ART. 2

ESTRUCTURA DE SEGURIDAD PARA EL ANÁLISIS GESTIÓN DE LOGS DE APLICACIONES MULTICAPA

ESTRUCTURA DE SEGURIDAD PARA EL ANÁLISIS GESTIÓN DE LOGS DE APLICACIONES MULTICAPA

SECURITY STRUCTURE FOR ANALYSIS AND MANAGEMENT OF MULTI-PAPER APPLICATIONS LOGS

Figueroa Fernández Víctor
figo37vic@gmail.com

RESUMEN

El presente estudio tiene como objetivo el diseño de un modelo para la implementación de una estructura de seguridad para el análisis y gestión de logs de aplicaciones multicapa, con el propósito de procesar, analizar y monitorear los eventos de seguridad que se presentan diariamente en los sistemas de información y dispositivos tecnológicos en general.

Hoy en día la gran mayoría de los sistemas informáticos y dispositivos tecnológicos poseen mecanismos para generar registros logs, los cuáles contienen información acerca del estado actual y funcionamiento de los mismos.

Actualmente las empresas u organizaciones que cuentan con sistemas informáticos manejan y procesan una gran cantidad de información, estos sistemas generan ficheros logs, con el fin de almacenar los tipos de accesos, errores y alertas que se dan en los distintos niveles de su estructura. Es así que ante cualquier incidente que se esté suscitando como ser ataques de: inserción de código malicioso, denegación de servicios o simplemente una traza de error en el código de un sistema, éstos ficheros logs vienen a ser de gran utilidad a la hora de facilitar la información para dar respuesta y seguimiento a cualquier evento de seguridad, actualmente la revisión de estos ficheros logs viene a ser un proceso exhaustivo que implica mucho esfuerzo tanto manualmente o a través de un software, causando detención en los servicios brindados, además de generar retrasos y pérdidas de recursos al analizar, buscar e identificar qué tipo evento se suscitó y en qué lugar de la estructura se generó, dado el volumen y la cantidad de registros logs que se generan diariamente.Ante esto surge la necesidad de las empresas de disponer de un sistema de análisis de la actividad de los sistemas, aplicaciones y equipos en general, cuya información se registra en los ficheros de logs que estos generan.

Es por ello que el análisis y gestión de logs aportan un valor agregado a la seguridad de la información dentro de las organizaciones, según Chuvakin, Schmidt, & Phillips, (2013) esta información analizada y gestionada adecuadamente podría convertirse en una base de datos de incidentes y eventos con utilidad en diversos fines, entre los cuales se encuentran la:

Administración de recursos, detección de intrusiones, la resolución de problemas, análisis forense y auditorías,

además de prevenir comportamientos inadecuados que causen fallas en los sistemas, garantizando la continuidad del negocio. Los métodos científicos que se utilizaron en el presente trabajo son el método deductivo, mediante el cual nos permite realizar un estudio comparativo de las principales metodologías, regulaciones, normas y guías de seguridad consultadas en la bibliografía y herramientas relacionadas con el análisis y gestión de logs, para que en base a los hechos observados nos permitan llegar a una propuesta de una solución. Entre los principales resultados obtenidos a través del desarrollo del presente trabajo de investigación resaltamos los siguientes:

1. Análisis de las metodologías, estándares inmersos en la gestión de logs.
2. Establecimiento de un procedimiento o modelo con los pasos necesarios para el diseño e implementación de la estructura de seguridad para el análisis y gestión de logs.
3. Selección de herramientas en software libre que satisfaga la estructura propuesta.
4. Implementación del modelo propuesto para el análisis y gestión de logs, tomando como caso de prueba ficheros logs del Sistema Académico Tariquia.

PALABRA CLAVE

Seguridad informática, Logs, Sistemas informáticos, Aplicaciones, eventos de seguridad, vulnerabilidad.

ABSTRACT

This study aims to design a model for the implementation of a security structure for the analysis and management of multilayer application logs, with the purpose of processing, analyzing and monitoring the security events that occur daily in the systems. of information and technological devices in general. Today, the vast majority of computer systems and technological devices have mechanisms to generate log records, which contain information about their current status and operation.

Currently companies or organizations that have computer systems handle and process a large amount of information, these systems generate log files, in order to store the types of access, errors and alerts that occur at different levels of its structure.

Thus, in the event of any incident that is occurring, such as attacks of: insertion of malicious code, denial of services or simply a trace of error in the code of a system, these log files are very useful when it comes to facilitating the information to respond and follow up on any security event, currently the review of these log files is an exhaustive process that involves a lot of effort either manually or through software, causing stoppage in the services provided, as well as generating delays and Resource losses when analyzing, searching and identifying what type of event was generated and where in the structure it was generated, given the volume and quantity of logs that are generated daily. Given this, the need arises for companies to have a system for analyzing the activity of systems, applications and equipment in general, whose information is recorded in the log files they generate. That is why log analysis and management contribute an added value to information security within organizations, according to Chuvakin, Schmidt, & Phillips, (2013) this information analyzed and managed properly could become a database of Incidents and events with utility for various purposes, among which are:

Resource management, intrusion detection, problem solving, forensic analysis and audits, as well as preventing inappropriate behaviors that cause system failures, ensuring continuity of the system. deal. The

scientific methods that were used in the present work are the deductive method, by means of which it allows us to carry out a comparative study of the main methodologies, regulations, norms and safety guides consulted in the bibliography and tools related to log analysis and management. , so that based on the observed facts allow us to arrive at a proposal for a solution. Among the main results obtained through the development of this research work we highlight the following:

1. Analysis of methodologies, standards immersed in log management.

2. Establishment of a procedure or prototype with the necessary steps for the design and implementation of the security structure for log analysis and management.

3. Selection of free software tools that satisfy the proposed structure.

4. Implementation of the proposed structure for log analysis and management, taking as a test case log files of the Tariquia Academic System.

KEYWORDS

Computer security, Logs, Computer systems, Applications, security events, vulnerability.

INTRODUCCIÓN

Hoy en día la información es considerada como uno de los activos más valiosos para las organizaciones. Los avances tecnológicos, en especial los que tienen que ver directamente con el manejo y procesamiento de la información han facilitado de forma significativa la labor de las empresas en general, es por ello que ante el crecimiento y desarrollo de las tecnologías de información también son muchas las amenazas a las que una organización debe hacer frente.

Los logs son registros de todos los eventos que ocurren dentro de los sistemas, aplicaciones y redes. Cada entrada en estos archivos contiene información relacionada a un evento específico que ocurrió dentro del sistema o red.

En un entorno TIC la mayoría de elementos son capaces de generar diferentes tipos de logs. Con referencia a Chuvakin, Schmidt, & Phillips, (2013, pág. 32) estos logs se pueden clasificar en:

- **Logs de Seguridad**, que se enfocan en eventos de detección y respuesta ante ataques, infección de código malicioso, robo de datos y otros incidentes de seguridad.
- **Logs de Operaciones**, que se produce para proveer información útil respecto a la ejecución de tareas y procesos en los sistemas.
- **Logs de Depuración de Aplicaciones**, este tipo especifico de logs se utiliza por programadores en ambientes de desarrollo (aunque su empleo no se recomienda también se pueden habilitar en ambientes de producción) para la verificación de la funcionalidad de la aplicación evaluada.

Una **aplicación multicapa** generalmente es un sistema de información que está organizado en varias capas, cada una de las cuales contiene un conjunto de clases con responsabilidades relacionadas con la capa a la que pertenecen.

Según Pamplona, (2018) las arquitecturas más comunes generalmente, se adopta una arquitectura para cada sistema de información, en función de sus ventajas e inconvenientes.Las arquitecturas más universales son: **Monolítica**, **Cliente-servidor, Arquitectura de tres niveles**.

Actualmente podríamos afirmar que la mayoría de los medios tecnológicos, generan ficheros logs, en donde

podemos encontrar todos los registros sobre la actividad y funcionamiento de los mismos, como ser un dispositivo de una red de datos, de un software o sistemas de información, bases de datos, servidores web, y aplicaciones en general.

Parte importante de la implementación y mantenimiento de los sistemas de información es el análisis del funcionamiento y estado actual de los sistemas.

Este análisis es importante para conocer y verificar la integridad de los servidores y el rendimiento de los equipos, para detectar fallas en el hardware y software, además de descubrir comportamientos que afecten la funcionalidad de las aplicaciones para luego tomar decisiones que mejoren la productividad y calidad de los servicios brindados.

Es por ello donde se denota la importancia de contar con sistemas capaces de analizar y procesar estos datos y ofrecer resultados en tiempo real de manera eficiente, que ofrezcan una visión clara y precisa de lo que está sucediendo, facilitándonos de gran manera la detección temprana de errores, debilidades, vulnerabilidades y ataques a los Sistemas de Información.

MATERIALES Y MÉTODOS

Los métodos científicos que se utilizaron en el presente trabajo son el método deductivo.

En cuanto a las técnicas e instrumentos que se utilizaron en este proyecto de investigación, son un análisis comparativo y documental, dado que se trabaja a partir de los datos que surgen de la indagación de diferentes normas, regulaciones y herramientas referentes al análisis y gestión de logs, y la observación en el proceso de la implementación del caso de prueba.

En cuanto a las metodologías para la gestión de logs existen una gran cantidad de normas y leyes, incluidas en PCI DSS, FISMA, CAG, GPG13 entre otras y marcos de mejores prácticas, como la NIST 800-92 e ISO2702.

A continuación, se describen algunas de las regulaciones y cómo éstas se relacionan con los logs, el análisis de logs, y la gestión de logs.

ISO/IEC 27002

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. (El portal de ISO 27001 en Español, 2012). Para este trabajo de investigación se tomó en cuenta el control, **A.12.4 Registros y monitoreo de Logs,** citado a continuación:

El Anexo **A** dé **(ISO/IEC 27002:2013)** tiene la subsección **A.12.4** Registro y monitoreo, para ayudarnos a manejar la mayoría de los problemas que se presentan en la gestión de logs:

- **12.4.1 Eventos y logs:** Registra información sobre acceso y acciones de usuarios, errores, eventos, etc. en sistemas de información. En este caso, si tiene múltiples aplicaciones, puede ser interesante enviar los logs generados por cada uno a un servidor central. Para ello, puede configurar un servidor syslog (syslog es un estándar para el registro de mensajes y puede operar en una red con una estructura de aplicación cliente-servidor), que básicamente le permitirá centralizar todos los logs en un servidor único.
- **12.4.2 Protección de la información de logs:** Los log deben estar protegidos, ya que no pueden

ser eliminados o modificados por personas no autorizadas. En general, cuando un atacante obtiene acceso a un sistema no autorizado, él elimina toda la información generada en los logs, para eliminar la evidencia de cualquier acción que haya llevado a cabo. Por lo tanto, debe establecer las reglas que permitan la modificación de estos registros solo por ciertas personas y, por otro lado, obviamente, las medidas de control de acceso del sistema deben fortalecerse.

- **12.4.3 Logs de administrador y operador:** los privilegios de los administradores y operadores de sistemas son diferentes de los privilegios de usuario normales, lo que significa que pueden realizar más acciones en los sistemas. En algunos casos, dicha actividad por defecto no se registra, y eso es un error porque si un atacante obtiene acceso a un sistema no autorizado, probablemente intente adquirir permisos de administrador y realice todas las acciones con los derechos de usuario de este administrador. Por lo tanto, los sistemas deberían registrar información sobre todos los usuarios, independientemente de los privilegios que tienen en los sistemas.

- **12.4.4 Sincronización del reloj:** Todos los sistemas deben configurarse con la misma hora y fecha; de lo contrario, si ocurre un incidente y queremos llevar a cabo una prueba de trazabilidad de lo que ha sucedido en los diferentes sistemas involucrados, puede ser difícil si cada uno tiene una configuración diferente. Por lo tanto, el escenario ideal sería que los sistemas tengan un tiempo sincronizado, y esto se puede lograr de manera automatizada con servidores de tiempo (conocidos técnicamente como servidores NTP, donde "NTP" significa un protocolo de Internet para la sincronización de relojes de sistemas).

PCI DSS

Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial.bre Normas de Seguridad de la PCI & LLC, 2016)

Para este trabajo de investigación se tomo en cuenta las siguientes tareas relacionadas con la gestión de logs, citados a continuación:

Activación de los registros (logs) de auditoria, Configuración de los datos a ser registrados, Protección de los registros de eventos.

NIST 800-92.

Guía para la gestión de registros de seguridad informática.

Para la realización de este proyecto de investigación se tomó como base la presente guía para la gestión de logs el cual nos traza los pasos necesarios para diseñar e implementar una estructura de gestión de logs, el cual describirnos a continuación:

El Instituto Nacional de Estándares y Tecnología (NIST) desarrolló este documento en cumplimiento de sus responsabilidades legales bajo la Ley Federal de Administración de Seguridad de la Información (FISMA) de 2002, Ley Pública 107-347, esta guía ha sido preparada para su uso para las agencias federales. (IBM, 2018)

La guía comienza con una introducción a la administración de logs de seguridad informática y sigue con tres secciones principales:

- Infraestructura de gestión de logs.
- Planificación de gestión de logs.
- Procesos operacionales de gestión de logs.

De hecho, esta es la forma correcta de pensar en cualquier proyecto de gestión de logs desde las organizaciones generalmente tienen desafíos con la planificación, la arquitectura de logs construcción, y luego con la

operación en curso, que debe mantenerse para siempre que la organización exista.

Kent & Souppaya, (2014) proporciona una visión general de alto nivel y orientación para la planificación, el desarrollo y la implementación de una estrategia efectiva de gestión de logs de seguridad en la cual define una infraestructura de gestión de logs como la que tiene cuatro funciones principales:

- **Generación**: análisis de logs, filtrado de eventos y agregación de eventos.
- **Almacenamiento de logs:** rotación, archivo, compresión, reducción, normalización, comprobación de integridad;
- **Log Análisis**: correlación de eventos, visualización e informes.

Eliminación – limpieza.

Además, aborda los siguientes desafíos de administración de logs de seguridad:

- Establecer políticas y procedimientos para la gestión de logs.
- Priorizar la gestión de logs de forma adecuada en toda la organización.
- Crear y mantener una infraestructura de gestión de logs.
- Proporcionar el soporte adecuado para todo el personal con responsabilidades de gestión de logs.
- Establecer procesos operativos de gestión de logs estándar.

FISMA

Es una ley federal diseñada para las agencias federales que abarca la Gestión de la Seguridad de la Información de 2002 (FISMA), De acuerdo con la ley, la guía detallada ha sido desarrollada por NIST para cubrir los detalles del cumplimiento de FISMA. (Chuvakin, Schmidt, & Phillips, 2013, pág. 362)

- A continuación, se detalla la guía FISMA / NIST en elementos accionables que se pueden implementar y mantener:
- La política de logs es lo primero. Pero no significa nada sin procedimientos operativos que se desarrollan base y política y luego poner en practica. (NIST, 2014)
- Esto probablemente requerirá cambios de configuración a múltiples tipos de sistemas; actualizaciones a los estándares de configuración prescritos en otra parte del documento están en orden. (NIST, 2014)
- En función de la política, defina qué evento se registrará y qué se generarán y registraran detalles para cada evento (AU-3). Comience el registro según. (NIST, 2014).
- Considere registrar toda la conectividad de salida para detectar la ex filtración de datos (Asegúrese de que las sesiones de acceso de usuario estén registradas. (NIST, 2014)
- Defina los métodos de almacenamiento de logs y los tiempos de retención y retener los registros generados. (NIST, 2014)
- Proteger los registros de los cambios, mantener el tiempo preciso para preservar la evidencia de los logs. (NIST, 2014)
- También de acuerdo con la política, implementar procedimientos de revisión de logs e informe de generación. Distribuir informes a las partes que deberían ver la información (también según la política creada en el ítem 1). (NIST, 2014).

RESULTADOS :A continuación, se expone los principales resultados obtenidos en la investigación detallados en los siguientes puntos.

Para la realización del modelo de la estructura de seguridad para el análisis y gestión de logs de aplicaciones informáticas, se tomó como base las actividades propuestas en la guía NIST SP800-92, complementandolo con algunas de las actividades con la norma ISO 27002, PCI, FISMA y la guía de gestion de logs de Chuvakin, Schmidt, & Phillips, (2013), de los cuáles se extraen las tareas y criterios necesarios para la gestión de logs.

Según el análisis de las normas y/o regulaciones, las etapas para el diseño e implementación de la estructura para el análisis gestión de logs debe estar conformado por las siguientes etapas, ***Planeación, Diseño, Selección de Herramientas e Implementación.***

I. Etapa de Planeación.

En esta etapa de planificación se complementó con la guía (Logging and Log Management), FISMA en donde se definen los criterios necesarios para el diseño de la estructura.

- Definir roles y responsabilidades.
- Definir fuentes generadoras de logs.
- Establecer Políticas y Procedimientos de logs para la; Generación de logs, Transmisión de logs, Análisis de logs, Establecer políticas alcanzables, Seguimiento de políticas, Hacer referencia a normas y regulaciones.
- Diseño de la infraestructura de gestión de logs.

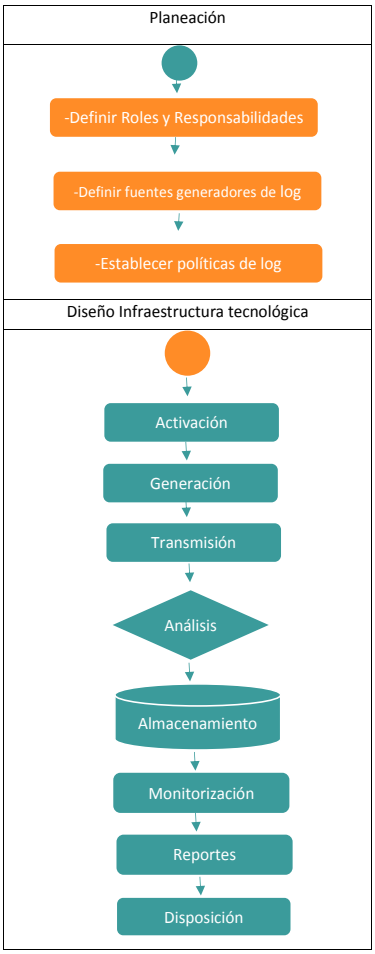
II. Etapa de Diseño de la infraestructura tecnológica

Las actividades para la etapa de diseño se complementaron con la norma ISO 27002 12.4, EMC-RSA, PCI y la guía (Logging and Log Management) en donde se debe adecuar una infraestructura tecnológica para la gestión centralizada de logs de acuerdo a las siguientes actividades.

- Activación de logs.
- Generación de logs.
- Transmisión de logs.
- Análisis de logs.
- Almacenamiento de logs.
- Monitorización.
- Generación de reportes.
- Mitigación de incidentes.
- Disposición de logs.
- Seguridad del registro de logs.

De acuerdo a las etapas de ***planeación*** y ***diseño*** anteriormente descritas la **Estructura de seguridad para el análisis y gestión de logs de aplicaciones informáticas con arquitectura multicapa queda de la siguiente manera:**

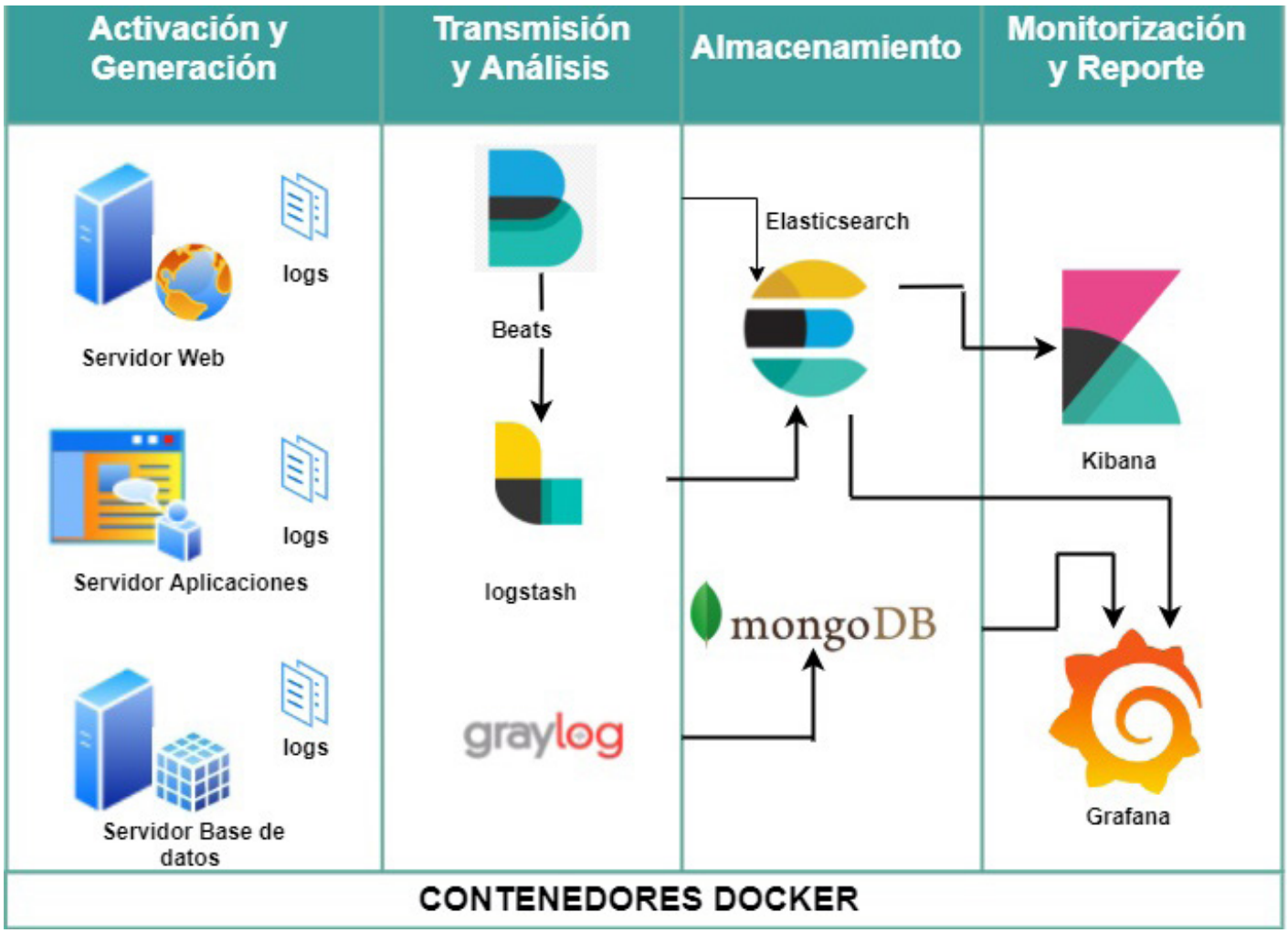
Figura 1. Estructura de seguridad para el análisis y gestión de logs.



III. Selección de herramientas en software libre en base a la estructura propuesta.

A la hora de seleccionar herramientas se tiene en cuenta las etapas de infraestructura de gestión de logs según la NITS y el diseño de la estructura tecnológica definida en el anterior punto.

Figura 2.
Estructura Tecnológica para la gestión y análisis de logs



A continuación, se describe las herramientas para la implementación de la estructura tecnológica, tomando en cuenta que existen otras soluciones y que las herramientas seleccionados para cada fase son opcionales y están sujetas a requerimientos en cuanto capacidad y disponibilidad de recursos para su instalación y puesta en marcha.

• **Docker**. Es un proyecto de código abierto que automatiza el despliegue de aplicaciones dentro de contenedores de software, proporcionando una capa adicional de abstracción y automatización de virtualización de aplicaciones en múltiples sistemas operativos.

- **Graylog**. Se trata de uno de los productos de gestión de logs más completos existentes en el mercado, ya que ofrece funcionalidades de monitorización, además del análisis y almacenamiento de mensajes. Para la recepción y el análisis cuenta con un servidor desarrollado en Java, mientras que para labores de monitorización ofrece una aplicación web escrita en Ruby que permite visualizar los mensajes y la actividad del servidor. (Graylog, 2018).

➤ Beats.Los Beats son agentes ligeros que se integran en las aplicaciones o servicios que tenemos y que mandan todo tipo de información hacía Logstash o Elasticsearch. Hay varios Beats ya disponibles como son: ***Filebeats, Metricsbeats, Packetbeat, Network Data,Winlogbeat, Auditbeat, Heartbeat (Elasticsearch, 2018).***

➤ ***Logstash*** Es una fuente de procesamiento de datos de fuente abierta, del lado del servidor que ingiere datos de una multitud de fuentes simultáneamente, las transforma y luego las envía a su "alijo" favorito (nuestra es Elasticsearch, naturalmente). (Elasticsearch, 2018)

➤ ***Elasticsearch.*** Es un motor de búsqueda basado en Apache Lucene que permite indexar grandes cantidades de datos para su posterior consulta de forma eficiente. Los datos o documentos que se indexan no necesitan tener una estructura determinada, aunque para un mejor funcionamiento y explotación de los mismos es recomendable su definición. (Canto, 2016)

➤ ***MongoDB.*** Es una base de datos orientada a documentos. Esto quiere decir que, en lugar de guardar los datos en registros, guarda los datos en documentos. Estos documentos son almacenados en BSON, que es una representación binaria de JSON.

➤ ***Kibana*** te permite visualizar tus datos de Elasticsearch y navegar por Elastic Stack, de modo que puedes hacer cualquier cosa, desde saber por qué te están bus cando a las 2:00 a.m. hasta comprender el impacto que la lluvia puede tener en tus números trimestrales. (Elasticsearch, 2018)

➤ ***Grafana***. Es una herramienta de código abierto para el análisis y visualización de métricas. Se utiliza frecuentemente para visualizar de una forma elegante series de datos en el análisis de infraestructuras y aplicaciones.

➤ Implementación de la estructura de seguridad tomando como caso de prueba logs del sistema académico Tariquia.

- Como caso de prueba tomaremos el Sistema Académico Tariquia de la Universidad Autónoma Juan Misael Saracho, el cual es un sistema que maneja información crítica en el desarrollo de las actividades y operaciones diarias de la UAJMS, el sistema académico Tariquia está compuesto por una infraestructura de aplicaciones que interactúan entre sí, los cuales generan logs en los distintos niveles como ser: logs de servidores web, logs de servidores de aplicaciones y logs de los servidores de base de datos.

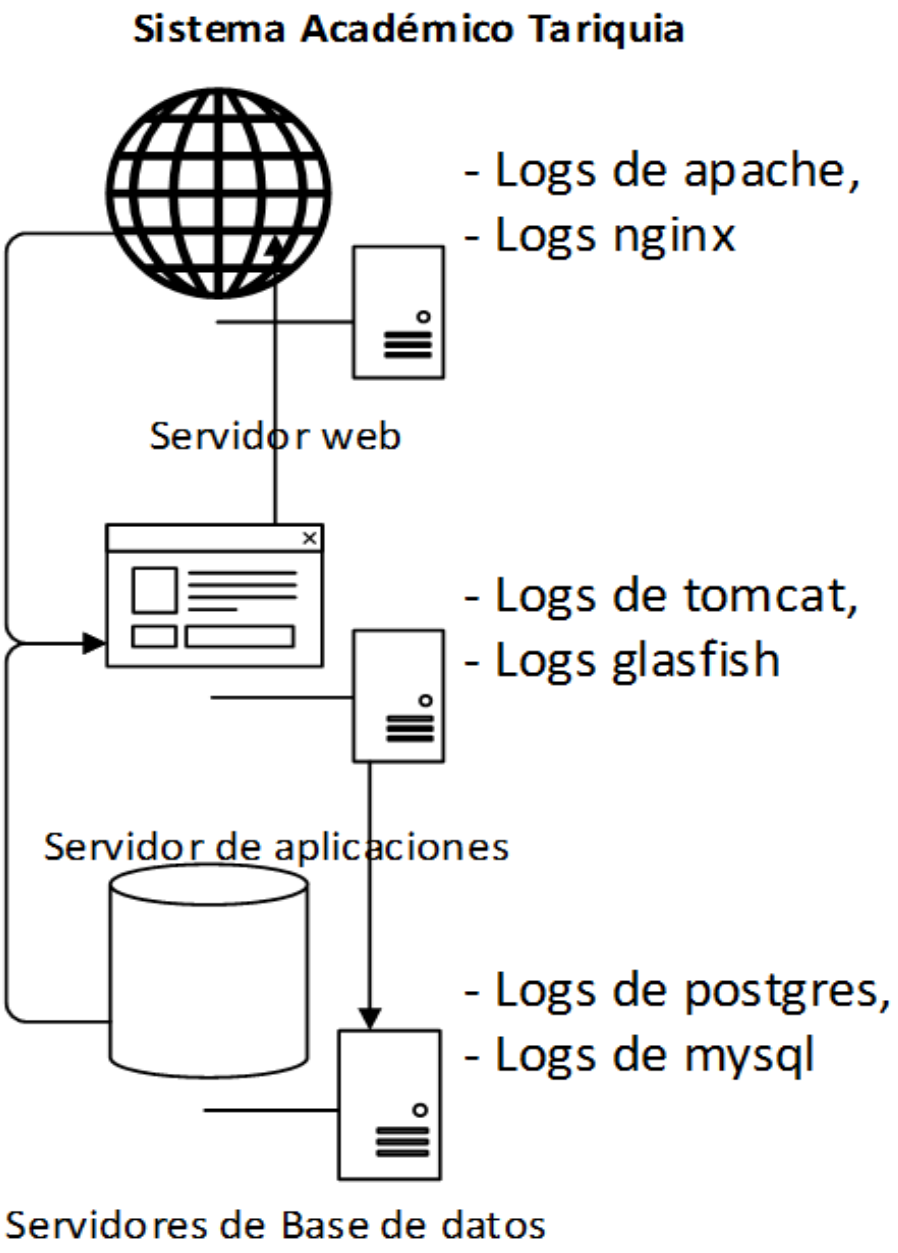
Las actividades que tomaremos en cuenta para la implementación de la estructura propuesta son las siguientes:

De las actividades descritas anteriormente a continuación, se realiza el análisis y el desglose de los pasos propuestos.

Definición de roles y responsabilidades

Se debe definir las responsabilidades dentro del proceso de gestión de logs, para que la gestión sea adecuada, se identifiquen las actividades de cada rol con respecto a los logs y definir las personas que se encuentran involucradas en el proceso.

Figura 3.
Estructura multicapa del Sistema Académico Tariquia



Fuente: Elaboración propia.

Tabla 1.
Definición de roles y responsabilidades, caso de prueba.

Roles según la NITS	Roles UAJMS	Responsabilidades según la NITS
Administradores de sistemas y redes	Jefe de sistemas de información, jefe de comunicación y mantenimiento de servicios, administradores de sistemas, administradores de bases de datos	Generalmente son los responsables de la configuración y activación de logs en las aplicaciones y dispositivos de red, además que deben ser los responsables en la administración y mantenimientos de los registros logs,
Administradores de seguridad	Jefe de sistemas, jefe de comunicación y mantenimiento, jefe de contenidos virtuales.	Son los responsables del seguimiento y monitorización de los registros logs
Equipos de respuesta a incidentes de seguridad informática	Técnicos analistas y programadores, técnicos de comunicación y mantenimiento	Encargados de usar datos de logs para manejar algunos incidentes que suscitan a diario
Desarrolladores de aplicaciones	Técnicos analistas y programadores	Encargados de configurar la generación de logs en el proceso de desarrollo de aplicaciones en general.

Fuente: Elaboración propia.

Según las actividades descritas en la Etapa I, a continuación, se realizó el análisis y el desglose de los pasos propuestos.

a. Definición de roles y responsabilidades.

Como se evidencia en la **Tabla 1,** se definió las responsabilidades dentro del proceso de gestión de logs, para que se identifiquen las actividades de cada rol con respecto a la gestión de logs, además se definió las personas que se encuentran involucradas en el proceso.

b. Definición de fuentes generadoras de logs.

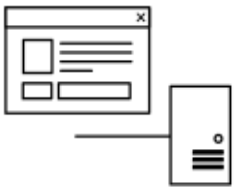
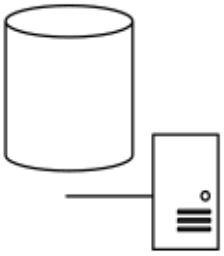
A continuación, como se evidencia en la Tabla 2, se definió las fuentes generadoras de logs de acuerdo al funcionamiento de la arquitectura del sistema Tariquia.

c. Establecer políticas de logs.

En esta fase la unidad encargada de la infraestructura TI debe definir políticas para el análisis gestión de logs en

Tabla 2.

Fuentes generadoras de logs, caso de prueba.

Origen	Fuentes generadoras de logs	Descripción
 Servidor web	Servidor Apache Servidor Nginx	Logs de accesos Logs de errores
 Servidor de aplicaciones	Tomcat	Log de accesos Log de errores
 Servidores de Base de datos	Postgres	Log de errores

Fuente: Elaboración propia.

todas sus etapas, así de esta manera se norma el funcionamiento y procedimiento de la misma, para el caso de prueba se definió las siguientes políticas de manera práctica:

El área de sistemas de la información está encargada de asegurar la activación y generación además del análisis y gestión de logs de seguridad de los sistemas de la organización, garantizando su continuidad, seguridad y reducción de posibles incidentes en procesos estratégicos de la organización.

La responsabilidad de la gestión de logs es del ingeniero de seguridad de la organización quien debe asegurar la operación, monitoreo, respuesta de incidentes y fallas además de la actualización del proceso de gestión de logs.

Se deben asegurar la generación de logs de auditoria y de seguridad en los sistemas críticos para los procesos de la organización.

Los responsables de los logs serán los técnicos analistas que tienen actividades de administradores y desarrolladores de cada uno de los sistemas, quienes tendrán que asegurar la activación, generación y transmisión de los mismos, además de definir y filtrar los tipos de logs de mayor impacto en sus sistemas para su análisis posterior.

d. Diseño de la infraestructura de gestión de logs.

Se deben disponer de todos los recursos tecnológicos necesarios para implementar y mantener una estructura de seguridad de análisis y gestión de logs, además toda infraestructura para la gestión de logs debe involucrar mínimamente los siguientes puntos:

➢ **Activación de logs.**

Se deben identificar las aplicaciones que manejan información crítica, que formarán parte del proceso de análisis y gestión de logs.

➢ **Almacenamiento de logs.**

Se deben establecer medios de resguardo y respaldo de los ficheros logs generados.

➢ **Retención de logs.**

Se deben establecer criterios de almacenamiento de los ficheros logs en la base de datos de tal mantener y priorizar los recursos consumidos.

➢ **Seguridad de logs.**

Se deben establecer técnicas y procedimientos que garanticen la disponibilidad e integridad de los ficheros logs, de tal manera que los registros almacenados sean fiables a la hora de realizar un análisis.

➢ **Monitoreo de logs.**

Se deben establecer criterios de monitoreo, en cuanto a que información visualizar, cuadros de mando, tablas, gráficos, que estén disponibles en tiempo real y también de manera histórica, además de definir un tipo de visualización por roles.

➢ **Disposición de logs.**

Se debe establecer criterios de eliminación de los logs, en cuanto a información histórica obsoleta, además de establecer técnicas automatizadas para la eliminación de los mismos.

A continuación, se realizó la implementación de la estructura tecnológica para la gestión de logs en base a las actividades y procesos descritos, en la Etapa II y Etapa III, diseño y selección de herramientas.

e. Implementación de la infraestructura tecnológica.

En esta etapa se realizó la implementación de la estructura en base a las actividades y procesos establecidos en el diseño y selección de herramientas.

1. Para lo cual necesitaremos las siguientes herramientas:

- **DockerPara MacOS**
- **OS X Catalina 10.11 o una versión más nue va de macOS ejecutándose en una Mac 2010 o posterior, con el soporte de hardware de In tel para la virtualización MMU.**
- **Al menos 4 GB de RAM.**
- **Imágenes Docker.**
    - Imagen de Elasticsearch
    - Imagen de Beats
    - Imagen de Logstash
    - Imagen de Kibana comando
    - Imagen Grafana

2. Una vez descargadas las imágenes, se realizó con las configuraciones de los **contenedores**, tomando como base el proyecto **docker-compose** compartido en el repositorio **github**, el cual permite adecuar las configuraciones a nuestras necesidades.

2.1. Docker Compose. Es una herramienta que permite simplificar el uso de Docker, generando scripts que facilitan el diseño y la construcción de servicios. Docker Compose, por defecto, busca instrucciones en el archivo docker-compose.yml.

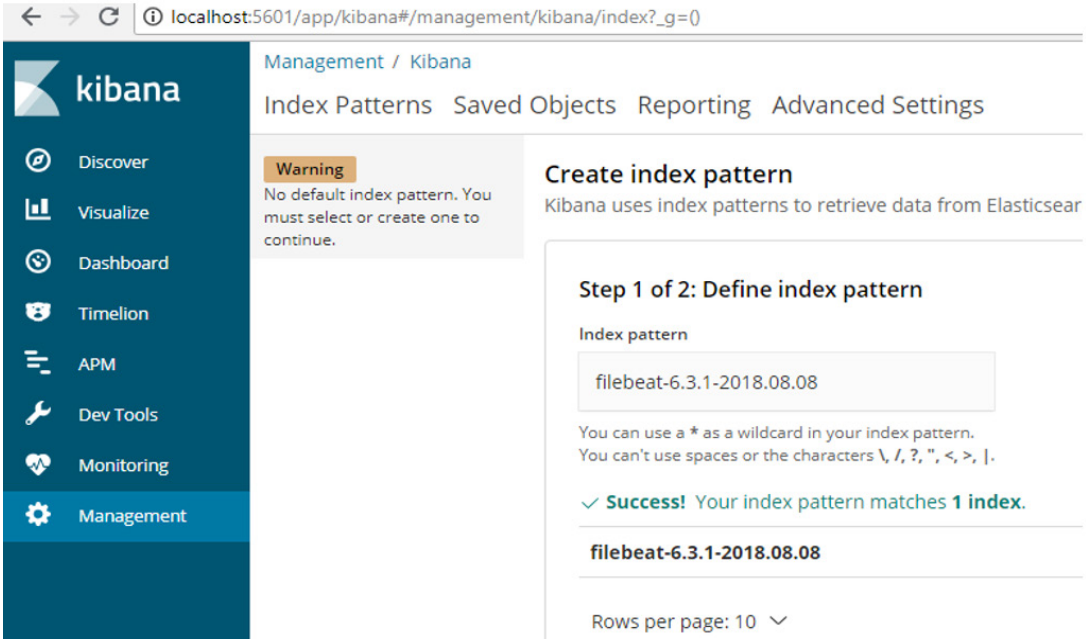
3. Como se precia en la **Figura 3,** una vez configurado el archivo docker-compose.yml se procedió ejecutar el archivo con el siguiente *comando*:

Figura 3.
Ejecutando docker-compose.yml

```
$ docker-compose -f docker-compose.yml up
Starting dockerelkmaster_elasticsearch_1 ... done
Starting dockerelkmaster_kibana_1        ... done
Starting dockerelkmaster_logstash_1      ... done
Attaching to dockerelkmaster_elasticsearch_1, doc
```

Comando:
$ docker-compose -f docker-compose.yml up

Figura 4.
Creando índices en kibana



En la **Figura 4**, se aprecia como se procedió a configurar los índices de Elasticsearch a través de Kibana los cuáles combinados poseen características y funcionalidades que nos permite utilizar y trabajar con grandes cantidades de datos, facilitándonos el manejo de búsquedas, filtros, creación de gráficos, entre otras funcionalidades.

En la **Figura 5,** se puede apreciar un cuadro de mando o Dashboard en tiempo real de los registros logs, el cual gracias Beats y Logstash que van recolectando y filtrando los ficheros logs, haciendo que el seguimiento a estos registros sea aun mas efectivo, cabe aclarar que kibana posee muchos cuadros y métricas permitiendo crear Dashboards personalizados que se ajusten a nuestras necesidades.

Figura 5. Dashboards de monitorización y seguimiento en tiempo real

DISCUSIÓN

Entre los principales resultados obtenidos en la investigación se pudo constatar lo siguiente:

Por medio de las metodologías, regulaciones y guías de buenas prácticas relacionadas en la gestión de logs, se procedió a determinar los pasos y actividades necesarias para el diseño e implementación de una estructura de seguridad para el análisis y gestión de logs, sin embargo, es importante aclarar que existen otras metodologías que se pueden ajustar a distintas necesidades, de las cuales también se pueden obtener otros criterios a la hora de diseñar una estructura para la gestión de logs.

Con el diseño de la estructura para el análisis y gestión de logs, el número de fuentes generadoras de logs varía según el tamaño y estructura tecnológica de cada organización, esto hace que los datos procesados requieran una distinta planificación para la asignación de recursos, debido a esto es importante establecer políticas para el diseño e implementación de la infraestructura tecnológica, con el fin de contar siempre con los recursos necesarios para cumplir los objetivos del proceso, por tal motivo cada organización debe establecer sus propias políticas de acuerdo a su realidad.

Con relación a las herramientas seleccionadas se ha procedido a evidenciar que cumplen con los criterios mínimos para el análisis y gestión de logs, facilitándonos de gran manera el seguimiento, el monitoreo en tiempo real, visualizaciones por tipo de rol, reportes gráficos, estadísticas, entre otras funcionalidades.

Cabe aclarar que algunas de las Herramientas de uso libre poseen limitaciones que son evidentes en organizaciones con infraestructura tecnológica más grandes, debido a la cantidad de recursos que son necesarios para el análisis y gestión de logs, además de temas como almacenamiento y seguridad.

En relación a la implementación del caso de prueba se logró obtener los siguientes resultados:

Mantener un control centralizado de los archivos logs generados por las aplicaciones informáticas multicapa: servidor de aplicaciones, servidor de base de datos.

Tener control centralizado de los incidentes registrados en los servidores asociados a los sistemas de información.

Mantener un análisis en tiempo real de la infraestructura de las aplicaciones informáticas y los servicios ejecutados.

Priorizar los eventos recibidos de vulnerabilidades y errores en las aplicaciones.

Presentar reportes gráficos de los diferentes eventos que suceden en las aplicaciones: servidor de aplicaciones, servidor de base de datos, como también las conexiones entrantes.

Los resultados obtenidos coinciden con el estudio de (David, Fabio, & Cristian, 2015), cuyos resultados permite afirmar que el análisis y gestión de logs colaboran en la toma de acciones y decisiones preventivas y correctivas de ámbito técnico, tecnológico y seguridad de la información, que busca reducir las vulnerabilidades de las tecnologías de la información en las instituciones.

Por otra parte, (Carrión Ramírez, 2015), con su trabajo de investigación denominado: "Diseño e Implementación de una solución de gestión centralizada de logs de aplicaciones", Confirma la existencia de una enorme cantidad de información potencialmente relevante para la seguridad de una organización, y la importancia de filtrar y procesar los logs recolectados desde las fuentes generadoras proporcionada por LogStash que permite descartar una enorme cantidad de información irrelevante con relación a los objetivos específicos planteados en la

política de gestión de logs.

En cuanto a las herramientas y la metodología para la gestión de logs (Alegre Diez, 2016) argumenta que estas aportan, decisiones más rápidas, decisiones más inteligentes, análisis de datos predictivos, además de un control en tiempo real sobre algún evento o incidente de seguridad.

Finalmente, entre algunas recomendaciones tenemos:

Es necesario establecer formatos de logs para las distintas fuentes generadoras de logs con el fin de estandarizar, y facilitar el procesamiento y análisis de los mismos.

Al momento de implantar una solución para el análisis y gestión de logs es necesario considerar un modelo o metodología de referencia estándar; sin embargo, se constató que el elemento fundamental, y por consiguiente más problemático, se encuentra en la definición de una política global para cada organización para el análisis y gestión de logs.

BIBLIOGRAFÍA

- Vieda, M. (6 de junio de 2013). Manuel Vieda Software Engineer. Obtenido de Manuel Vieda Software Engineer: https://manuelvieda.com/blog/administracion-de-logs/
- Universidad, B. (mayo de 2018). ESTATUTO ORGÁNICO, REGLAMENTOS Y DISPOSICIONES DE LA UNIVERSIDAD BOLIVIANA, APROBADOS EN EL X CONGRESO NACIONAL DE UNIVERSIDADES. La Paz. Obtenido de UMSA: http://portal.faadu.edu.bo/faadu/images/FAADU/Docs/a01_estatuto_universidad_boliviana.pdf
- Stackify. (26 de mayo de 2017). Best Log Management Tools: 51 Useful Tools for Log Management, Monitoring, Analytics, and More. enido de https://stackify.com/best-log-management-tools/
- Society, T. I. (2001). The BSD syslog Protocol. Obtenido de The BSD syslog Protocol: https://www.ietf.org/rfc/rfc3164.txt
- Shenk, J. (3 de noviembre de 2018). SANS Institute. Obtenido de SANS Institute: https://www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012-log-event-management-survey-results-sorting-noise-35230
- Secretaria de Desarrollo, U. (2009). MANUAL DE ORGANIZACIÓN Y FUNCIONES. tarija.
- SANS Institute InfoSec Reading Room. (octubre de 2014). Ninth Log Management Survey Report. Obtenido de https://www.sans.org/reading-room/whitepapers/analyst/ninth-log-management-survey-report-35497
- SANS Institute. (2014). Ninth Log Management Survey Report. Log Management Survey. Obtenido de SANS Institute.
- NIST. (2014). National Institute of Standards and Technology. Obtenido de National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r3.pdf
- Laboratory Information Technology. (2006). Guide to Computer Security Log Management.
- ISO/IEC 27002:2013. (octubre de 2013). iso2700.es. Obtenido de iso2700.es: http://www.iso27000.es/download/ControlesISO27002-2013.pdf
- ISO tools. (19 de marzo de 2015). ISO tools. Obtenido de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA: https://www.isotools.

org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

☛ Graylog, I. (3 de julio de 2018). Graylog. Obtenido de Enterprise Log Management for All: https://www.graylog.org/

☛ grafana. (4 de julio de 2018). grafana labs. Obtenido de https://grafana.com/.

☛ Gracia, L. L. (31 de julio de 2018). un poco de java. Obtenido de https://unpocodejava.com/2013/07/30/que-es-kibana/

☛ EMC-RSA. (2018). EMC-RSA Envision. Obtenido de EMC-RSA Envision: http://www.eircomictdirect.ie/docs/rsa/envision-wp.pdf

☛ Elasticsearch. (2018). elastic. Obtenido de elastic: https://www.elastic.co/elk-stack

☛ elasticsearch. (2018). elastic. Obtenido de logstash: https://www.elastic.co/products/logstash

☛ Docker Inc. (6 de julio de 2018). docker. Obtenido de https://www.docker.com/

☛ Couto, J. A. (2 de agosto de 2014). MongoDB: Características y futuro. Obtenido de http://juanroy.es/es/mongodb-caracteristicas-y-futuro/

☛ Consejo sobre Normas de Seguridad de la PCI, & LLC. (abril de 2016). Industria de tarjetas de pago (PCI). Obtenido de Industria de tarjetas de pago (PCI): https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2_es-LA.pdf

☛ conogasi.org. (2 de septiembre de 2018). conogasi. Obtenido de conogasi.org/articulos/clasificacion-de-software-de-sistemas-y-aplicaciones/

☛ CIS. (29 de julio de 2018). Twenty Critical Controls for Effective Cyber Defense. Obtenido de Consensus Audit Guidelines: https://www.sans.org/critical-security-controls/

☛ Chuvakin, D., Schmidt, K., & Phillips, C. (2013). Logging and Log Management - The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. USA: Elsevier.

☛ Carrión Ramírez, B. (2015). Diseño e Implementación de una solución de gestion centralizada de logs de aplicaciones, sistemas y dispositivos basada en Logstash que permita la creación de cuadros de mando para explorar, analizar y monitorear eventos de seguridad.

☛ Canto, D. M. (febrero de 2016). damarcant. Obtenido de ELK Stack (I): indexación de documentos con Elasticsearch: http://damarcant.blogspot.com/2016/02/elk-stack-i-indexacion-de-documentos-con-elasticsearch.html

☛ Big Data International Campus. (2018). Big Data Blog. Obtenido de Big Data Blog: http://www.campusbigdata.com/big-data-blog/item/82-data-mining-vs-big-data

☛ Amoedo, D. (23 de mayo de 2018). Ubunlog. Obtenido de Grafana, un software de código abierto para análisis y supervisión: https://ubunlog.com/grafana-software-analisis-supervision/

☛ Adame Lorite, J. (2 de octubre de 2012). Bytes & Chips. Obtenido de Bytes & Chips: https://bytesandchips.net/2012/10/02/consejos-y-buenas-practicas-del-logging-de-aplicaciones/

☛ Acosta, J. (10 de octubre de 2017). Openwebinar. Obtenido de https://openwebinars.net/blog/que-es-elk-elasticsearch-logstash-y-kibana/

☛ AccelOps. (2013). Good Practice Guide (GPG13). Obtenido de http://www.infosecurityeurope.com/__novadocuments/48577?v=635304353883700000

☛ El portal de ISO 27001 en Español. (2012). Obtenido de El portal de ISO 27001 en Español: http://

www.iso27000.es/iso27000.html

☛ ArcSight SIEM. (2018). Obtenido de http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/index.html

☛ Apache http server project. (2018). Obtenido de Apache http server project: http://httpd.apache.org/docs/current/logs.html

☛ alienvault. (31 de julio de 2018). Obtenido de https://www.alienvault.com/.

☛ Kent, K., & Souppaya, M. (2014). Guide to Computer Security Log Management". Gaithersburg,: National Institute of Standards and Technology.

☛ David, J., Fabio, L., & Cristian, A. (2015). GUÍA METODOLÓGICA PARA LA GESTIÓN CENTRALIZADA DE REGISTROS DE SEGURIDAD A TRAVÉS DE UN SIEM. Bogota: UNIVERSIDAD CATÓLICA DE COLOMBIA.

☛ Alegre Diez, B. A. (2016). Gestion de logs. Universidad Internacional de la Rioja.