ARTÍCULO 8

Recibido: 5/5/2022
Aprobado: 6/6/2022

Modelo de actividades para la gestión de logs de sistemas de información

Model of activities for the management of logs of systems

Víctor Hugo Figueroa Fernández [1]

[1] *Ingeniero Informático, Docente en la Facultad de Ciencias y Tecnología. Universidad Autónoma Juan Misael Saracho. Tarija – Bolivia.*

Correspondencia del autor(es): figo37vic@gmail.com [1].

Resumen

Hoy en día la mayoría de los sistemas de información poseen mecanismos para generar ficheros logs en todos sus niveles, como ser base de datos, aplicaciones y servidores.El presente estudio tiene como objetivo diseñar un modelo de actividades para la gestión de logs de los sistemas de información, que permita gestionar los datos que se generan, con el fin contar información accesible para identificar los diferentes eventos que se suscitan a diario.Parte importante de la implementación y mantenimiento de los sistemas de Información en una organización es el de garantizar el correcto funcionamiento de los distintos sistemas y servicios que proveen, por esto es importante contar con un mecanismo que gestione los datos e información de los diferentes ficheros logs con el fin de realizar un análisis que permita prevenir, identificar y prever acciones relacionadas con la seguridad de la información.

Los métodos científicos que se utilizaron en el presente trabajo son el método deductivo, además del estudio de documentos y/o normas, regulaciones relacionadas con la gestión de logs.Entre los principales resultados obtenidos de la presente investigación se tienen los siguientes: Análisis y comparación de las normas y/o regulaciones relacionadas con la gestión de logs y el Diseño de un modelo de actividades para la gestión de logs de los sistemas de información.

Palabras clave: Seguridad informática, Modelo, Gestión, Logs, Sistemas Información.

Abstract

Today most information systems have mechanisms to generate log files at all levels, such as databases, applications and servers.

The objective of this study is to design a model of activities for the management of logs of information systems, which allows managing the data that is generated, in order to have accessible information to identify the different events that occur daily.

An important part of the implementation and maintenance of information systems in an organization is to guarantee the correct functioning of the different systems and services they provide, for this reason it is important to have a mechanism that manages the data and information of the different log files. in order to carry out an analysis that allows to prevent, identify and anticipate actions related to information security.

The scientific methods used in this work are the deductive method, in addition to the study of documents and/or standards, regulations related to log management.

Among the main results obtained from this research are the following: Analysis and comparison of the standards and/or regulations related to log management and the Design of a model of activities for the management of information system logs.

Key words: Computer security, Model, Management, Logs, Information Systems.

1. Introducción

Hoy en día con 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 organizaciones en general, es por ello que ante el crecimiento y desarrollo de las tecnologías de información también son más las amenazas a las que una organización debe hacer frente.

Según (Chuvakin, et al., 2013, p. 37) un log es un mensaje de algo generado por algún dispositivo o sistema para indicar que algo ha sucedido.

Además (Adame Lorite, 2012) define que el log o traza de aplicación es el procesado y almacenamiento de información relativa a la ejecución de una aplicación. Contiene datos de entidades, cambios de estado y componentes software involucradas en dicha ejecución.

(Kent & Souppaya, 2006) define que, un log es un registro de los eventos que ocurren dentro de los sistemas y redes de una organización. Los Logs están compuestos de entradas de registro; cada entrada contiene información relacionada con un evento específico que ha ocurrido dentro de un sistema o red. Originalmente, los logs se usaban principalmente para solucionar problemas, pero ahora los logs sirven para muchas funciones en la mayoría de las organizaciones, como optimizar el rendimiento del sistema y la red, registrar las acciones de los usuarios y proporcionar datos útiles para investigar actividades maliciosas

Con referencia a Chuvakin, Schmidt, & Phillips, (2013, pág. 32) los ficheros 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 específico 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.

Los Sistemas de Información (SI) se refiere a un conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente.

Todo sistema de información se compone de una serie de recursos interconectados y en interacción, dispuestos del modo más conveniente en base al propósito informativo trazado, como puede ser recabar información personal, procesar estadísticas, organizar archivos, entre otros.

Actualmente podríamos afirmar que la mayoría de los sistemas y 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.

Los **ficheros logs** se generan ante cualquier evento que se esté suscitando en un sistema, aplicación o estructura tecnológica, esto se debe a diferentes causas como ser: ataques de inserción de código malicioso, denegación de servicios o simplemente una traza de error en el código de un sistema, o falla de algún dispositivo.

La gestión de logs aportan un valor agregado a la seguridad de la información dentro de las organizaciones, según (Chuvakin, et al., 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 sis-

temas, garantizando la continuidad del negocio.

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.

2. 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, se realizó un análisis comparativo y documental, Análisis y síntesis, Histórico Lógico, a partir de los datos que surgen de la indagación de diferentes normas y regulaciones referentes a la gestión de logs.

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

A continuación, de acuerdo al análisis de la Tabla 1. el estándar NITS 800-92 es el que cubre la mayor parte de las actividades necesarias para la gestión de logs, además se resalta también la norma ISO 27001 y las regulaciones como la PCI DSS, FISMA, HIPPA, para la gestión de logs.

Controles y/o Actividades	ISO 27 002	PCI DSS	NITS 800-92	CAG	GPG13	FISMA	HIPPA
Activacion de logs		√	√				
Generacion y registro de long			√	√			
Sincronizacion	√		√				
Seguridad de los logs	√	√	√			√	
Definir formatos de long		√	√	√			
Almacenamiento de logs	√	√	√	√	√	√	
Retencion de logs			√				
Analisis de logs		√	√	√		√	
Monitorizacion de logs	√		√		√		√
Revision periodica de los logs		√	√		√		√
Politicas y procedimientos de auditoria	√	√	√		√	√	√
Definir eventos auditables		√	√				
Contenido de los registros de eventos		√	√				
Capacidad de almacenamiento			√				
Respuesta a fallos de sistema de auditoria							

Tabla 1. Tabla Comparativa Controles para la Gestión de Logs. Fuente. Elaboración Propia.

3. Resultados

A continuación, se expone los principales resultados obtenidos.

Según el análisis de las normas y regulaciones relacionadas con la gestión de logs, las etapas para el diseño del modelo de actividades para la gestión de logs de sistemas de información debe estar conformado por las siguientes etapas:

Planeación, Diseño y Selección de Herramientas, como se muestra en la **Figura 1**.

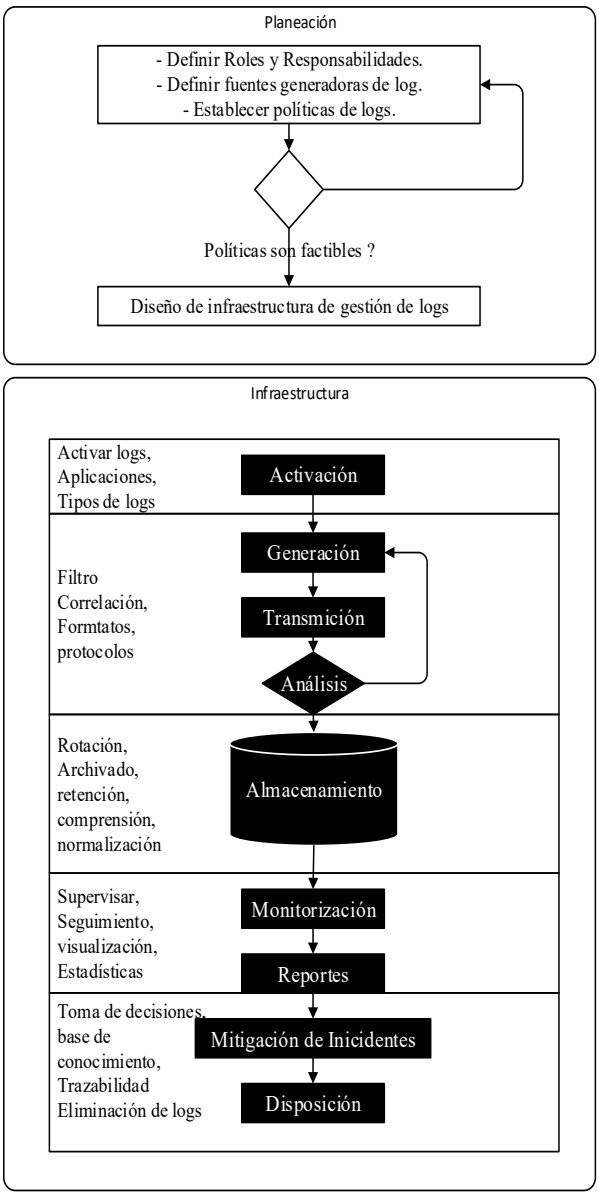

Figura 1. Modelo Actividades para la Gestión de Logs
Fuente: Elaboración propia

4. 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.

4.1. Definir roles y responsabilidades.

Definir roles y responsables de la configuración y activación de logs de acuerdo a las plataformas y/o aplicaciones que serán parte del proceso de gestión de logs.

Según (Kent & Souppaya, 2006) 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.

Como, por ejemplo, Administradores de sistemas y redes, Administradores de seguridad, Desarrolladores de aplicaciones, Oficiales de seguridad de la información, Directores de Información (CIO), Auditores, y Personas involucradas en la adquisición de software que debe o puede generar datos de registro de seguridad informática.

4.2. Definir fuentes generadoras de logs.

Se debe definir que plataformas, aplicaciones y tipos de logs formarán parte del proceso de gestión de logs.

Según (Chuvakin, Schmidt, & Phillips, 2013), se recomienda identificar los activos ya sea software o hardware que tengan más criticidad para el negocio, algunas de las herramientas que ayudan a realizar esto es mediante reuniones y entrevistas con los responsables de los activos, metodologías para valorar riesgos e impactos, además del inventario de activos.

Cabe señalar que cada organización tiene su propia infraestructura de TI y la importancia de sus activos dependen de sus necesidades de negocio.

4.3. 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.

4.4. Diseño de la infraestructura de gestión de logs.

Después de establecer una política inicial e identificar los roles y las responsabilidades, una organización debería diseñar una o más infraestructu-

ras de administración de registros que respalden efectivamente la política y los roles.

5. 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.

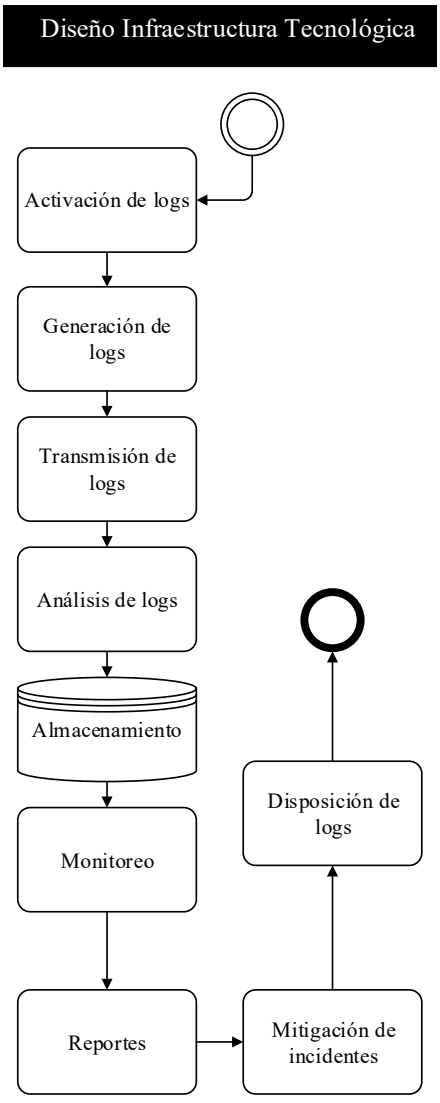

Figura 2. Actividades para el Diseño Infraestructura Tecnológica
Fuente. Elaboración Propia

5.1. Activación de logs.

En esta etapa se debe configurar o activar la generación de logs en las aplicaciones, sistemas y/o equipos informáticos definidas en el alcance que formaran parte de la gestión de logs.

Según (EMC-RSA, 2018), es recomendable habilitar el registro de datos de auditoria en los sistemas, dispositivos y aplicaciones que sean críticos para la organización y los cuales deberían participar en la gestión de logs, tener configurado de manera apropiada, permite que la auditoria de estos sistemas genere las alarmas correspondientes. Los logs también deben ser capturados para identificar campos específicos requeridos por normas regulatorias, por ejemplo, identificación de usuario, marco de tiempo, información de red y la etiqueta del nivel impacto de un evento.

5.2. Generación de logs.

En esta etapa se asegura que los registros de logs de las aplicaciones, sistemas y/o equipos informáticos configuradas en la activación de logs sean generados correctamente. y transmitidos a la plataforma de gestión de logs.

Según Kent & Souppaya, (2006):

Todas las fuentes de información de logs definidas en la planeación son involucrados en esta actividad, al igual que los responsables y administradores de estos activos, debido a que deben garantizar que estas fuentes generen sus propios registros, además de habilitar mediante configuración el envío y filtro de los registros de logs, garantizando eficiencia y efectividad en la gestión de logs.

Filtrar los eventos de acuerdo a la experiencia obtenida en la administración del activo, un exceso de logs puede generar pérdidas de información, además de problemas operacionales, como se mencionó anteriormente es necesario identificar y filtra los log de interés.

Que el formato generado por los protocolos para recolección y transmisión sean soportados por la arquitectura de la gestión de logs, se debe-

ría utilizar un formato estándar y apoyarse en la documentación de los activos generadores de logs y servidores de logs o SIEM, es recomendado utilizar protocolos como syslog o bases de datos.

Además, EMC-RSA, (2007) menciona que los registros de datos generados y obtenidos por el sistema de gestión de logs, debe ser capaz de realizar trazabilidad a través de usuarios únicos e individuales. La sincronización del tiempo en la generación de logs de las fuentes es de vital importancia ya que influye en la confianza del análisis de los mismos, por tal motivo se recomienda utilizar un servidor NTP (Network Time Protocolo, protocolo de red para sincronizar los relojes de los sistemas informático), para sincronizar el tiempo de los sistemas involucrados en la gestión de logs.

5.3. Transmisión de logs.

Definir mecanismos para asegurar la transmisión de los registros de logs generados a la plataforma de gestión de logs.

Según EMC-RSA, (2007) se debe tener en cuenta asegurar el proceso de transmisión de la información sensible a través del sistema de gestión centralizada de registros, al igual que en su almacenamiento, se debe garantizar controles para acceder a la información y no permitir acceso no autorizado a estos eventos.

5.4. Análisis de logs.

En esta etapa se debe Implementar mecanismos para la retención de logs durante un periodo de tiempo de manera automática tomando en cuenta políticas y/o procedimientos para la retención de logs.

Según Kent & Souppaya, (2006),La visualización del log muestra entradas de registro en un formato legible para el ser humano. La mayoría de los generadores de registros proporcionan algún tipo de capacidad de visualización de registros; los servicios de visualización de registro de terceros también están disponibles. Algunos visualizadores de registros proporcionan capacidades de filtrado y agregación.

Según Chuvakin, Schmidt, & Phillips, (2013), el análisis de mensajes de logs, o simplemente el análisis de logs, se ocupa de analizar los datos de registro para derivar el significado de los mismos. Tener sus datos en un solo lugar le permite juntar o correlacionar el mensaje de log para derivar el significado. Esto es especialmente importante en un entorno altamente distribuido en el que puede tener múltiples recopiladores de logs remotos y debe correlacionar los mensajes de logs recibidos en un recopilador con los recibidos en otro.

5.5. Almacenamiento de logs.

En esta etapa se debe definir mecanismos y políticas para el almacenamiento de logs.

Kent & Souppaya, (2006) menciona que en la gestión de logs es clave definir la retención y almacenamiento de los logs, estos requerimientos se deben especificar mediante políticas, donde se define el tipo de almacenamiento, tamaño, costo, velocidad de recuperación, archivado y destrucción de los logs.

Según (Chuvakin, Schmidt, & Phillips, 2013), aunque se encuentran varios métodos para el almacenamiento, en el caso de un sistema de archivos de logs, este debe soportar la comprensión que permite mejorar la seguridad y reducir notablemente el almacenamiento, aunque existen otros formatos como lo son los basados en texto, binarios, archivos y texto plano. Además, es importante que soporte la rotación en los sistemas de archivo de log, ya que como se mencionó anteriormente, puede configurarse por tiempo o tamaño dando flexibilidad a la hora de la consulta o análisis de logs, si el sistema no lo soporta debería utilizarse aplicaciones de terceras partes.

Por otra parte (CIS, 2018), menciona que se debe asegurar de que todos los sistemas que almacenan registros tengan el espacio de almacenamiento adecuado para los registros generados.

5.6. Monitorización.

En esta etapa se debe implementar mecanismos para el procesamiento de datos almacenados para facilitar la monitorización y visualización de la información.

Es necesario establecer mecanismos que se pueden usar para supervisar y revisar los datos de registros de logs y los resultados del análisis automatizado. En algunas infraestructuras de administración de logs, los mecanismos de monitorización también se pueden usar para proporcionar administración para los servidores de logs y los clientes. Además, los privilegios de usuario de la consola a veces pueden limitarse solo a las funciones y fuentes de datos necesarias para cada usuario. (Kent & Souppaya, 2006)

5.7. Generación de reportes.

Configurar y ajustar reportes estadísticos e históricos para validación de comportamientos de la infraestructura tecnológica.

Un paso importante en la administración y gestión de logs, es el análisis de los reportes, estos se convierten en un apoyo y recurso para el área de seguridad en la lucha de mitigar riesgos y reducir vulnerabilidades.

Es necesario que en las organizaciones se definan y establezcan tareas operativas, de acuerdo a la misión y visión de la organización cumpliendo con los objetivos propuestos en la política de seguridad, para realizar un análisis correcto y efectivo de los reportes de registros.

Se sugiere que se realicen tareas de análisis de reportes de manera: diaria, semana, mensual, trimestral, para identificar posibles cambios en estructuras de los registros.

Según (Kent & Souppaya, 2006) se sugiere evaluar la efectividad y ajustes de la política de seguridad una vez al año.

5.8. Mitigación de incidentes.

En esta etapa se debe establecer procedimientos gestión de incidentes para mitigar las amenazas identificadas y reportadas mediante la gestión de logs.

Durante el análisis de los registros de logs, es posible identificar eventos de importancia como incidentes o problemas operacionales que requieran de una respuesta. Cada organización define el procedimiento para tratar estos eventos, desarrollando políticas o aplicando estándares como ITIL.

Dentro de las mejores prácticas se recomienda construir una base de conocimientos de incidentes de seguridad, con información de vulnerabilidades conocidas, el significado de los mensajes de registro y datos que ayuden a identificar los incidentes que se estén generando. (Kent & Souppaya, 2006)

Cada persona tiene conocimientos y competencias distintas, y los incidentes de seguridad tienden a involucrar distintos activos de la organización, es por efectividad al solucionar estos incidentes que las organizaciones deben armar grupos de trabajo, para realizar un análisis completo a los incidentes presentados.

5.9. Disposición de logs.

En esta etapa se debe aplicar procedimientos y políticas para la eliminación apropiada de logs.

Dentro del proceso de gestión de logs, es importante generar políticas para archivar y eliminar los registros, teniendo en cuenta los procedimientos establecidos por la organización.

Eliminar los logs de manera que no haya trazabilidad de estos registros.

Los administradores de seguridad son los responsables de generar las políticas para el almacenamiento de los registros por el tiempo adecuado y generar los procedimientos de eliminación segura de acuerdo a las normas establecidas.

Según Kent & Souppaya, (2006) la eliminación de registros elimina todas las entradas de un registro que precede a una fecha y hora determinada. La eliminación de registros a menudo se realiza para eliminar datos de registro antiguos que ya no se necesitan en un sistema porque no es importante o se ha archivado.

Sobrescribir los registros con mayor tiempo de antigüedad, este proceso es viable cuando se utilizan registros de control o complementos y no son registros vitales para las investigaciones o para realizar los análisis de los incidentes generados.

5.10. Seguridad del registro de logs.

En esta etapa se debe implementar mecanismos de seguridad para la protección de logs en las actividades de recolección, transmisión, almacenamiento y retención.

Según la ISO/IEC 27002:2013, (2013) 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.

6. Selección de herramientas en software libre en base al modelo propuesto.

De acuerdo a la Figura 3. En esta etapa según el modelo de actividades de gestión de logs, se eligieron herramientas que se ajustan a la estructura tecnológica según la guía de gestión de logs de la NITS y el diseño del modelo de actividades de gestión de logs definida en la Etapa II. Las herramientas seleccionadas para cada fase son opcionales y están sujetas a requerimientos en cuanto capacidad y disponibilidad de recursos para su instalación y puesta en marcha

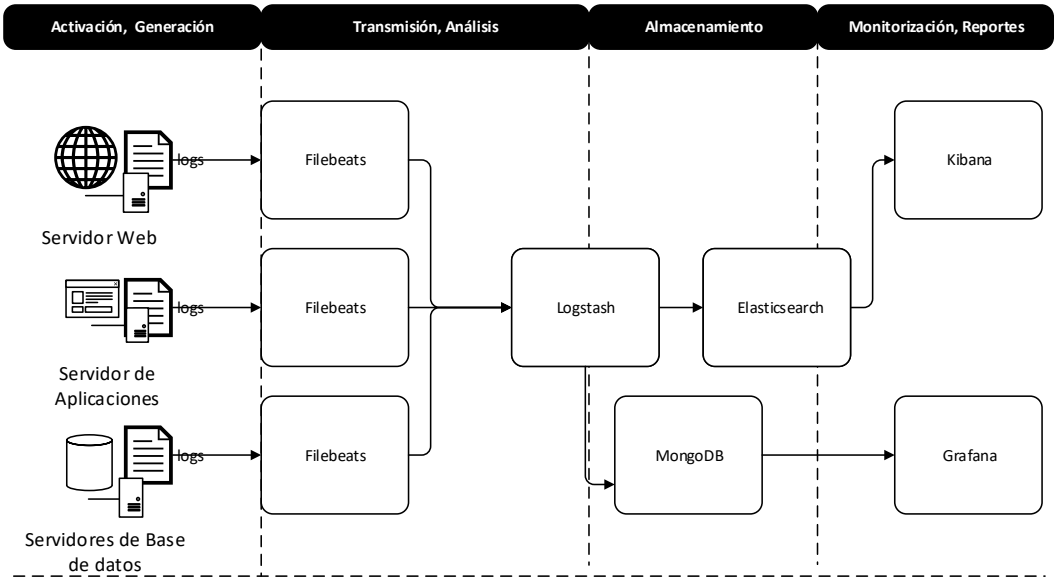

Figura 3. Selección de herramientas según diseño de actividades de la infraestructura tecnológica.
Fuente. Elaboración Propia

A continuación, se describen algunas de las herramientas seleccionadas.

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 (Gómez, 2018).

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. (GENBETA DEV, 2018)

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 buscando 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 (Group, 2018).

7. 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 de un modelo para la 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 o modelo para la gestión de logs.

Las actividades propuestas en el diseño de la infraestructura tecnológica se consideraron por medio del estudio de regulaciones, normas, estándares y modelos de buenas prácticas relacionados con el análisis y gestión de logs, para finalmente evaluar su implementación en un ambiente de prueba.

Con el diseño del modelo de actividades para la 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, 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.

Los resultados obtenidos coinciden con el estudio de (MSc. Oiner, Dra. C. Vivian, Ing. René, & Rodrígue, 2012), cuyos resultados permite afirmar que el modelo de actividades para la gestión de logs permite estandarizar el registro de eventos y propiciar múltiples objetivos, en función de las características y necesidades del escenario de aplicación.

Por otra parte, (JULIAN DAVID, LEONARDO FABIO, & CRISTIAN ANDRÉS, 2015), con su trabajo de investigación denominado: "Guía Metodológica Para La Gestión Centralizada De Registros de Seguridad A Través De Un Siem", menciona que para que el proceso de gestión de logs tenga consistencia y efectividad. Se debe tener en cuenta, que dependiendo de la estructura de la empresa, es posible obviar o adicionar algunas de las actividades propuestas.

8. Bibliografía

- 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/
- Alegre Diez, B. A. (2016). *Gestion de logs*. Universidad Internacional de la Rioja.
- 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
- 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.
- 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.
- 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
- 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.
- Elasticsearch. (2018). elastic. Obtenido de elastic: https://www.elastic.co/elk-stack
- GENBETA DEV. (17 de 08 de 2018). https://www.genbeta.com. Obtenido de GENBETA: https://www.genbeta.com/desarrollo/mongodb-que-es-como-funciona-y-cuando-podemos-usarlo-o-no

- Gomez, R. (1 de 12 de 2018). Obtenido de Irontec: https://blog.irontec.com/introduccion-muy-breve-y-desenfadada-a-docker/
- Graylog, I. (3 de julio de 2018). *Graylog*. Obtenido de Enterprise Log Management for All: https://www.graylog.org/ group, S. w. (11 de 11 de 2018). Davinici group. Obtenido de https://www.davincigroup.es/: https://www.davincigroup.es/grafana-sistema-monitorizacion/
- ISO/IEC 27002:2013. (octubre de 2013). *iso2700.es*. Obtenido de iso2700.es: http://www.iso27000.es/download/ControlesISO27002-2013.pdf
- JULIAN DAVID, A. C., LEONARDO FABIO, C. B., & CRISTIAN ANDRÉS, M. D. (2015). GUÍA METODOLÓGICA PARA LA GESTIÓN CENTRALIZADA DE REGISTROS. Colombia: UNIVERSIDAD CATÓLICA DE COLOMBIA.
- Kent, K., & Souppaya, M. (2006). Guide to Computer Security Log Management". Gaithersburg,: National Institute of Standards and Technology.
- MSc. Oiner, G. B., Dra. C. Vivian, E. S., Ing. René, R. B., & Rodrígue, D. C. (2012). Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones. Scielo.
- 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