RIELAC
Revista de Ingeniería Electrónica, Automática y Comunicaciones

Modelo de madurez para la gestión de logs en centros de datos: automatización y buenas prácticas.

Ailin V. Padrón Guerra

RESUMEN

La gestión óptima de logs en centros de datos es clave para fortalecer la vitalidad de los servicios y el rendimiento de las infraestructuras. Este artículo propone un modelo de madurez que evalúa y mejora este proceso, centrado en dos ejes: el ciclo de vida de los logs y funciones críticas como el monitoreo continuo y la automatización. A través de una revisión exhaustiva de literatura y un análisis comparativo de herramientas, se diseñó un modelo de madurez con varios niveles, cada uno con indicadores medibles. La validación se realizó mediante un ejercicio práctico en un entorno controlado de centro de datos, donde se aplicaron técnicas como análisis en tiempo real y normalización de logs. Los resultados demostraron que organizaciones en niveles superiores de madurez pueden reducir el tiempo de detección de incidentes sacando de la ecuación el factor humano para detectar la alerta y mejorando así su capacidad de respuesta ante incidencias. Además, se identificó que la integración de tecnologías de análisis avanzado es crucial para alcanzar el nivel optimizado. El artículo incluye la propuesta de un conjunto de herramientas como buenas prácticas, que permiten a una empresa con niveles bajos de madurez mejorar su gestión de logs, destacando su escalabilidad en entornos con recursos limitados y su alineación con estándares internacionales. Esta propuesta ofrece un marco práctico para que los centros de datos prioricen inversiones y optimicen su gestión de logs, garantizando altos niveles de disponibilidad y desempeño en los servicios críticos.

Palabras claves: Gestión de logs, centros de datos, modelo de madurez, automatización, optimización, monitoreo continuo.

ABSTRACT

Optimal log management in data centers is key to strengthening service vitality and infrastructure performance. This article proposes a maturity model that evaluates and improves this process, focusing on two axes: the log lifecycle and critical functions such as continuous monitoring and automation. Through an exhaustive literature review and a comparative analysis of tools, a maturity model with several levels, each with measurable indicators, was designed. Validation was performed through a practical exercise in a controlled data center environment, where techniques such as real-time analysis and log normalization were applied. The results demonstrated that organizations at higher levels of maturity can reduce incident detection time by taking the human factor out of the equation to detect the alert, thus improving their incident response capability. In addition, it was identified that the integration of advanced analytics technologies is crucial to reach the optimized level. The article includes a proposal for a set of tools as best practices that enable companies with low maturity levels to improve their log management, highlighting their scalability in environments with limited resources and their alignment with international standards. This proposal offers a practical framework for data centers to prioritize investments and optimize their log management, ensuring high levels of availability and performance in critical services.

Keywords: ***Log management, data centers, maturity model, automation, optimization, continuous monitoring.***
Maturity model for log management in data centers: automation and best practices

Recibido: 05/2025 Aceptado: 08/2025

1.- INTRODUCCIÓN

La gestión eficiente de logs en entornos distribuidos representa un desafío crítico para los equipos de operaciones y ciberseguridad. Estudios recientes demuestran que la falta de estandarización en la recolección, almacenamiento y análisis de logs incrementa significativamente el tiempo de respuesta ante incidentes (MTTR), afectando la disponibilidad de los servicios [1]. De acuerdo con estudios presentados en la IEEE International Conference on Web Services (ICWS) en 2024, más del 60% de las organizaciones enfrentan dificultades para correlacionar eventos debido a la heterogeneidad en los formatos de logs (texto plano, JSON, syslog) y la dispersión de fuentes (servidores, firewalls, microservicios) [2].

Uno de los principales problemas reportados en la literatura es la incapacidad de localizar líneas de log específicas en entornos escalables, lo que consume hasta un 70% del tiempo de los administradores de Tecnologías de la Información (TI) en tareas manuales [3]. Esta ineficiencia se agrava en arquitecturas modernas como IoT, cloud híbrido y Big Data, donde el volumen de logs supera los terabytes diarios, exigiendo estrategias de agregación y filtrado automatizado [4].

La ausencia de políticas claras para la estructuración de logs (ej.: campos comunes como timestamp, severity, source) dificulta el análisis automatizado y aumenta la dependencia de procesos ad-hoc, como el uso de herramientas tradicionales (grep), inadecuadas para entornos distribuidos [5]. Investigaciones destacan que logs no normalizados generan falsos positivos en sistemas SIEM, retrasando la detección de amenazas [6].

Además, aspectos de cumplimiento normativo exigen garantizar la integridad y confidencialidad de los logs, un requisito incumplido cuando se almacenan en texto plano o sin controles de acceso [7]. En Cuba, gran cantidad de organizaciones carecen de políticas de retención de logs principalmente por falta de modelos, buenas prácticas y capacitación de especialistas exponiéndose a riesgos legales.

Estos hallazgos justifican la necesidad de un modelo de madurez que evalúe y mejore la gestión de logs mediante dos ejes: (1) el ciclo de vida completo y (2) funciones críticas como monitoreo continuo y automatización. En este artículo se propone un modelo basado en estándares internacionales (ISO/IEC 27035, ITIL) y buenas prácticas validadas en la literatura reciente [8], [9].

2.- GESTIÓN DE LOGS

Un log es un archivo que captura toda actividad dentro del sistema operativo, aplicación software o dispositivo. Estos archivos documentan automáticamente cualquier información definida por los administradores de sistemas, incluyendo: mensajes, reportes de error, peticiones de archivo, transferencia de archivos, peticiones login/logout, entre otros. De igual manera la actividad viene marcada con fecha y hora, lo que ayuda a mantener un log del evento en cuestión. En muchos casos, por cuestiones legales las organizaciones se deben adherir a una regulación específica que dicta como se almacena y analizan los datos. Mas allá de los requerimientos legales, el análisis de los logs, cuando se hace de forma eficaz, puede proporcionar diferentes beneficios para los administradores de infraestructura y servicios de centro de datos. De esta forma serían capaces de identificar errores con mayor rapidez. Con una herramienta avanzada de análisis de logs, la organización puede incluso ser capaz de localizar los problemas antes de que se produzcan, lo que reduce en gran medida el tiempo y el costo de remediación [10].

El log también ayuda a revisar los eventos que llevan al error, lo que puede hacer que el problema sea más fácil de solucionar (troubleshooting), así como de prevenir en el futuro. La gestión de logs es fundamental porque permite detectar, investigar y responder a incidentes de seguridad en tiempo real. Los logs registran todas las actividades en sistemas, redes y aplicaciones, lo que los convierte en una fuente clave de información para identificar amenazas y vulnerabilidades.

La gestión de logs en centros de datos se ha convertido en un aspecto crítico y estratégico para garantizar la seguridad, la eficiencia operativa y el cumplimiento normativo en un entorno tecnológico cada vez más complejo y dinámico. En este contexto, es relevante mencionar el marco propuesto por la Asociación de Profesionales en Gerencia de Datos (DAMA Internacional) en su publicación de 2017, la segunda versión del DMBOK (Data Management Body Of Knowledge) [11]. Este marco proporciona una guía integral sobre la gestión de datos, estableciendo 11 áreas de conocimiento y 7 elementos ambientales que son esenciales para cualquier iniciativa relacionada con los datos. El DMBOK busca unificar conceptos y buenas prácticas, sirviendo como referencia para profesionales y organizaciones. En su núcleo, se encuentran las "Metas y Principios" para la gestión de datos, que son fundamentales para guiar las estrategias de manejo de información. Además, el DMBOK se sostiene sobre tres pilares esenciales:

Personas: Los recursos humanos son clave en la implementación efectiva de estrategias de gestión.
Procesos: Los procedimientos estandarizados aseguran la consistencia y calidad en el manejo de datos.
Tecnología: Las herramientas tecnológicas son vitales para facilitar la gestión y optimización de los sistemas.

Actualmente las organizaciones dependen de infraestructuras digitales robustas, lo que hace que la capacidad para optimizar la gestión de los logs generados por sistemas, redes y aplicaciones sea fundamental.

Para abordar estos desafíos, es esencial que dicha capacidad sea proactiva y reactiva: proactiva en la identificación temprana de problemas y reactiva en la respuesta efectiva a incidentes. Además, desde una perspectiva de gestión, es crucial que la solución sea integrada y centralizada, permitiendo una visión completa de las operaciones. La magnitud de los datos que se manejan exige un enfoque que priorice la flexibilidad como la habilidad para ajustar recursos, implementar nuevas tecnologías y modificar configuraciones sin interrumpir las operaciones existentes, y la escalabilidad para aumentar su capacidad y rendimiento al agregar más recursos sin afectar su funcionamiento. Asimismo, para extraer información valiosa, es imprescindible implementar un análisis de datos sofisticado y una visualización efectiva que facilite la identificación de problemas antes de que se conviertan en crisis, y que también optimice la eficiencia operativa al permitir una respuesta rápida y fundamentada ante cualquier anomalía [12].

Investigaciones previas han abordado diversos aspectos de la gestión de logs. Por ejemplo, autores como James Turnbull en "The Art of Monitoring" [13] han revelado la importancia del monitoreo continuo para detectar incidentes de seguridad en tiempo real, mientras que Hwaiyu Geng, en el "Data Center Handbook" [14], subraya que la implementación de prácticas sólidas de gestión de logs no solo mejora la seguridad y el rendimiento operativo, sino que también permite una respuesta más ágil ante incidentes, asegurando así la continuidad del negocio en los centros de datos.

En Cuba, en la Gaceta Oficial No. 45 Ordinaria, publicada el 4 de julio de 2019 [15], se establece una normativa para fomentar de forma racional un sistema de centros de datos con condiciones tecnológicas, respaldo y seguridad adecuados, como soporte al proceso de informatización y a las necesidades de las entidades que lo requieran. Además, el Decreto-Ley 78 sobre seguridad y protección de la información clasificada, publicado en la Gaceta Oficial No. 88 Ordinaria del 13 de septiembre de 2024, establece en su artículo 157 [7] la obligatoriedad de implementar sistemas de registro (logs) para todo equipamiento de seguridad, redes, servidores y servicios. Dichos registros deben documentar eventos que permitan la detección, caracterización e investigación de incidentes. También universidades de Cuba tienen investigaciones que han contribuido a mejorar los procesos de gestión de logs, enfocándose principalmente en la creación de sistemas centralizados que facilitan la auditoría y aumentan la eficiencia en la gestión [16].

A pesar de los avances, muchas organizaciones aún enfrentan desafíos significativos en materia de gestión que incluyen el manejo de grandes volúmenes de datos, la automatización, el análisis en tiempo real y la integración de herramientas diversas. Además, la falta de estandarización y el cumplimiento normativo añaden capas de dificultad a la situación actual.

2.1.- ETAPAS PARA LA GESTIÓN DE LOGS

Los logs son uno de los mecanismos más antiguos y reconocidos para la observabilidad de sistemas y aplicaciones. Desde sus inicios, se han utilizado para registrar información crucial sobre el estado de una aplicación, incluyendo mensajes de error, advertencias y datos de depuración. La gestión de logs es un proceso esencial en la seguridad informática, que se enfoca en la recopilación, procesamiento y análisis de los registros generados por diversos sistemas y dispositivos [17].

La gestión de logs no solo es vital para entender el funcionamiento interno de las aplicaciones, sino que también desempeña un papel fundamental en la detección de incidentes, el análisis forense y el cumplimiento normativo. Al permitir a las organizaciones identificar y responder rápidamente a problemas de seguridad, la gestión de logs contribuye a la mejora continua de la seguridad. En un entorno digital donde las amenazas son cada vez más sofisticadas, contar con un sistema efectivo de gestión de logs se convierte en una necesidad para proteger los activos y garantizar la integridad de la información.

La Figura 1, desarrollada por la autora para este artículo, presenta el ciclo de vida de una gestión de logs optimizada y sostenible. Este modelo integral abarca varias etapas clave diseñadas sistemáticamente para garantizar la eficacia en la recolección, almacenamiento, análisis y visualización de logs. Este ciclo se puede clasificar en acciones proactivas y reactivas, lo que permite implementar estrategias más efectivas [18].

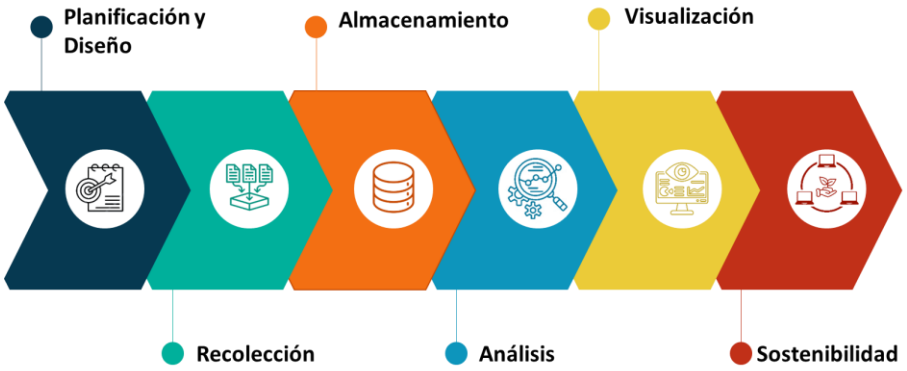

Figura 1
Etapas del ciclo de vida de la gestión de logs

Planificación y Diseño (Proactiva): Esta etapa inicial es fundamental para establecer una visión clara sobre la gestión de logs. Se deben identificar las posibles fuentes generadoras de logs, como servidores y aplicaciones, diseñar políticas y declarar objetivos que alineen la gestión de logs con las metas estratégicas de la organización. Esto incluye definir los criterios de calidad, los tipos de datos a recolectar y las normas de cumplimiento que deben seguirse.

Recolección (Proactiva): En esta etapa, se lleva a cabo la generación, captura y el envío de logs hacia un sistema centralizado o distribuido; garantizando la configuración de mecanismos que aseguren que los datos sean transmitidos correctamente. Además, es crucial aplicar políticas de retención de logs, garantizando que los datos estén disponibles para análisis, auditoría y cumplimiento legal.

Almacenamiento (Proactiva): Los logs recolectados se almacenan en bases de datos optimizadas capaces de manejar grandes volúmenes de datos en tiempo real. En esta etapa, se debe asegurar que los sistemas de almacenamiento cumplan con las políticas establecidas, incluyendo el tiempo legalmente requerido para conservar los registros.

Análisis (Reactiva): En esta etapa, se procesan los logs almacenados para identificar patrones, anomalías o incidentes. Un análisis efectivo permite a las organizaciones reaccionar rápidamente ante problemas potenciales y mejorar sus procesos.

Visualización (Reactiva): Presentación dinámica y en tiempo real de los logs procesados mediante dashboards interactivos para facilitar la identificación de patrones complejos y agilizar la respuesta ante incidentes mediante alertas visuales y sonoras que pueden reducir el tiempo de resolución. Al convertir datos crudos en representaciones gráficas intuitivas, esta etapa elimina la necesidad de análisis manual extensivo y posibilita la detección de anomalías de manera ágil. La visualización efectiva requiere herramientas que soporten filtros dinámicos, capacidad de hacer navegación jerárquica hasta los logs originales, y personalización de dashboards para diferentes roles técnicos.

Sostenibilidad (Proactiva): Esta etapa implica la revisión periódica del proceso de gestión de logs, enfocándose en tres aspectos claves: efectividad, eficiencia y alineación con los objetivos establecidos en la etapa de planificación y diseño. Se evalúa que el sistema de gestión de logs mantenga su capacidad para detectar y responder eficazmente a incidentes, optimizar el uso de recursos técnicos y humanos y adaptarse continuamente a los cambios tecnológicos, mediante revisiones periódicas de políticas, actualizaciones de procedimientos y ajustes en las herramientas implementadas.

El éxito del ciclo de vida de la gestión de logs está estrechamente relacionado con definir un nivel de madurez en esta área dentro de la organización, que permita evaluar las funciones vitales y el cumplimiento de dichas etapas. La madurez no es solo una tendencia; es una métrica crítica.

3.- SOLUCIÓN PROPUESTA

La presente sección introduce la solución propuesta para un modelo de madurez que estandarice la gestión de logs, priorice la automatización y optimice recursos técnicos.

Un modelo de madurez actúa como una hoja de ruta para las organizaciones, permitiéndoles identificar su nivel actual de

competencia en la gestión de logs y establecer objetivos claros para el desarrollo futuro. Este modelo se basa en funciones vitales específicas que corresponden a cada etapa del ciclo de vida de los logs como muestra la Tabla 1:

Tabla 1
Funciones vitales en el proceso de gestión de logs

Función Vital	Descripción	Etapa Correspondiente	Justificación
Definición de Políticas	Establecer normativas y procedimientos claros para la gestión de logs.	Planificación y Diseño	Las políticas claras aseguran un enfoque coherente y alineado con los objetivos organizacionales.
Captura de Datos	Recolectar información relevante y aplicar políticas de retención de logs.	Recolección	La captura precisa garantiza que se registren todos los logs necesarios, garantizando que los datos estén disponibles y sean útiles para análisis, auditoría y cumplimiento legal.
Automatización	Implementar procesos automatizados para la generación, recolección, almacenamiento y análisis de logs.	Recolección Almacenamiento Análisis Visualización	La automatización es imprescindible para reducir errores humanos, aumentar la eficiencia y asegurar la consistencia en la gestión de logs.
Normalización de Formatos	Estandarizar los formatos de los logs para asegurar la consistencia en su manejo.	Recolección Almacenamiento	La normalización permite una integración más sencilla de datos provenientes de diversos servicios y equipos desplegados en la infraestructura tecnológica, mejorando la calidad del análisis.
Estructuración	Estructurar y almacenar logs de manera segura y accesible, con motores de búsqueda capaces de manejar grandes volúmenes de datos en tiempo real.	Almacenamiento	La capacidad de estructurar el almacenamiento es crucial para gestionar grandes volúmenes en tiempo real, esto permite reducir los tiempos de análisis y asimismo la detección de incidentes.
Evaluación de Patrones	Analizar los logs recolectados para identificar tendencias, anomalías y oportunidades de mejora.	Análisis	La evaluación continua permite detectar problemas proactivamente, mejorando la seguridad y el rendimiento del centro de datos.

Seguridad de los datos	Implementar medidas de seguridad para proteger los logs contra accesos no autorizados y pérdidas.	Recolección Almacenamiento	Permite garantizar la integridad de los datos y el acceso seguro.
Supervisión Continua	Visualizar en tiempo real los logs para detectar incidentes o problemas potenciales.	Visualización	La supervisión activa ayuda a responder rápidamente a irregularidades, minimizando el impacto en las operaciones.
Mantenimiento Proactivo	Asegurar el mantenimiento y la actualización continua del sistema de gestión de logs.	Sostenibilidad	El mantenimiento proactivo es vital para adaptarse a nuevas tecnologías y amenazas, garantizando la efectividad a largo plazo.

Lo anterior explicado se enfoca en garantizar la seguridad, la calidad y la usabilidad de los logs, estableciendo principios para una gestión de logs efectiva y sostenible para la organización.

Para definir un modelo de madurez en la gestión de logs (Figura 2), es esencial estructurarlo en función de los tres pilares fundamentales: Personas, Procesos y Tecnología. Cada nivel de madurez debe describir cómo se cumplen estos pilares y qué características se asocian a cada uno (Tabla 2).

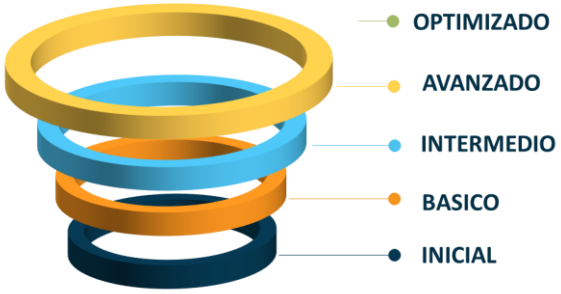

Fig. 2
Niveles de madurez en la gestión de logs

Tabla 2
Modelo de madurez en la gestión de logs

Nivel	Personas	Procesos	Tecnología	Funciones vitales
1: INICIAL	El personal de administración, alta dirección y especialistas de Ciberseguridad carecen de formación específica en la gestión de logs, lo que resulta en una	No existen procesos definidos; las actividades se realizan sin una metodología establecida y sin documentación.	La organización utiliza herramientas básicas o no tiene sistemas establecidos para la gestión de logs.	Captura de datos sin procedimientos establecidos.

	falta de conciencia sobre su importancia.			
2: BÁSICO	Existen algunos roles definidos, pero la capacitación es limitada y no todos los implicados están informados sobre las mejores prácticas.	Los procesos son documentados pero inconsistentes por la falta de uniformidad, coherencia o estabilidad de los procesos o prácticas.	Se implementan herramientas básicas para la recolección y almacenamiento, pero su uso es irregular.	Definición de políticas insipiente Captura de Datos
3: INTERMEDIO	El personal recibe capacitación adecuada, y se forman equipos interfuncionales que colaboran en la gestión de logs.	Los procesos son estandarizados y se siguen regularmente, aunque pueden no estar completamente optimizados.	Se utilizan tecnologías específicas que facilitan la recolección y almacenamiento eficiente de logs al realizarlo de forma automatizada.	Definición de Políticas Captura de Datos Automatización Normalización de formatos
4: AVANZADO	Se promueve la formación periódica del personal, fomentando una cultura organizacional centrada en la mejora continua.	Los procesos son optimizados mediante el uso de métricas y KPIs que permiten evaluar su efectividad.	Se implementan herramientas avanzadas que permiten el análisis en tiempo real y mejoran la toma de decisiones.	Definición de Políticas Captura de Datos Automatización Normalización de formatos Estructuración Evaluación de Patrones Seguridad de los datos
5: OPTIMIZADO	La organización cuenta con expertos en gestión de logs que ejercen un liderazgo proactivo, promoviendo la innovación.	Los procesos están completamente integrados y alineados con los objetivos estratégicos del negocio, garantizando su relevancia.	Se utilizan tecnologías innovadoras como inteligencia artificial, aprendizaje automático y Big Data, que facilitan la automatización total del proceso y el análisis predictivo, permitiendo anticipar problemas antes de que ocurran.	Definición de Políticas Captura de Datos Automatización Normalización de formatos Estructuración Evaluación de Patrones Seguridad de los datos Supervisión Continua Mantenimiento Proactivo

En el modelo de madurez descrito en la Tabla 2 se proporciona un marco claro para evaluar el desarrollo organizacional en relación con los pilares fundamentales de personas, procesos y tecnología. Al avanzar a través de estos niveles, las organizaciones pueden mejorar significativamente su capacidad para gestionar logs, lo que a su vez contribuye a una mayor seguridad, calidad e impacto positivo en sus operaciones generales.

3.1.- Validación del Modelo y Buenas Prácticas para la Evolución en la Gestión de Logs

Para demostrar la aplicabilidad del modelo propuesto, se evalúa el caso de una empresa de TI que opera actualmente en un nivel básico de madurez (nivel 2). Mediante un diagnóstico basado en las funciones vitales y etapas del ciclo de vida definidas anteriormente, se identifican brechas críticas y se proponen buenas prácticas tecnológicas que permiten a una empresa con niveles bajos de madurez mejorar su gestión de logs, destacando su escalabilidad en entornos con recursos limitados y su alineación con estándares internacionales.

Diagnóstico Inicial de la Empresa de TI
Nivel actual: Básico (Nivel 2)
Personas: Equipos con conocimientos técnicos, pero sin capacitación en estandarización (ej: uso de Syslog o CEF).
Procesos: Recolección centralizada parcial (solo 40% de los sistemas), sin normalización de formatos.
Tecnología: Herramientas básicas (rsyslog + grep), sin capacidades de análisis en tiempo real.

Brechas identificadas (vs. Nivel 3 Intermedio):
1. Falta de automatización en el almacenamiento, análisis y visualización de logs.
2. Almacenamiento no estructurado (texto plano en servidores locales).
3. Tiempo de detección de incidentes alto y dependiente de procesos manuales.

Buenas Prácticas para Avanzar al Nivel Intermedio

Enfocados en el pilar tecnológico el siguiente paso es seleccionar las herramientas adecuadas que permitan escalar hacia niveles superiores (intermedio/avanzado). La Tabla 3 presenta una variedad de herramientas fundamentales para la gestión de logs en servicios e infraestructura de centros de datos, organizadas según su etapa, función vital y nivel de madurez, así como la justificación de su uso. Desde herramientas básicas de recolección como rsyslog y nxlog; eficientes para la captura y transporte centralizado de logs, hasta plataformas de análisis integral como Splunk Enterprise y la suite Elastic Stack (Elasticsearch para almacenamiento y búsqueda distribuida, Logstash para procesamiento avanzado, y Kibana para visualización interactiva en tiempo real), cada solución aporta capacidades diferenciadas que cubren las distintas etapas del ciclo de vida de los logs. [19].

Tabla 3
Herramientas fundamentales para la gestión de logs

Herramienta	Descripción	Etapa/ Función vital/ Nivel de madurez	Justificación
rsyslog	Herramienta de registro que permite la recolección y el envío de logs desde diferentes fuentes.	Recolección/ Captura de Datos/ Básico - Intermedio	Arquitectura basada en servidores que centralizan logs, permitiendo fácil acceso y análisis.
nxlog	Solución para la recolección y el envío de logs que soporta múltiples formatos y protocolos.	Recolección/ Captura de Datos/ Básico - Intermedio	Arquitectura flexible que permite la integración con diversas plataformas y sistemas operativos.
Elasticsearch	Motor de búsqueda y análisis que permite almacenar, buscar y analizar grandes volúmenes	Almacenamiento y Análisis/ estructuración, evaluación de patrones, seguridad de los datos/	Arquitectura distribuida que permite escalabilidad horizontal, búsqueda eficiente de datos y análisis

	de datos.	Intermedio - Avanzado	en tiempo real.
Logstash	Herramienta para la recolección, transformación y envío de datos a Elasticsearch.	Recolección/ Captura de Datos, Normalización de formatos, automatización/ Intermedio - Avanzado	Herramienta que permite la ingestión flexible de datos desde múltiples fuentes y formatos. Transformaciones en tiempo real.
Kibana	Interfaz de usuario para la visualización y exploración de datos almacenados en Elasticsearch.	Análisis, Visualización/ Automatización, Supervisión continua/ Intermedio - Avanzado	Integración con Elasticsearch para crear dashboards interactivos y visualizaciones avanzadas de datos en tiempo real.
Splunk	Plataforma para búsqueda, monitoreo y análisis de datos.	Análisis, Visualización/ Automatización, Supervisión continua/ Intermedio	Arquitectura centralizada que integra múltiples fuentes de datos y proporciona análisis en tiempo real.
Nagios	Herramienta de monitoreo que permite supervisar el estado de los sistemas y servicios en tiempo real.	Visualización/ Supervisión continua/ Intermedio - Avanzado	Arquitectura distribuida que permite la supervisión centralizada con alertas automáticas ante incidentes.
Prometheus	Sistema de monitoreo y alerta que recopila métricas en tiempo real para el análisis del rendimiento.	Visualización/ Supervisión Continua/ Intermedio - Avanzado	Arquitectura basada en contenedores que facilita el escalado horizontal y la recopilación eficiente de métricas.
Grafana	Plataforma de visualización que se integra con diversas fuentes de datos para crear dashboards interactivos.	Análisis/ Supervisión Continua/ Intermedio - Avanzado	Integración con ELK Stack o Prometheus para visualización avanzada y generación de informes.
Ansible	Herramienta de automatización para la configuración y gestión del sistema, facilitando tareas repetitivas.	Recolección/ Automatización/ Intermedio - Avanzado	Arquitectura basada en scripts que permite implementar configuraciones consistentes en múltiples entornos y automatizar procesos.
Chef/Puppet	Herramientas para la automatización del aprovisionamiento y configuración del sistema.	Recolección/ Automatización/ Intermedio - Avanzado	Arquitectura orientada a agentes que permite gestionar configuraciones en tiempo real y asegurar automatizaciones.

Considerando lo anterior, se propone la combinación de Rsyslog, NXLog, Logstash, Elasticsearch y Kibana como muestra la Figura 3. Esta arquitectura proporciona una solución integral que puede posicionar a la empresa en un buen nivel de madurez en la gestión de logs [20].

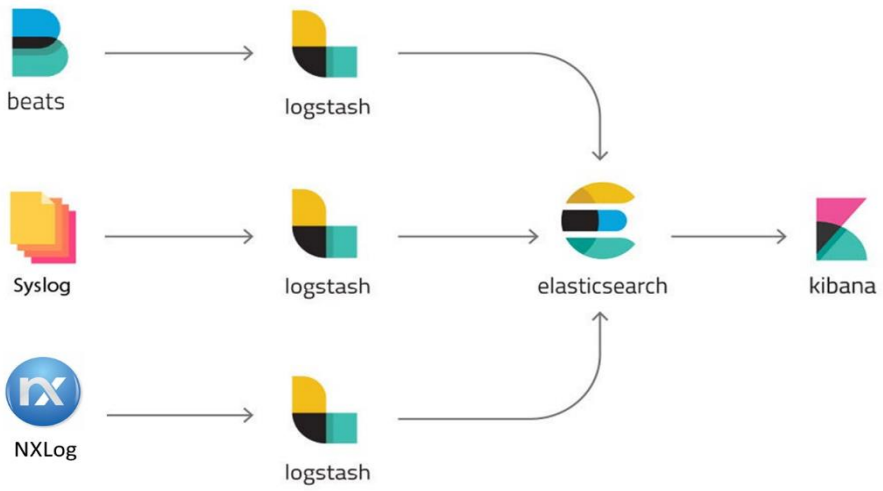

Figura 3
Arquitectura de la solución propuesta

Detalles de implementación:
- ✓ Instalar Logstash con filtros para normalizar logs de firewalls, servidores (Linux) y aplicaciones (Apache/Nginx).
- ✓ Usar Elasticsearch para indexar los datos y crear reglas de alerta en Kibana (ej: notificar ante >500 errores HTTP/5xx en 1 min).
- ✓ Capacitar al equipo en consultas avanzadas y creación de visualizaciones.

Proyección hacia Niveles Superiores (camino al nivel 4- avanzado):
- ✓ Integrar Inteligencia Artificial para detección proactiva (ej: Elastic Machine Learning).
- ✓ Adoptar SIEM comercial (Splunk) u open-source (Wazuh).

Este caso demuestra cómo el modelo de madurez; aplicado sistemáticamente, permite transformar una gestión de logs reactiva en una capacidad estratégica. Las buenas prácticas aquí descritas son escalables: organizaciones en niveles iniciales pueden comenzar con soluciones open-source (ELK), mientras aquellas con mayor madurez deben enfocarse en analítica predictiva (IAOps - Inteligencia Artificial para Operaciones de TI). La clave reside en alinear cada inversión tecnológica con las funciones vitales pendientes de implementar [21][22].

4.- CONCLUSIONES

El modelo de madurez propuesto resuelve una brecha crítica identificada en la literatura: la falta de un proceso integral que vincule las etapas del ciclo de vida de los logs (técnicas) con las funciones vitales (estratégicas). Al estructurarlo en cinco niveles evolutivos, se proporciona a las organizaciones una herramienta de diagnóstico cuantificable; basada en los pilares Personas, Procesos y Tecnología para medir su progreso real.

La validación práctica del modelo demostró que la transición del nivel básico al intermedio requiere priorizar la automatización, normalización, el almacenamiento estructurado y la capacitación del personal de administración.

Para centros de datos con recursos limitados la arquitectura propuesta (ELK Stack + Rsyslog) ofrece un punto de entrada escalable, compatible con regulaciones como la ISO 27001. Para entornos maduros la integración de IAOps (ej: Elastic ML) es el diferenciador clave para alcanzar el nivel optimizado, permitiendo análisis predictivos.

Este artículo abre dos rutas de investigación; la adaptación del modelo a entornos híbridos (cloud/on-premise) y el desarrollo de métricas estandarizadas para evaluar el ROI en la gestión de logs.

La gestión de logs ya no es un subproducto de las operaciones de TI, sino un activo estratégico. Este modelo proporciona el mapa para transformar datos caóticos en inteligencia accionable.

REFERENCIAS

1. Alavian P, Eun Y, Liu K, Meerkov SM, Zhang L. The (α, β)-Precise Estimates of MTBF and MTTR: Definition, Calculation, and Observation Time. IEEE Trans Autom Sci Eng. 2021 Jul;18(3):1469-77. doi: 10.1109/TASE.2020.3017134.
2. Qian B, et al. HEDGE: Heterogeneous Semantic Dynamic Graph Framework for Log Anomaly Detection in Digital Service Network. In: 2024 IEEE International Conference on Web Services (ICWS). Shenzhen, China; 2024. p. 208-16. doi: 10.1109/ICWS62655.2024.00041.
3. Jayapal C, S G, C KS, A J. Automation of Trace Analysis. In: 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). Coimbatore, India; 2023. p. 1-6. doi: 10.1109/ICAECA56562.2023.10199556.
4. Victor H, Kobayashi S, Yamauchi T. Analyzing Post-injection Attacker Activities in IoT Devices: A Comprehensive Log Analysis Approach. In: 2023 Eleventh International Symposium on Computing and Networking Workshops (CANDARW). Matsue, Japan; 2023. p. 292-7. doi: 10.1109/CANDARW60564.2023.00055.
5. Wang Y. Design of Visual Log Analysis System. In: 2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE). Jinzhou, China; 2023. p. 1649-52. doi: 10.1109/ICSECE58870.2023.10263397.
6. Aktar MN, et al. Enhancing False Positive Alert Detection in Security Information and Event Management System Using Recurrent Neural Network. In: 2024 27th International Conference on Computer and Information Technology (ICCIT). Cox's Bazar, Bangladesh; 2024. p. 2794-9. doi: 10.1109/ICCIT64611.2024.11022066.
7. Gaceta Oficial No. 88, Ordinaria, 13 de septiembre de 2024, Decreto Ley.78, Artículo 157.
8. Al-Ashmoery Y, Haider H, Haider A, Nasser N, Al-Sarem M. Impact of IT Service Management and ITIL Framework on the Businesses. In: 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI). Sana'a, Yemen; 2021. p. 1-5. doi: 10.1109/MTICTI53925.2021.9664763.
9. Tanović A, Hasibović AĆ. Benefits of ITIL Incident Management Process Implementation in one Public Institution in Bosnia and Herzegovina. In: 2024 47th MIPRO ICT and Electronics Convention (MIPRO). Opatija, Croatia; 2024. p. 1954-9. doi: 10.1109/MIPRO60963.2024.10569337.
10. Etalle S, Massacci F, Yautsiukhin A. The Meaning of Logs. In: Lambrinoudakis C, Pernul G, Tjoa AM, editors. Trust, Privacy and Security in Digital Business. TrustBus 2007. Berlin: Springer; 2007. p. 157-68. (Lecture Notes in Computer Science; vol. 4657). doi: 10.1007/978-3-540-74409-2_17.
11. DAMA International. Data Management Body of Knowledge (DMBOK). 2nd ed. 2017.
12. Vijayaraghavan H, Kellerer W. MobiFi: Mobility-Aware Reactive and Proactive Wireless Resource Management in LiFi-WiFi Networks. IEEE Trans Netw Serv Manag. 2024 Dec;21(6):6597-613. doi: 10.1109/TNSM.2024.3455105.
13. Smith JB. The Art of Monitoring. 1st ed. New York: O'Reilly Media; 2016.
14. Schneider HD, Pritchett MJD. Data Center Handbook. 2nd ed. New York: McGraw-Hill Education; 2018.
15. Gaceta Oficial No. 45, Ordinaria, 4 de junio de 2019.
16. Rubier JP, Perurena RM. Marco de trabajo para la gestión centralizada de trazas de seguridad usando herramientas de código abierto. Rev Cubana Cienc Inform. 2015 Jul-Sep;9(3).
17. Agrawal M, Krishnannair K. Implementing Enterprise Observability for Success: Strategically plan and implement observability using real-life examples. Packt Publishing; 2023.
18. Forms.app. Proceso de análisis de datos: Pasos y métodos clave [Internet]. Forms.app Blog. 2025 [cited 2025 Apr]. Available from: https://forms.app/es/blog/proceso-de-analisis-de-datos
19. Apium Academy. Las 10 mejores herramientas de software para la gestión de logs [Internet]. Apium Academy. 2025 [cited 2025 May]. Available from: https://apiumacademy.com/es/mejores-herramientas-software-gestion-logs/
20. Zeydan E, Baranda J, Mangues-Bafalluy J, Martínez R, Vettori L. Log Management in NFV Service Orchestration. In: 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Rome, Italy; 2021. p. 1-2. doi: 10.1109/SECON52354.2021.9491606.
21. Imagina Formación. Aprende ELK (Elasticsearch, Logstash, Kibana) – Tutorial de primeros pasos [Internet]. Imagina Formación. 2025 [cited 2025 Jul]. Available from: https://imaginaformacion.com/tutoriales/aprende-elk-elasticsearch-logstash-kibana-tutorial-de-primeros-pasos
22. Elastic. Security Solution [Internet]. Elastic Documentation. 2025 [cited 2025 Jul]. Available from: https://www.elastic.co/docs/solutions/security

CONFLICTO DE INTERESES

La autora no manifestó la existencia de posibles conflictos de intereses que debieran ser declarados en relación con este artículo.

AUTORA

Ailin V. Padrón Guerra, https://orcid.org/0009-0000-7634-6399, Graduada de Ingeniería en Telecomunicaciones y Electrónica (Universidad Tecnológica de La Habana José Antonio Echeverría, Cujae, 2017). Es especialista del grupo de servicios de centro de datos de la división de infraestructura y servicios de la Empresa de Tecnologías de la Información (ETI) de Biocubafarma. Intereses de investigación centrados en la gestión de servicios y computación en la nube. Email: ailinvpg@gmail.com.