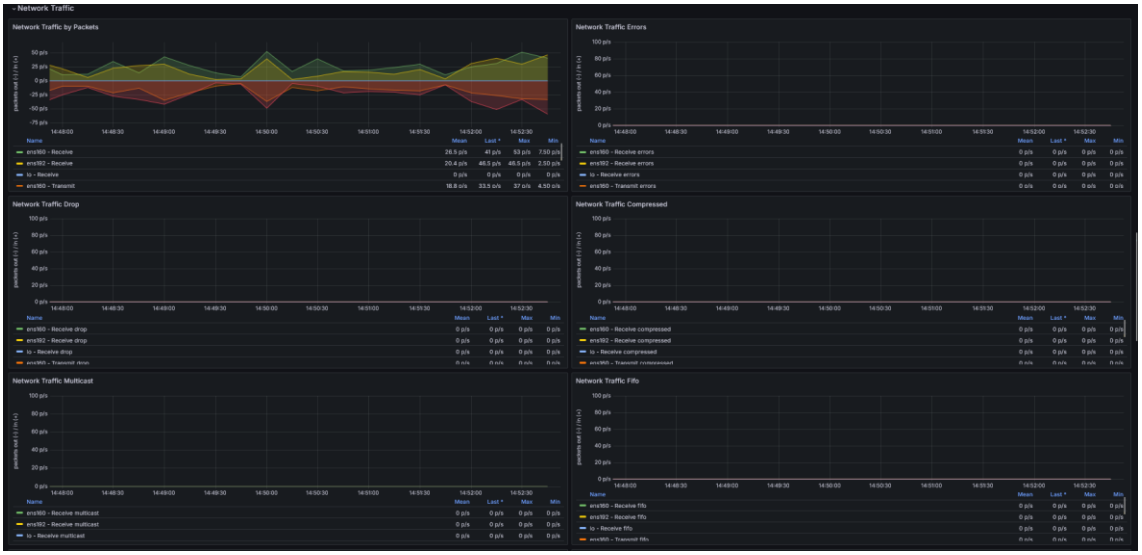


Figura 76 *Monitoreo de red*

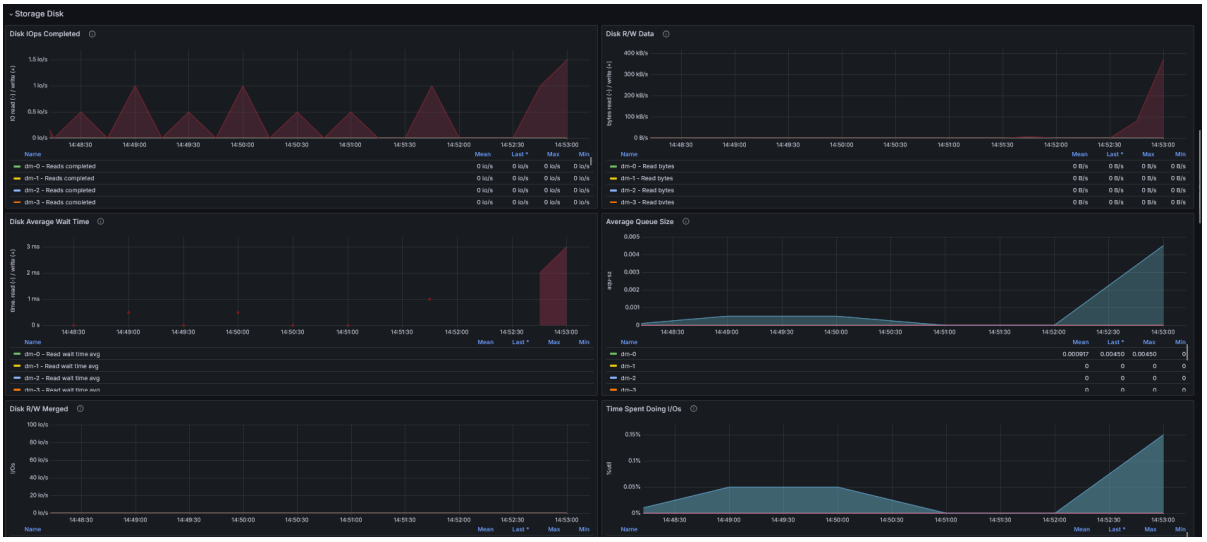


Figura 77 *Monitoreo disco*

Anexo 3 *Dashboard Apache*

Figura 78 *Dashboards apache*

Anexo 4 *Dashboard Mysql*

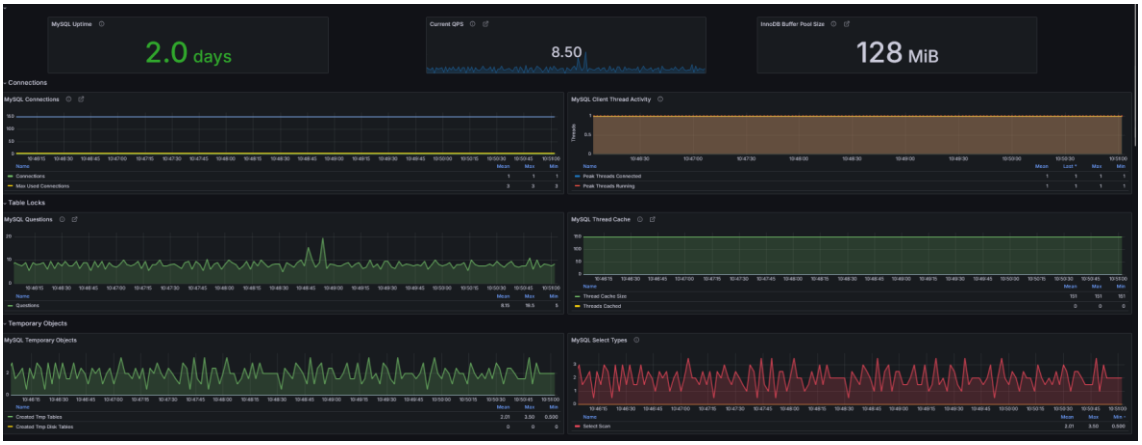


Figura 79 *Dashboards mysql parte 1*

Figura 80 *Dashboards mysql parte 2*

Figura 81 *Dashboards mysql parte 3*

Anexo 5 *Elasticsearch*

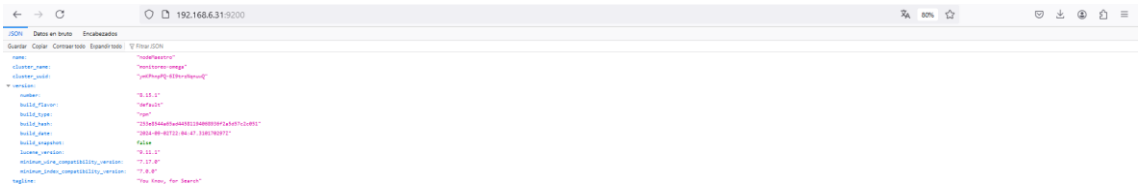


Figura 82 *Funcionamiento del nodo*

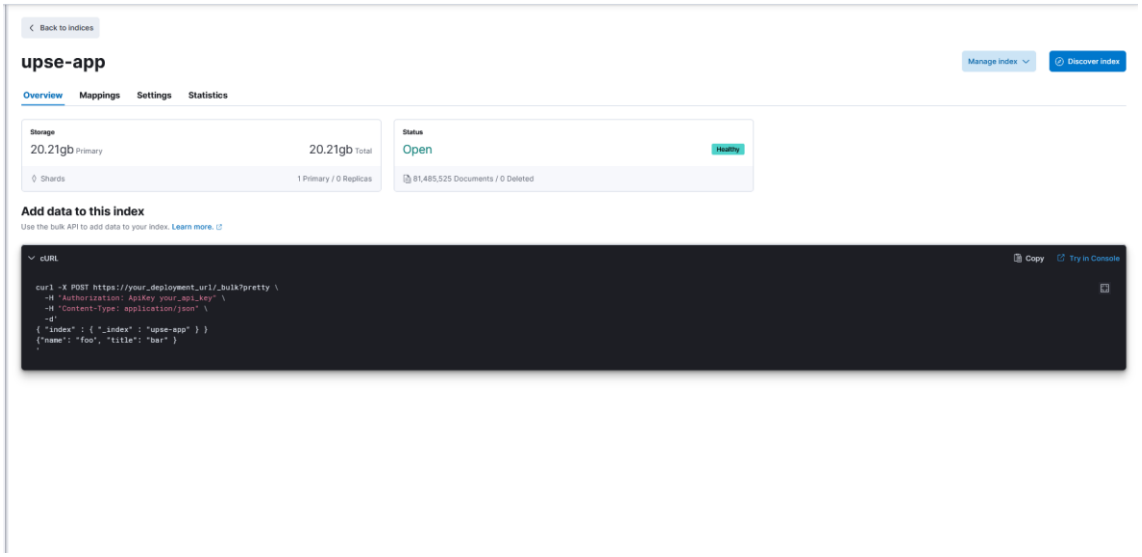


Figura 83 *Cantidad de log Registrados*

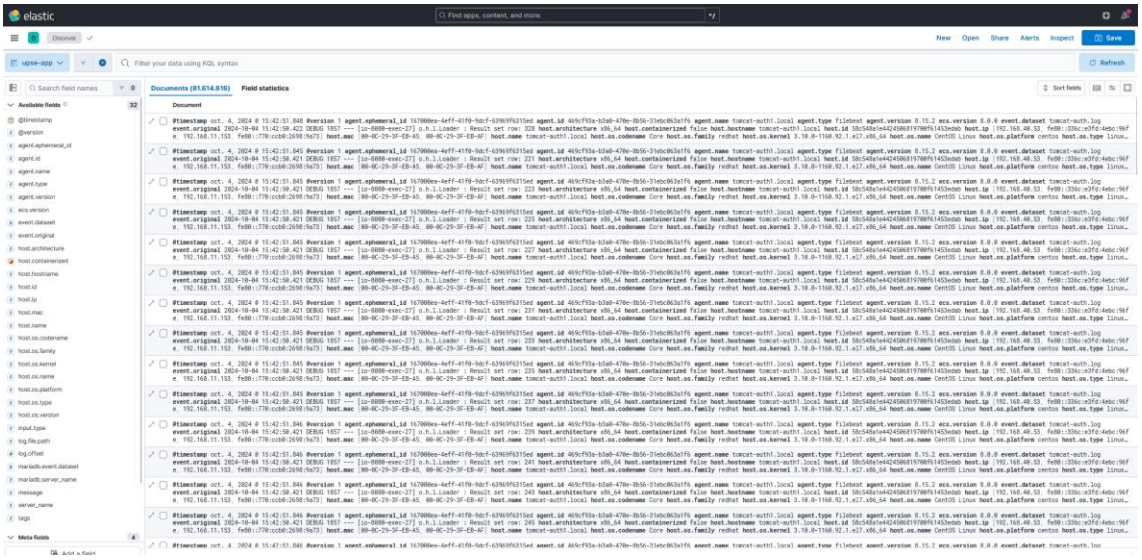


Figura 84 *Inspección de log*

Figura 85 *Latencia HTTP*

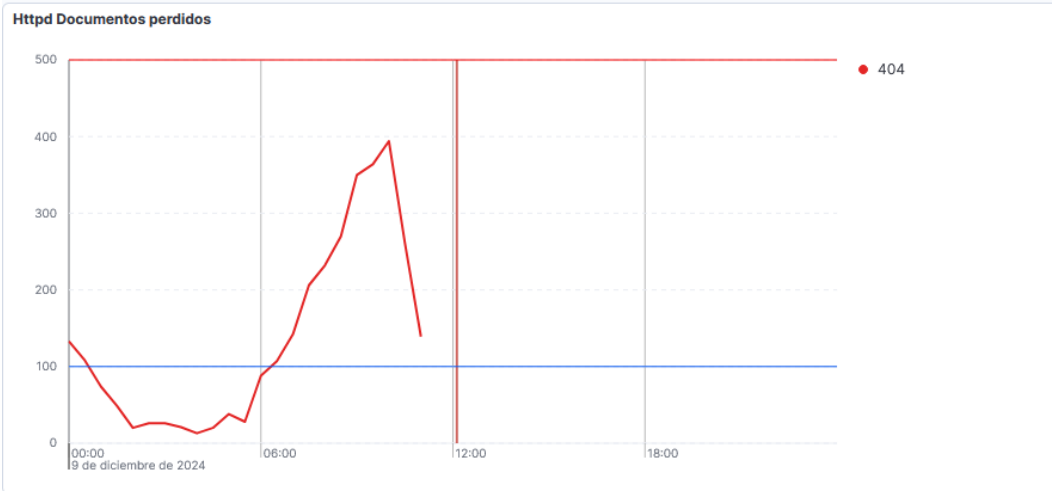


Figura 86 *Perdida de documentos HTTP*

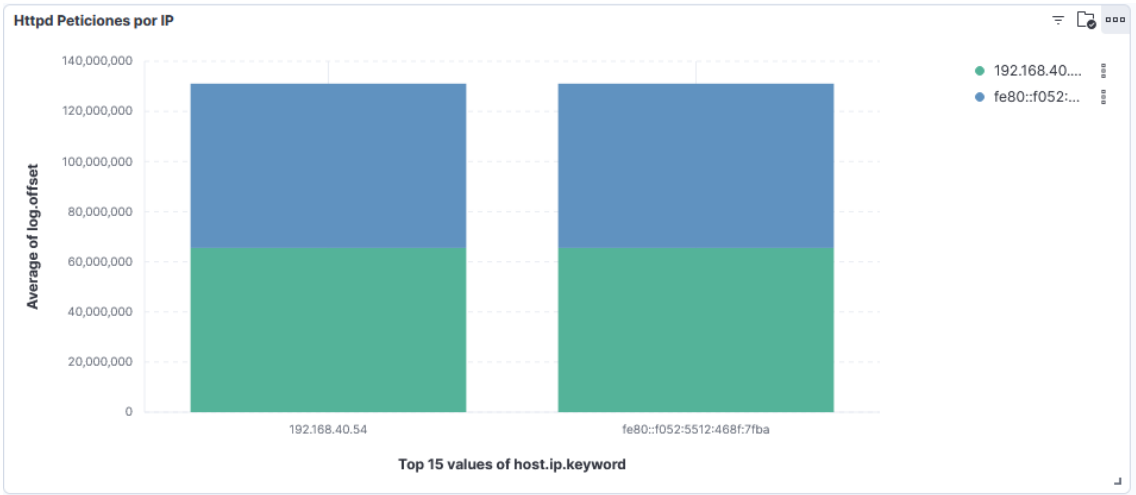


Figura 87 *Peticiones por IP*

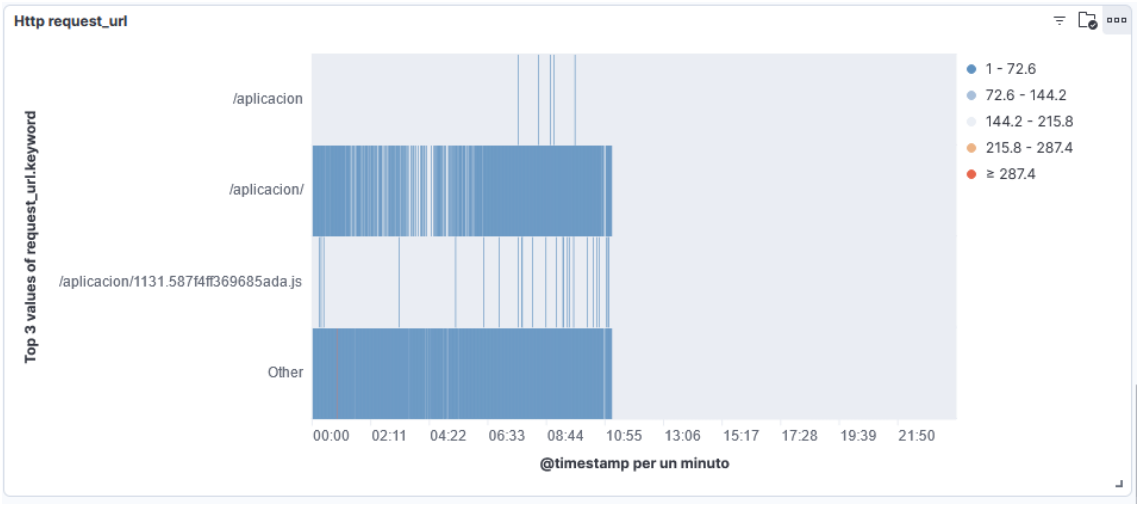


Figura 1 *Peticiones por URL*

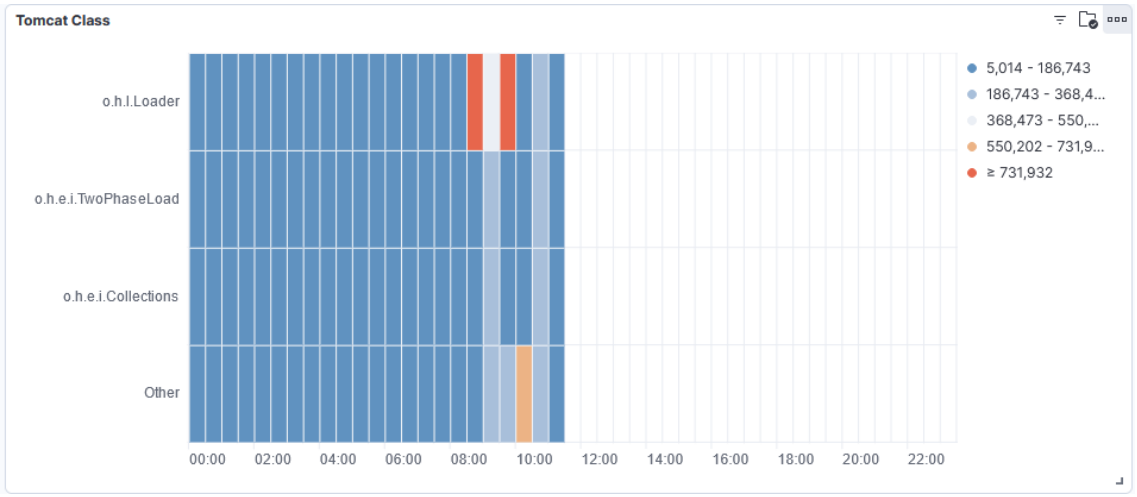


Figura 90 *clases Tomcat*

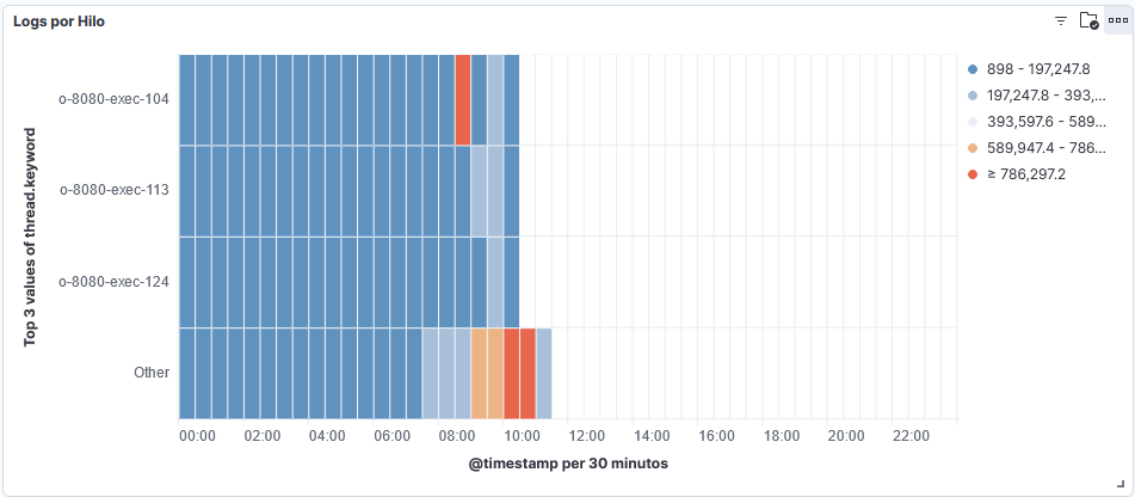


Figura 91 *Hilos Tomcat*

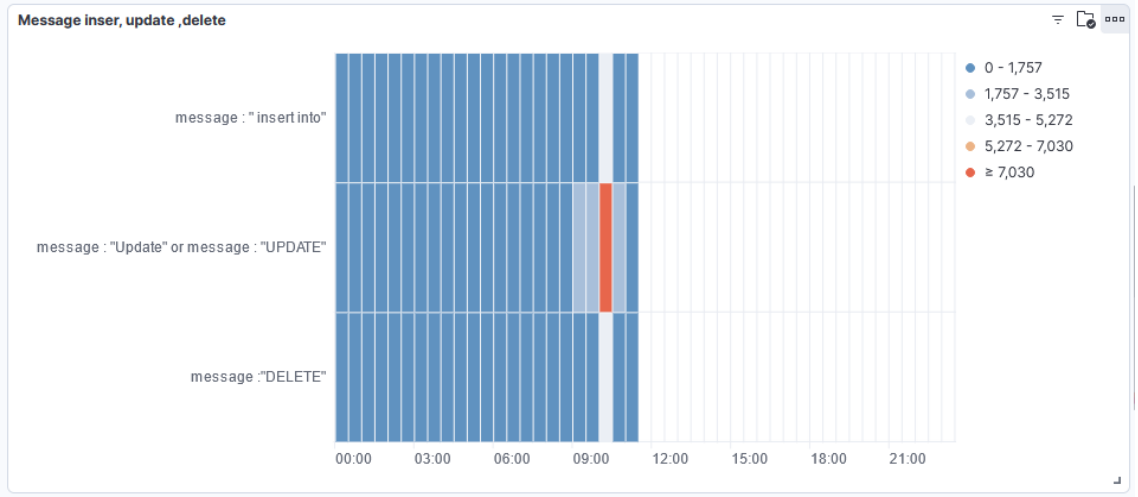


Figura 91 *Inserciones Tomcat*

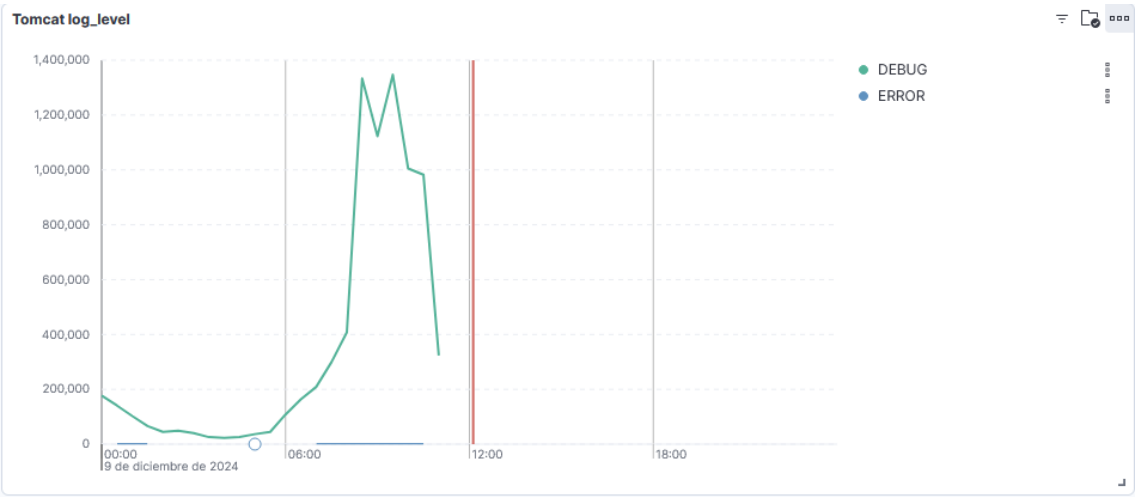


Figura 93 *Cantidad de registros por nivel*

Figura 94 *Haproxy por IP*

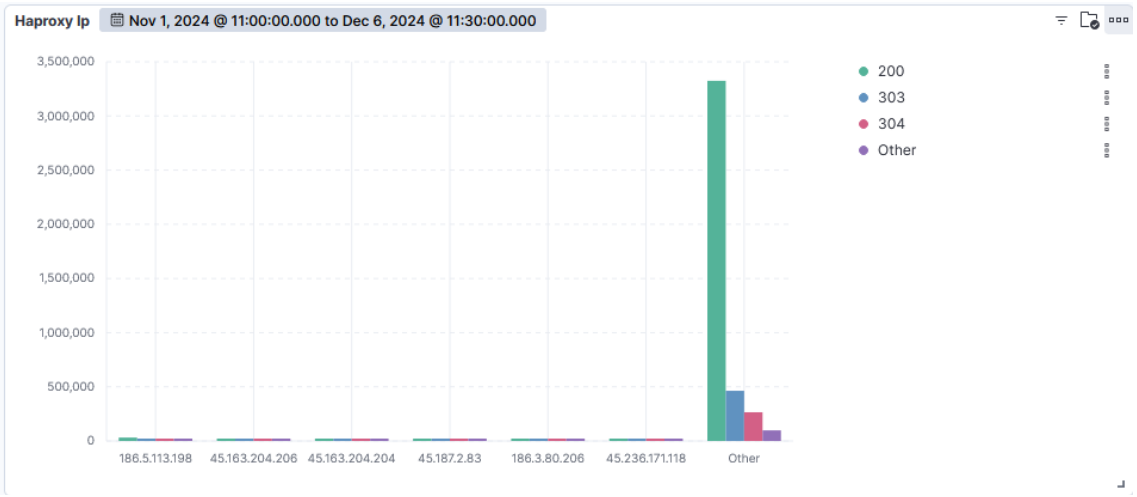


Figura 94 *Cantidad de registros por nivel*

Figura 95 *Cantidad de registros por nivel*

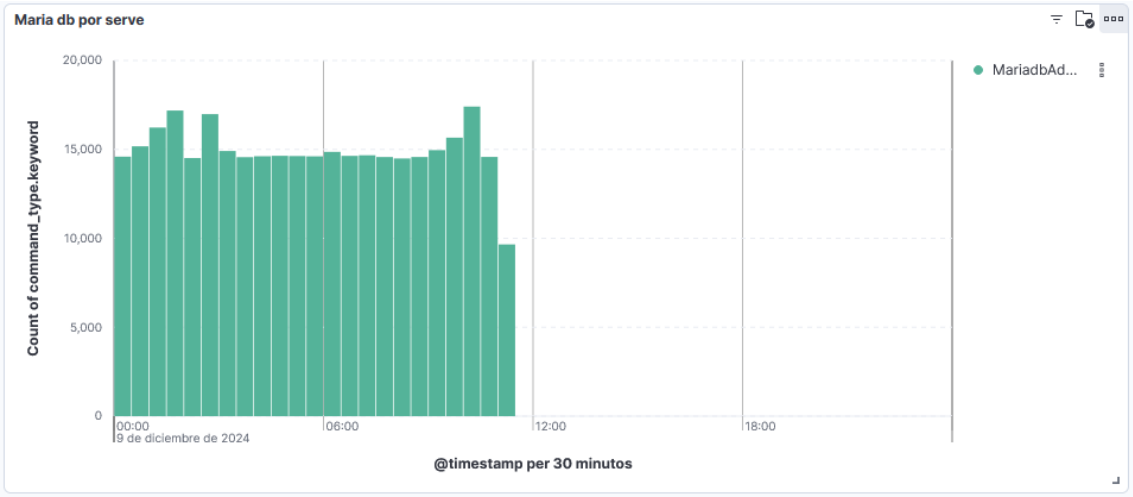


Figura 96 *Cantidad de registros por nivel*

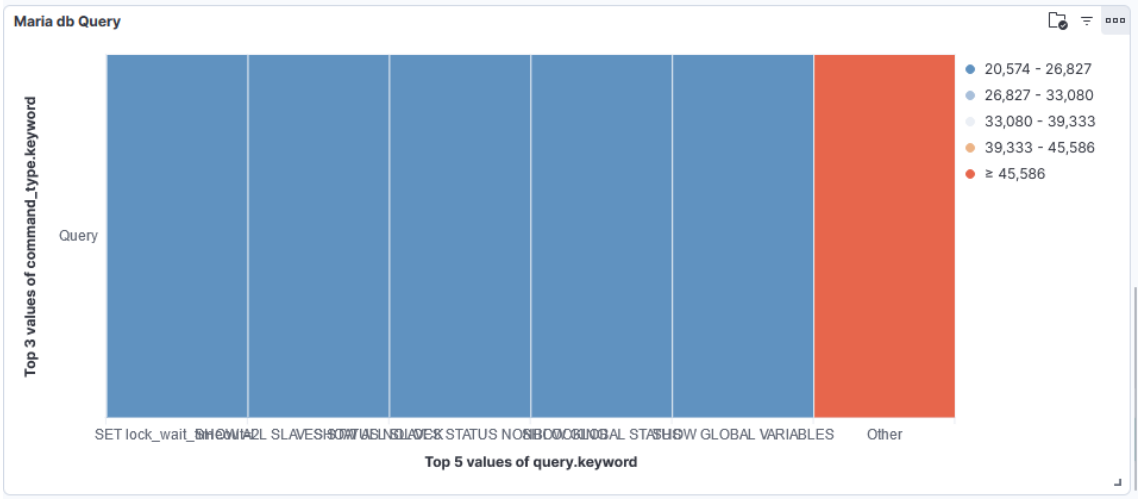


Figura 97 *Cantidad de registros por nivel*

Anexo 6 *Json Upse-app*

```
PUT /upse-app
{
 "mappings": {
   "properties": {
     "@timestamp": {
       "type": "date"
     },
     "@version": {
```

```
  "type": "text",
  "fields": {
    "keyword": {
      "type": "keyword",
      "ignore_above": 256
    }
  }
},
"agent": {
  "properties": {
    "ephemeral_id": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    },
    "id": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    },
    "name": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
```

```
    },
    "type": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    },
    "version": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
},
"ecs": {
  "properties": {
    "version": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
},
"event": {
  "properties": {
```

```
    "dataset": {
      "type": "keyword"  // Cambiado de text a keyword
    },
    "original": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
},
"host": {
  "properties": {
    "architecture": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    },
    "containerized": {
      "type": "boolean"
    },
    "hostname": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
```

```
},
"id": {
  "type": "text",
  "fields": {
    "keyword": {
      "type": "keyword",
      "ignore_above": 256
    }
  }
},
"ip": {
  "type": "text",
  "fields": {
    "keyword": {
      "type": "keyword",
      "ignore_above": 256
    }
  }
},
"mac": {
  "type": "text",
  "fields": {
    "keyword": {
      "type": "keyword",
      "ignore_above": 256
    }
  }
},
"name": {
  "type": "text",
  "fields": {
    "keyword": {
      "type": "keyword",
      "ignore_above": 256
    }
  }
```

```
},
"os": {
 "properties": {
  "codename": {
   "type": "text",
   "fields": {
    "keyword": {
     "type": "keyword",
     "ignore_above": 256
    }
   }
  },
  "family": {
   "type": "text",
   "fields": {
    "keyword": {
     "type": "keyword",
     "ignore_above": 256
    }
   }
  },
  "kernel": {
   "type": "text",
   "fields": {
    "keyword": {
     "type": "keyword",
     "ignore_above": 256
    }
   }
  },
  "name": {
   "type": "text",
   "fields": {
    "keyword": {
     "type": "keyword",
     "ignore_above": 256
```

```
          }
         }
        },
        "platform": {
         "type": "text",
         "fields": {
          "keyword": {
           "type": "keyword",
           "ignore_above": 256
          }
         }
        },
        "type": {
         "type": "text",
         "fields": {
          "keyword": {
           "type": "keyword",
           "ignore_above": 256
          }
         }
        },
        "version": {
         "type": "text",
         "fields": {
          "keyword": {
           "type": "keyword",
           "ignore_above": 256
          }
         }
        }
       }
      }
     },
     "input": {
      "properties": {
```

```
    "type": {
     "type": "text",
     "fields": {
      "keyword": {
       "type": "keyword",
       "ignore_above": 256
      }
     }
    }
   }
  },
 "log": {
  "properties": {
   "file": {
    "properties": {
     "path": {
      "type": "text",
      "fields": {
       "keyword": {
        "type": "keyword",
        "ignore_above": 256
       }
      }
     }
    }
   },
   "offset": {
    "type": "long"
   }
  }
 },
 "mariadb": {
  "properties": {
   "event": {
    "properties": {
     "dataset": {
```

```
          "type": "keyword"
        }
       }
     },
     "server_name": {
       "type": "text",
       "fields": {
         "keyword": {
           "type": "keyword",
           "ignore_above": 256
         }
       }
     }
   }
 },
 "message": {
   "type": "text",
   "fields": {
     "keyword": {
       "type": "keyword",
       "ignore_above": 256
     }
   }
 },
 "server_name": {
   "type": "text",
   "fields": {
     "keyword": {
       "type": "keyword",
       "ignore_above": 256
     }
   }
 },
 "tags": {
   "type": "text",
   "fields": {
```

```
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
 }
}
```


Anexo 7 *validación de instrumento: Encuesta*

RÚBRICA: INSTRUMENTO DE ENCUESTA PARA EXPERTOS EN CIBERSEGRUDAD.																	
CRITERIOS		SUFICIENCIA				CLARIDAD				COHERENCIA				RELEVANCIA				OBSERVACIÓN
Nº	PREGUNTAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
1	¿ Cargo actual?				x				x				x				x	
2	¿Años de experiencia en el departamento de TICs?				x				x				x				x	
3	¿Nivel de familiaridad con las normativas ISO 27001 e ISO 27002?				x				x				x				x	
4	¿Existen políticas documentadas de seguridad específicas para la protección de los servidores en la universidad?				x				x				x				x	
5	¿Qué medidas de protección se implementan en los servidores? (Seleccione hasta 3)				x				x				x				x	
6	¿Con qué frecuencia se revisan o actualizan las políticas de seguridad de los servidores?				x				x				x				x	

Figura 88 *validación de instrumento parte 1*

7	¿El departamento de TICs ha realizado evaluaciones de riesgo para la infraestructura de servidores?				x				x				x				x	
8	¿Qué herramientas utilizan para la recolección y análisis de logs en los servidores? (Seleccione hasta 2)				x				x				x				x	
9	¿Con qué frecuencia se revisan los logs generados por los servidores?				x				x				x				x	
10	¿La universidad ha implementado la centralización de logs?				x				x				x				x	
11	¿Considera que el sistema de monitoreo actual cumple con los controles de seguridad establecidos por la ISO 27001?				x				x				x				x	
12	¿Cómo calificaría la efectividad de las políticas de seguridad implementadas para los servidores en la universidad?				x				x				x				x	
13	¿Qué áreas considera más críticas para mejorar la seguridad de los servidores? (Seleccione hasta 3)				x				x				x				x	
14	¿Qué mejoras considera necesarias en la infraestructura actual de seguridad para alinearse con las normativas ISO 27001 e ISO 27002? (Seleccione hasta 3) ¿Cree que la				x				x				x				x	

Figura 89 *validación de instrumento parte 2*

15	infraestructura actual está preparada para enfrentar un ataque de ciberseguridad de gran escala?				x				x				x				x	
16	¿Qué tan probable considera la implementación de un sistema de centralización de logs en los próximos 12 meses?				x				x				x				x	
17	¿Cree que el personal encargado del monitoreo y gestión de logs está suficientemente capacitado para llevar a cabo estas tareas de manera eficiente?				x				x				x				x	
18	¿Cuál es el mayor obstáculo para implementar un sistema de centralización de logs?				x				x				x				x	
19	¿Cuánto cree que contribuiría una capacitación regular en ciberseguridad a mejorar la seguridad de la infraestructura de servidores?				x				x				x				x	

Figura 90 *validación de instrumento parte 3*

Anexo 8 *Encuesta Implementación*

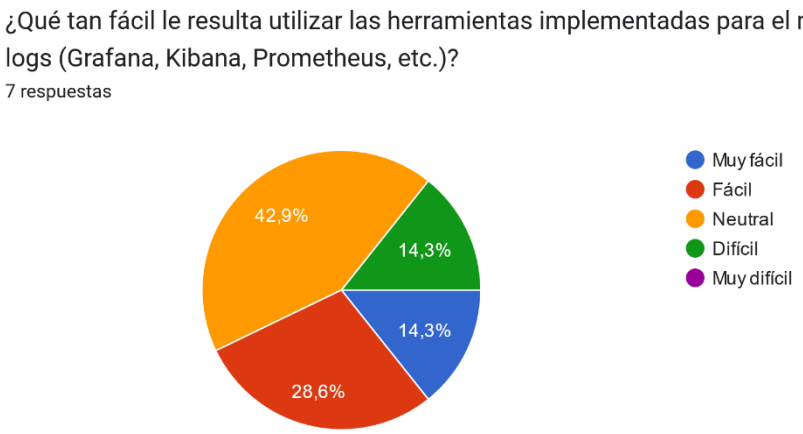


Figura 91 *Análisis de herramientas implementadas*

De acuerdo con los resultados de la encuesta, la facilidad de uso de las herramientas implementadas para el monitoreo y análisis de logs (Grafana, Kibana, Prometheus, etc.) presentó opiniones variadas. Un **42.9%** de los participantes calificó su experiencia como neutral, mientras que el **28.6%** consideró que las herramientas son fáciles de usar. Por otro lado, un **14.3%** indicó que el uso de las herramientas resulta muy fácil, y otro **14.3%** lo percibió como difícil. Es importante destacar que ningún participante calificó el uso de estas herramientas como muy difícil, lo que sugiere que, aunque existen áreas de mejora, el nivel de complejidad general es aceptable y manejable para la mayoría de los usuarios.

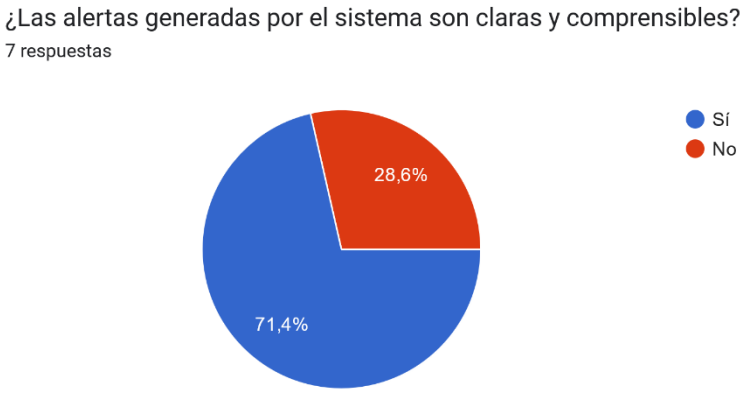


Figura 92 *Análisis de alertas*

En relación con la claridad y comprensión de las alertas generadas por el sistema, el **71.4%** de los participantes afirmó que las alertas son claras y comprensibles, mientras

que el **28.6%** consideró lo contrario. Esto indica que, en general, la mayoría de los usuarios percibe las alertas como efectivas y fáciles de entender, aunque existe un porcentaje significativo que identifica áreas de mejora en su diseño o presentación para garantizar una mejor comprensión y utilidad.

Figura 93 *Análisis de monitoreo*

Los resultados muestran que el 100% de los encuestados considera que los paneles de monitoreo son intuitivos y útiles para su trabajo diario. Este dato refleja una aceptación completa de los paneles como una herramienta efectiva para las tareas de monitoreo, indicando que su diseño y funcionalidad cumplen con las expectativas de los usuarios. Este nivel de satisfacción es un indicador positivo del impacto del sistema implementado en las operaciones diarias.

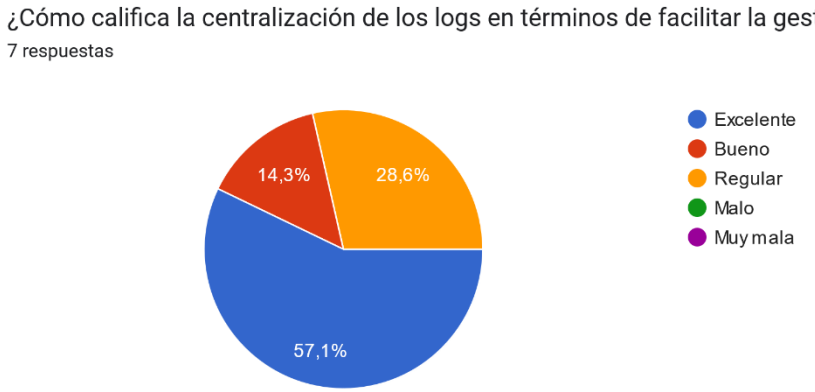


Figura 94 *Análisis de calificación de los registros*

Respecto a la centralización de los logs y su impacto en la gestión de eventos, el 57.1% de los encuestados calificó esta funcionalidad como excelente, mientras que el 28.6% la consideró buena. Un 14.3% la calificó como regular, y ningún participante señaló que fuese mala o muy mala. Estos resultados evidencian que la mayoría de los usuarios percibe la centralización de logs como una herramienta eficiente y efectiva para facilitar la gestión de eventos, aunque un pequeño porcentaje considera que aún hay margen de mejora en esta funcionalidad.

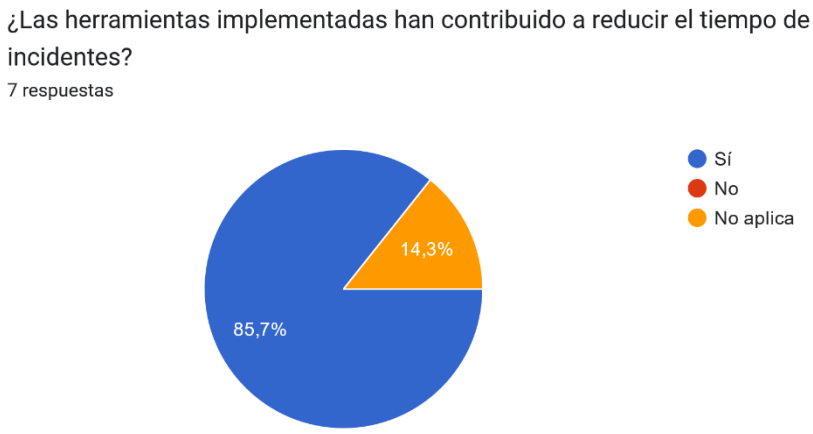


Figura 95 *Análisis de tiempo de respuesta ante incidentes*

El **85.7%** de los encuestados afirmó que las herramientas implementadas han contribuido a reducir el tiempo de respuesta ante incidentes, mientras que el **14.3%** indicó que no han notado dicha mejora. Este resultado resalta el impacto positivo que ha tenido la implementación de las herramientas en la gestión de incidentes, permitiendo a la mayoría de los usuarios responder de manera más eficiente. Sin embargo, es importante considerar el porcentaje restante para identificar posibles áreas de mejora o casos específicos donde la solución no ha tenido el mismo efecto.

Figura 96 *Análisis de alineación con normativa iso*

Según los resultados, el 71.4% de los encuestados considera que el sistema se alinea con las normativas de seguridad establecidas en la ISO 27001, específicamente en su sección 12.4 sobre "Logging and Monitoring". Sin embargo, un 28.6% opina que el sistema no cumple completamente con estas normativas. Esto indica que, aunque la mayoría reconoce la conformidad del sistema con los estándares, es importante evaluar los aspectos señalados por los usuarios que no lo perciben así, con el fin de identificar brechas y realizar los ajustes necesarios para garantizar un cumplimiento total.

Figura 97 *Análisis de tiempo de facilidad en gestión de eventos*

Los resultados reflejan que el 71.4% de los encuestados está **totalmente de acuerdo** con que la centralización de los logs facilita la gestión de eventos de seguridad, mientras que

el 28.6% está **de acuerdo** con esta afirmación. Ningún participante expresó una postura neutral, en desacuerdo o totalmente en desacuerdo, lo que indica un consenso positivo sobre la efectividad de la centralización de los logs en el contexto de la gestión de eventos. Este resultado refuerza la importancia de esta funcionalidad como una herramienta clave para la mejora de la seguridad.

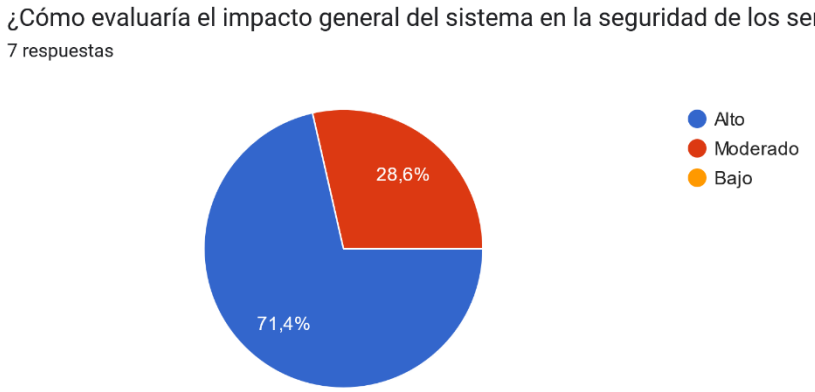


Figura 98 *Análisis de impacto general en el sistema*

El 71.4% de los encuestados evaluó el impacto general del sistema en la seguridad de los servidores como **alto**, mientras que el 28.6% lo calificó como **moderado**. Ningún participante indicó que el impacto fuese bajo, lo que demuestra que la mayoría de los usuarios perciben el sistema como una herramienta efectiva para mejorar la seguridad de los servidores. Este resultado resalta la relevancia de la implementación realizada y su contribución positiva al fortalecimiento de la seguridad en la infraestructura evaluada.