Sistema de monitoreo basado en ELK Stack para mejorar el gobierno de TI

Monitoring system based on ELK Stack to improve IT governance

Angelo Bryan Barahona Cotarate¹, Katherin Vanessa Rodriguez Zevallos² y Frank Edmundo Escobedo Bailón³

¹ Universidad Nacional Tecnológica de Lima Sur (UNTELS). Av. Revolución Sector 3 Grupo 16 Mz B Lt 6- Villa El Salvador, Lima, Perú. Correo electrónico: angelo.bbc2@gmail.com

² Universidad San Ignacio de Loyola (USIL). Pasaje Ayancocha 143 - Huánuco, Huánuco, Perú. Correo electrónico: vane251089@hotmail.com. ORCID: <https://orcid.org/0000-0001-8350-720>

³ Universidad Nacional Tecnológica de Lima Sur (UNTELS). Calle Carlos Alayza y Roel 2392 Dpto. 104 - Lince, Lima, Perú. Correo electrónico: fescobedo@untels.edu.pe. ORCID: <https://orcid.org/0000-0002-2058-0976>

Resumen

Actualmente, las herramientas de monitoreo en el mercado ayudan a mantener en óptimas condiciones la infraestructura de TI y con esto mejorar la gestión de TI de una organización que proporciona un alineamiento estratégico. El objetivo del estudio es analizar la manera de responder de forma rápida frente a los incidentes que se originan en los recursos de TI, mediante un sistema de monitoreo basado en ELK Stack, dando lugar a una mejora en el gobierno de TI dentro de la organización. Se hizo la revisión de distintas fuentes de documentos bibliográficos de una antigüedad no mayor a 5 años y con artículos descritos como investigaciones. Dentro del gobierno de TI, una herramienta de monitoreo basado en ELK Stack genera flexibilidad al generar reportes con data limpia y facilita la toma de decisiones mediante dashboards dinámicos. ELK Stack al ser un marco de trabajo Open Source, dividido en 3 herramientas con distintos propósitos, prioriza la adaptación de un monitoreo adecuado a los planes de una organización con las tecnologías de información. La implementación de un sistema de monitoreo no solo mejora el tiempo de respuesta frente a las incidencias, sino también mejora el desempeño del personal a nivel operativo y a nivel gerencial.

Palabras clave: Sistema de monitoreo, ELK Stack, Gestión de TI, Proceso ETL.

Abstract

Currently, monitoring tools in the market help to maintain in optimal conditions the IT infrastructure and thus improve the IT management of an organization providing a strategic alignment. Objective: The objective of the study is to analyze how to respond quickly to incidents that originate in IT resources, through a monitoring system based on ELK Stack, leading to an improvement in IT governance within the organization. A review of different sources of bibliographic documents no older than 5 years and with articles described as research was made. Within IT governance, a monitoring tool based on ELK Stack generates flexibility by generating reports with clean data and facilitates decision making through dynamic dashboards. ELK Stack being an Open Source framework, divided into 3 tools with different purposes, prioritizes the adaptation of adequate monitoring to an organization's plans with IT. The implementation of a monitoring system not only improves the response time to incidents, but also improves the performance of personnel at the operational level and at the managerial level.

Keywords: Monitoring system, ELK Stack, IT Management, ETL Process

Introducción

La tecnología va aumentando su importancia en la administración de una organización a medida

que los años avanzan. El constante crecimiento de los recursos de tecnologías de información (TI) supone el aumento de información y a su

vez, procesar grandes volúmenes de datos en tiempo real desde distintas fuentes para la satisfacción de los usuarios finales tanto internos como externos de una organización.

La situación actual, originada por el COVID-19, forzó a las organizaciones a invertir en un gobierno de TI para enfrentar a la competencia o adaptarse a la nueva normalidad. Es cierto que el área de tecnologías de información ya no es vista como un equipo de servicio técnico sino como parte importante en la toma de decisiones a nivel gerencial de las organizaciones.

Esta investigación se inició después de considerar la situación crítica de los recursos de TI frente a los incidentes recurrentes que amenazan la continuidad del negocio de las organizaciones. Mantener una buena gestión de TI para el apoyo en la determinación de los responsables de la planificación estratégica de las tecnologías de información, de la toma de decisiones y de la explotación de los recursos operativos es una tarea crucial.

Esta situación es un desafío en el aspecto de la continuidad del negocio, ya que es imposible monitorear continuamente el estado de los recursos de TI debido a la limitación de disponibilidad las 24 horas del día en la mano de obra. Esto a menudo conduce a una situación demasiado tarde para ser manejada. Para eso, es importante tener un sistema de monitoreo con características de autonomía, confiable y flexible. El uso de la

automatización del monitoreo no solo incrementa la eficiencia de los recursos de tecnologías de la información, sino también la eficiencia del personal encargada de estas, reduciendo los costos o dando énfasis a otras mejoras dentro de la organización.

El objetivo principal es responder de manera rápida frente a los incidentes que se originan en los recursos de TI, mediante un sistema de monitoreo basado en ELK Stack, dando lugar a una mejora en el gobierno de TI dentro de la organización.

Metodología

La presente investigación se basa en resultados obtenidos por estudios anteriores, en cuanto a la efectividad de la implementación de un sistema de monitoreo en las empresas, los cuales se ensamblan con el modelo conceptual obtenido de documentos bibliográficos.

Para la búsqueda de los documentos bibliográficos se utilizaron distintas fuentes documentales. Los siguientes recursos se usaron para la obtención del material bibliográfico: Google Académico, Scielo, Redalyc, Dialnet y repositorios universitarios. Los registros obtenidos por fuente oscilaron entre 15 y 23 investigaciones tras la combinación de las siguientes palabras claves:

- ELK Stack
- Gestión de TI
- Sistema de monitoreo

Para la validación de estos documentos bibliográficos se optaron por las siguientes

descripciones: artículo científico, tesis, artículo de revisión y libros. Se lograron encontrar aproximadamente 90 documentos, de los cuales, se consideraron solo los documentos con antigüedad no mayor a 5 años (2015 - 2020) y que tengan las descripciones mencionadas. Mediante el filtro bajo las restricciones de los documentos, se observaron 40 documentos potenciales y de estos 28 fueron usados en el presente artículo.

Materiales y métodos

Sistema de monitoreo de TI

Es una herramienta de seguimiento que permite recolectar, tratar, analizar y generar información a un grupo de actores interesados en la implementación de un determinado proyecto, con el fin de informar y contribuir a una mejor toma de decisiones. (Lauriac, 2016)

Según Alestra (2020), existen los siguientes tres tipos de herramientas destinadas al monitoreo de TI:

- Herramientas de observación
- Herramientas analíticas
- Herramientas de engagement

Existen los siguientes tipos de monitoreo implicados como tareas que los encargados de TI deben realizar:

- Monitoreo de desempeño
- Monitoreo de sistema
- Monitoreo de usuario
- Monitoreo de seguridad

Existen dos puntos de vista para tratar el proceso de monitoreo a una red: el monitoreo activo y el monitoreo pasivo. Ambos son

complementarios, aunque sean totalmente diferentes. (Escobar, 2015)

Monitoreo Activo: Este tipo de técnica se lleva a cabo introduciendo paquetes de prueba, o generando el envío a determinadas aplicaciones para medir el tiempo de respuesta. Esta técnica de monitoreo agrega tráfico en la red y se emplea para medir el rendimiento de esta. (Sanchez, 2016)

Monitoreo Pasivo: Se basa en la recolección de datos desde la obtención y análisis del tráfico que circula por la red. Se emplean diversos dispositivos para generar esta navegación de datos desde el equipo monitoreado hasta el centro de monitoreo. Este enfoque no aumenta el tráfico en la red a diferencia del monitoreo activo. (Sanchez, 2016)

Gobierno de TI

Es una práctica que tanto organizaciones privadas como públicas implementan con el fin de tener un control de su estructura de las TI y garantizar la sostenibilidad y el desarrollo continuo conjunto, por medio del alineamiento entre los objetivos de las TI y los objetivos estratégicos de la organización. Se basa fundamentalmente en el alineamiento de las TI con el negocio. (Gaseta et al., 2019)

El gobierno de TI se distribuye en tres dimensiones:

- Estructura de gobierno de las tecnologías respectivas
- Proceso de gobernabilidad

– Métricas de resultados

La primera dimensión descrita tiene como objetivo lograr la alineación estratégica de TI con los procesos del negocio incluyendo métodos para la toma de decisiones, establecimiento de la dirección y políticas que serán tomadas como referencia en toda la organización. La segunda dimensión descrita se enfoca en el desempeño de cuentas en la

organización de TI, se generan todas las ideas para establecer las políticas y procedimientos para la elaboración y cumplimiento de los proyectos de inversión. La tercera dimensión da una evaluación tanto al gobierno de TI como a los procesos y estructura, dando por seguro que todos los resultados deseados están siendo cumplidos. (Bowen et al., 2007)

Figura 1: Arquitectura de un proceso ETL (tomado de Kimball, 2004)

Las actividades del gobierno de TI se pueden agrupar en cinco áreas de enfoque las cuales son: entrega de valor, administración de riesgos, administración de recursos, medición de

desempeño y alineamiento estratégico. (Marulanda et al., 2017)

Proceso ETL

Hace referencia a los procedimientos de

extracción (Extract) de datos de múltiples fuentes, reformatearlos o transformarlos (Transform) con el objetivo de adaptar los datos a las necesidades presentadas como requerimientos para su uso y carga (Load) de la información en otra base de datos o Datawarehouse. (Ontiveros et al., 2017)

Como se puede observar en la Figura 1, los procesos ETL siguen una serie de actividades establecidas desde la recolección de datos hasta la presentación y análisis de resultados. Para obtener resultados, se opta por 4 actividades, los cuales son: extracción, depuración, conformación/normalización y entrega. Cabe recalcar que la actividad de entrega no es contemplada como principal, ya que no necesariamente se generan procesos ETL para la visualización de datos. (Kimball, 2004)

En síntesis, estos procesos se definen como aquellos que permiten a una organización manipular datos. Empezando desde la extracción desde un sistema origen, pasando por la transformación y terminando en la carga a otro sistema destino. Esto permite obtener un análisis de calidad y completar las tareas con más eficiencia para alcanzar los objetivos empresariales y una mejor toma de decisiones. (Trujillo, 2018)

a) Extracción: La información se extrae de diferentes fuentes, desde tradicionales hasta las tecnológicas. Esta fase estandariza los datos para iniciar la siguiente fase. Siempre se

tiene en cuenta que ni una de las actividades realizadas en esta fase altere en el sistema origen. Si los datos a extraer son conglomerados y diversos, genera posibilidades de colapso o pérdida de información en el sistema origen. Debido a esto, muchas operaciones de extracción suelen ser programados en periodos definidos donde el impacto de posibles riesgos sea nulo. (Trujillo, 2018)

Según Oracle (2012), existen tipos de extracciones que son manipulados por módulo denominado Change Data Captura (CDC). Esta herramienta es frecuentemente utilizada en Data Warehousing, permitiendo el control de cambios que ocurren en una tabla y como salida entrega las modificaciones de una forma rápida. Los tipos de extracción, elegidas según la necesidad de la organización, son los siguientes: extracción total, extracción incremental y notificación de actualización.

b) Transformación: Hace referencia a la reformación y limpieza de datos cuando se vea como una necesidad. En esta fase se aplican una serie de requerimientos del negocio para convertirlos en datos que después serán cargados. El desarrollador o analista del proceso ETL debe estar encargado de esta tarea, ya que esta fase requiere de manipulación de datos reales y conocimiento de los requerimientos y modelo del negocio.

(Trujillo, 2018)

- c) Carga: Esta etapa tiene como objetivo facilitar el análisis o brindar apoyo en un proceso de negocio. En esta fase, la data que proviene de la transformación es cargada en el sistema destino. La carga puede abarcar muchas actividades, dependiendo de los requerimientos de la organización. En algunas bases de datos

será necesario sobrescribir la data antigua con la nueva, mientras que en otras será necesario acoplar estos datos y tratarlas en conjunto. En síntesis, esta fase corresponde a la carga de información en los repositorios de información destino. Existen dos métodos básicos para el desarrollo del proceso de carga, los cuales son: Rolling y acumulación simple. (Trujillo, 2018)

Figura 2: *Arquitectura de ELK Stack (tomado de Lozada, 2018)*

Elastic Stack

ELK Stack es un margen de trabajo basado en tres proyectos de código abierto referidos en las siglas “ELK”: Elasticsearch, Logstash y Kibana. Elasticsearch es un motor de búsqueda y análisis. Logstash es un pipeline destinado al procesamiento de datos del lado del servidor que recolecta datos desde diferentes fuentes de manera simultánea, los transforma y los envía a Elasticsearch. Kibana permite la visualización de los datos a partir de la fuente de datos en Elasticsearch. ELK sincroniza estos proyectos en la arquitectura que se muestra en la Figura 2.

ELK Stack evoluciona para dar lugar a Elastic Stack, adaptando nuevos enfoques basados en las necesidades actuales que las organizaciones perciben. (Elastic, 2020a)

La introducción de nuevas herramientas como los Beats transformaron la arquitectura estándar del margen de trabajo ELK Stack como se aprecia en la Figura 3. Debido a esto, decidieron cambiar de nombre también al margen de trabajo por Elastic Stack. Los Beats son ligeros agentes que se instalan en equipos para la recopilación de diferentes tipos de datos y enviarlos al proceso que se trabajaba en ELK Stack. (Berman, 2020)

Figura 3: *Arquitectura de Elastic Stack (tomado de Invivoo, 2020)*

Según Alvarado (2020), Elastic Stack facilita una variedad de casos de uso, debido a la rapidez y escalabilidad de Elasticsearch para indexar muchos tipos de contenidos. Los escenarios donde Elastic Stack se puede desenvolver son:

- Búsqueda de aplicaciones.
- Búsqueda de sitio web.
- Búsqueda empresarial.
- Logging.
- Monitoreo de contenedores.
- Monitoreo de rendimiento de aplicaciones.
- Métricas geoespaciales.
- Seguridad.
- Análisis de procesos.

Beats

Según Alvarado (2020), Beats es una plataforma

para enviar datos desde un sistema origen hasta el stack de una manera organizada. Los Beats son Data Shippers que actúan como agentes, ya que entregan directamente la data al Elasticsearch y/o Logstash sin algún proceso de transformación de por medio. Existen los siguientes tipos de agentes Beats:

- Filebeat
- Metricbeat
- Heartbeat
- Packetbeat
- Winlogbeat
- Audiobeat
- Functionbeat

Logstash

Según Chhajed (2015), Logstash es una

canalización de datos que ayuda a recopilar y analizar una gran variedad de datos tanto estructurados como no estructurados. Logstash tiene las siguientes características:

- Procesamiento de datos centralizados
- Compatibilidad con formatos de registro personalizados
- Desarrollo de complementos

Elasticsearch

Es un motor de búsqueda de código abierto basado en Apache Lucene que proporciona escalabilidad horizontal, confiable y capacidad multiusuario para búsquedas en tiempo real. El formato de comunicación que tiene se basa en

JSON sobre una API RESTful. Al estar ligado con Apache Lucene, esta herramienta puede indexar datos de forma dinámica sin algún antecedente de su estructura. (Chhaged, 2015)

Según Sachdeva (2017), Elasticsearch ejecuta de forma perfecta en pequeñas y grandes empresas, debido a su escalabilidad. Todos los datos son almacenados en documentos JSON. Proporciona análisis y búsqueda de data en tiempo real. Además, es posible su ejecución en cualquier tipo de infraestructura de TI. Tiene un nodo de respaldo para la reorganización y equilibrio automático del flujo de los datos.

Figura 4: Dashboards en Kibana (tomado de Elastic, 2020b)

Kibana

Es una plataforma de visualización de datos de código abierto que permite dar una representación visual de los datos estructurados y no estructurados que están almacenados en los índices de Elasticsearch. Este escrito completamente en HTML y JavaScript, dando la oportunidad de mostrar gráficos sumamente flexibles. Kibana desempeña su función al exponer datos a través de vistosos histogramas, geomapas, gráficos circulares, etc. (Chhaged, 2015)

Kibana es una herramienta que tiene como objetivo el análisis intuitivo y visualización de grandes volúmenes de datos en tiempo real. La interfaz flexible de esta herramienta hace que sea la experiencia del usuario al crear, guardar, editar, compartir, exportar e incrustar datos visualizados sea más fácil para una mayor comunicación. (Sachdeva, 2017)

Resultados y discusión

Según Casas & Sempértegui (2016), mencionan que un sistema de monitoreo influye de forma positiva en la gestión de TI. Para llegar a estos resultados se basaron en la reducción de desempeño por parte del administrador de red al tener la información en línea y tomar conocimiento detallado sobre el funcionamiento de los principales componentes de infraestructura de TI en la institución educativa donde se realizaba el estudio.

Según Velasco & Cagua (2017), el uso de herramientas Open Source es eficaz para mejorar la administración de recursos de TI. Este tipo de herramientas permiten al personal de TI alinear las estrategias de TI con las estrategias del negocio (alineamiento estratégico).

De acuerdo con Sierra & Daz (2018), los sistemas de monitoreo basados en software libre ahorran tiempo y costos, sea pequeña o mediana empresa. Al reducir los costos, el personal encargado de la supervisión de la infraestructura de TI tendrá una reducción de esfuerzo de su trabajo para enfocarse en la mejora.

Según Moreano (2015), comentan que el uso de una herramienta Open Source no implica gratuidad, ya que existe el trabajo empeñado en los desarrolladores del proyecto que no fueron descritos en sus objetivos. ELK Stack es una herramienta muy interactiva con los usuarios al estar divididos por herramientas independientes de esta manera se puede dividir la especialización en un equipo fácilmente.

Sánchez (2017) menciona que se redujo considerablemente las anomalías que generaban la degradación en la red mediante la activación de alertas desde una herramienta de monitoreo. Las alertas de monitoreo en ELK Stack pueden adaptarse al modelo de negocio de la empresa, por lo general se dividen en: fatal, critical, warning y unknown.

Según Cisneros (2018) nos comenta que la implementación de un sistema de monitoreo con

la infraestructura requerida para que se genera un monitoreo de cuarta generación incrementa los ingresos de una empresa terciaria al darles la posibilidad de ofrecer nuevos servicios en este caso el servicio de monitoreo de infraestructura de TI.

Cajahuaringa (2015) menciona que una herramienta de monitoreo mejora considerablemente en la recepción de incidentes que antes no se observaban, dando a entender que ahora se tiene una visión más amplia de la infraestructura de TI en una empresa dedicada a la prestación de los servicios relacionados con TI. Además, los reportes que esta herramienta genera dan lugar a mejores decisiones en alta gerencia.

De acuerdo con Quispe (2018), un déficit en el área de TI no siempre es por falta de personal sino por ausencia de recursos tecnológicos acorde al área como una herramienta de monitoreo. El autor logró medir la satisfacción tanto del personal operativo como gerencial viendo resultados positivos.

Según Saavedra (2015), la posibilidad de atender los principales requerimientos para la gestión de equipos de seguridad mediante distintas tecnologías disponibles y de libre acceso. Para implementar proyectos basados en procesos de ETL es necesario contar con un enfoque holístico para interrelacionar distintas herramientas.

Abi-gosen & Tejada (2015) nos comentan que es completamente necesario contar con un modelo

de Gobierno de TI adaptado a la empresa para garantizar una eficaz operación en la entrega de la infraestructura de TI, apoyado en la mitigación de riesgos y evitando los problemas que se originan de forma recurrente.

Conclusiones

La implementación de la herramienta de monitoreo y basada en ELK Stack influye de manera positiva en las 3 dimensiones de la gestión de TI. Permite redistribuir la estructura del gobierno de TI, ya que se notará una reducción de esfuerzo de algunos personales. El proceso de gobernabilidad será mas flexible para futuros cambios de acuerdo con el alineamiento estratégico que se rijan. Las métricas de resultados se verán reflejadas de forma positiva si la implementación se realiza de la forma adecuada en cada organización.

El área de tecnologías de información es la más beneficiada con la implementación de un sistema de monitoreo. No solo la eficiencia de los recursos de tecnologías de la información se verá incrementada sino también la eficiencia del personal encargada de estas, ya que el sistema de monitoreo permite una comunicación de alertas 24 horas al día y no habrá la necesidad de esperar a que el problema sea notificado por los usuarios finales.

La implementación de una herramienta Open Source de monitoreo significa una reducción de costos considerable. Es posible la automatización o mejora de los procesos a nivel operativo y

táctico que impliquen información de la infraestructura de TI. Además, implica un ahorro de costes en las inversiones de las tecnologías de información debido a la disminución de riesgos y prevención de incidentes que la herramienta proporciona.

Referencias bibliográficas

- Abi-gosen, O., & Tejada, C. (2015). Adaptación de modelo de Gobierno y Gestión de TI para la empresa virtual IT Expert basado en COBIT 5 [Universidad Peruana de Ciencias Aplicadas]. <http://hdl.handle.net/10757/346736>
- Alestra. (2020). ¿Qué es el monitoreo de TI? <http://blog.alestra.com.mx/que-es-el-monitoreo-de-ti>
- Berman, D. (2020). The Complete Guide to the ELK Stack. <https://logz.io/learn/complete-guide-elk-stack/#intro>
- Bowen, P., Decca, M.-Y., & Rohde, F. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. International Journal of Accounting Information Systems. <https://doi.org/10.1016/j.accinf.2007.07.002>
- Cajahuaringa, L. (2015). Uso de un sistema de gestión de monitoreo para la mejora de la administración de servidores de clientes hosting en GMD (Vol. 1, Issue 1) [Universidad Nacional Tecnológica de Lima Sur]. <http://www.ncbi.nlm.nih.gov/pubmed/17289255> <http://dx.doi.org/10.1016/j.jclepro.2011.10.008> http://www.uwaba.or.tz/National_Road_Safety_Policy_September_2009.pdf <http://dx.doi.org/10.1016/j.resconrec.2011.03.010> <http://dx.doi.org/10.1016/j.pecs.20>
- Casas, R., & Sempértegui, M. (2016). Implementación de un sistema de monitoreo y supervisión de la infraestructura y servicios de red para optimizar la gestión de TI en la Universidad Nacional Pedro Ruiz Gallo [Universidad Nacional Pedro Ruiz Gallo]. <http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/3424/BC-TES-TMP-2247.pdf?sequence=1&isAllowed=y>
- Chhajed, S. (2015). Learning ELK Stack.
- Cisneros, B. (2018). Implementación de un nuevo sistema de monitoreo en GMD para aumentar la eficacia operativa [Universidad San Ignacio de Loyola]. <http://repositorio.usil.edu.pe/handle/USIL/3637>
- Elastic. (2020a). ¿Qué es el ELK Stack? <https://www.elastic.co/es/what-is/elk-stack>
- Elastic. (2020b). Kibana. <https://www.elastic.co/es/kibana>
- Escobar, F. (2015). Sistema de análisis y control de red de datos & VoIP para el gobierno provincial de Tungurahua. <https://repositorio.uta.edu.ec/jspui/handle/123456789/19369>
- Gaseta, E., Motta, A., & Boca Piccolini, J. (2019). Gobierno de las tecnologías de la información. In REDCEDIA. <https://doi.org/10.2307/j.ctvpv4zxsx>
- Invivo. (2020). Monitoring and detection of anomalies with ELK. <https://www.invivo.com/blog/monitoring-and-detection-of-anomalies-with-elk/>
- Kimball, R. (2004). The Data Warehouse ETL Toolkit (Vol. 4, Issue 1). Wiley Publishing, Inc.
- Lauriac, N. (2016). Diseño e implementación de un sistema de monitoreo. Terre Des Hommes, 46.
- Lozada, S. (2018). ¿Qué es ELK? ElasticSearch, Logstash y Kibana.

- <https://openwebinars.net/blog/que-es-elk-elasticsearch-logstash-y-kibana/>
- Marulanda, C., López, M., & Valencia, F. (2017). Gobierno y gestión de ti en las entidades públicas. AD-Minister, 31, 75–92. <https://doi.org/10.17230/ad-minister.31.5>
- Moreano, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management) [Universidad San Francisco de Quito]. <http://repositorio.usfq.edu.ec/handle/23000/4911>
- Ontiveros, E., Vizcaíno, D., & López Sabater, V. (2017). Las ciudades del futuro: inteligentes, digitales y sostenible. http://www.observatorioabaco.es/bibliotecadocs/805_FT_CIUDADESINTELEGENTES_2017.pdf
- Oracle. (2012). Oracle Change Data Capture. <https://www.oracle.com/technetwork/es/articles/datawarehouse/oracle-change-data-capture-1545279-esa.html>
- Quispe, J. (2018). Implementación de un sistema de monitoreo y control de red para un canal De Televisión basado en herramientas Open Source y Software Libre [Universidad Nacional del Altiplano]. http://tesis.unap.edu.pe/bitstream/handle/UNAP/9019/Quispe_Bustincio_Jhon_Watson.pdf?sequence=1&isAllowed=y
- Saavedra, R. (2015). Diseño e implementación de un sistema integrado de gestión de equipos de seguridad [Pontificia Universidad Católica del Perú]. <http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6409>
- Sachdeva, G. (2017). Practical ELK Stack. <https://doi.org/10.1007/978-1-4842-2626-1>
- Sánchez, D. (2017). Implementación de un sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial [Universidad Técnica de Ambato]. <https://repositorio.uta.edu.ec/handle/123456789/25707>
- Sanchez, L. (2016). Implementación de un sistema de monitoreo para instituciones fiscales beneficiarias del proyecto de dotación de conectividad [Pontificia Universidad Católica del Ecuador]. http://repositorio.puce.edu.ec/bitstream/handle/22000/11144/Informe_Caso_de_Estudio_Unidad_de_Titulacion.pdf?sequence=1&isAllowed=y
- Sierra, W., & Daz, W. (2018). Diseño e implementación de un sistema de detección de anomalías de red mediante el análisis avanzado de logs utilizando software libre en un ambiente de laboratorio que permita la optimización de recursos tecnológicos (Vol. 2) [Universidad Piloto de Colombia]. <http://polux.unipiloto.edu.co:8080/00004741.pdf>
- Trujillo, T. (2018). Gestión de datos empresariales utilizando procesos ETL [Universidad Autónoma del Estado de México]. http://ri.uaemex.mx/bitstream/handle/20.500.11799/95251/Gestion_de_datos_empresariales_utilizando_procesos_ETL.pdf?sequence=1&isAllowed=y
- Velasco, C., & Cagua, G. (2017). Implementación de un sistema de monitoreo de redes utilizando herramientas Open Source y proveer servicios de directorio a través de Active Directory en la Facultad de Filosofía, Letras Y Ciencias de la Educación de la Universidad De Guayaquil [Universidad Politécnica Salesiana]. <https://dspace.ups.edu.ec/bitstream/123456789/13474/1/UPS-GT0018>