DIVISIÓN DE POSGRADO

Título del trabajo:

Arquitectura para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data.

Línea de Investigación:

Tecnologías de la Información y Comunicaciones.

Modalidad de titulación:

Proyecto de desarrollo.

Programa de Maestría

Maestría en Sistemas de Información, mención en Inteligencia de Negocios.

Título a obtener:

Magister en Sistemas de Información, mención en Inteligencia de Negocios.

Autor:

Ing. Fabián Balseca Chávez.

Tutor:

MSc. Luis Llanganate.

Samborondón – Ecuador

2019

Dedicatoria

Al amor de mi vida, Claudia Silvana, mi compañera de viaje en esta vida y eje fundamental en mi desarrollo personal y profesional.

A mis amados hijos, Thomás y Victoria, por ser la luz y alegría de mis días, son el motor que me impulsa a esforzarme.

A mis padres, José Eduardo y (†) Fanny Leonor, no me basta el reconocimiento por todos sus sacrificios, su amor de padres y por animarme a seguir siempre adelante.

A mis suegros, Carlos Humberto y Silvia Oderay, por el afecto y apoyo que siempre me han manifestado.

Agradecimientos

A Dios y la Madre Dolorosa, por regalarme el don de la vida y el entendimiento.

A la Universidad Tecnológica ECOTEC y en su nombre al Claustro Docente de la Maestría en Sistemas de Información, por los conocimientos impartidos en las aulas de clases.

Mi reconocimiento al MSc. Luis Fernando Llanganate Moreno, por su guía y consejo durante la ejecución de mi proyecto de titulación.

A toda mi familia, amigos y compañeros de clases, por el apoyo moral en todo momento.

Certificado de revisión final

Que el presente proyecto de desarrollo titulado:

"Arquitectura para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data."

Fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos que se dictan en la guía de elaboración del trabajo de titulación, por lo que se autoriza al Ingeniero Fabián Eduardo Balseca Chávez, que proceda a su presentación.

Samborondón, 10 de agosto de 2019.



Tutor: MSc. Luis Fernando Llanganate Moreno.

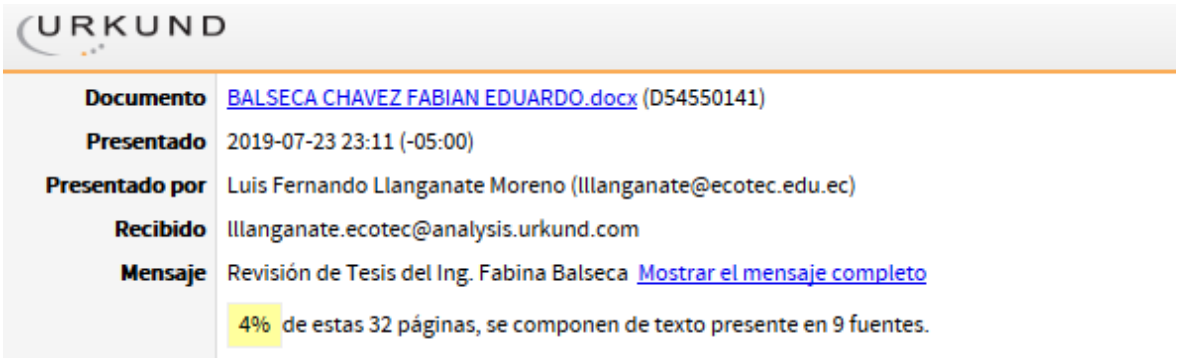
Certificado del porcentaje de coincidencias

Habiendo sido nombrado, MSc. Luis Fernando Llanganate Moreno, tutor del trabajo de titulación *"Arquitectura para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data"* elaborado por Ingeniero Fabián Eduardo Balseca Chávez, con mi respectiva supervisión como requerimiento parcial para la obtención del título de Magister en Sistemas de Información con mención en Inteligencia de Negocios.

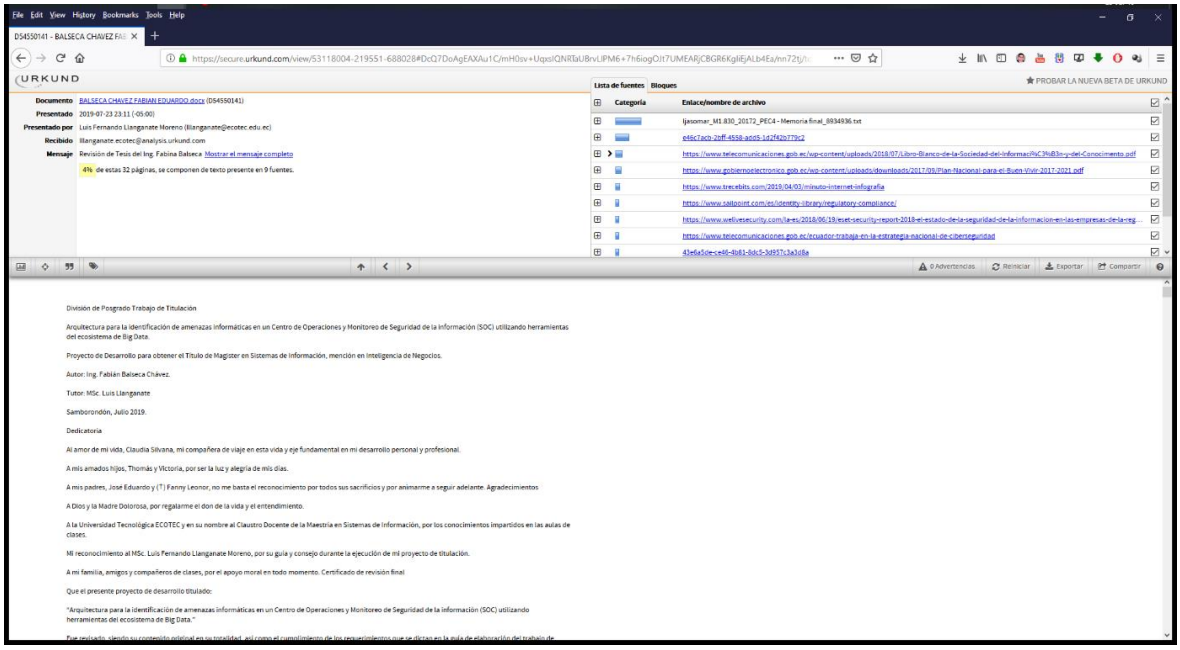
Se informa que el mismo ha resultado tener un porcentaje de coincidencias 4 % (CUATRO POR CIENTO) mismo que se puede verificar en el siguiente link:

https://secure.urkund.com/view/53118004-219551-688028

Adicional se adjunta la captura de pantalla de dicho resultado.


URKUND

Documento	BALSECA CHAVEZ FABIAN EDUARDO.docx (D54550141)
Presentado	2019-07-23 23:11 (-05:00)
Presentado por	Luis Fernando Llanganate Moreno (lllanganate@ecotec.edu.ec)
Recibido	lllanganate.ecotec@analysis.urkund.com
Mensaje	Revisión de Tesis del Ing. Fabina Balseca Mostrar el mensaje completo
	4% de estas 32 páginas, se componen de texto presente en 9 fuentes.



MSc. Luis Fernando Llanganate Moreno.

Profesor Tutor de la Ciencia

Resumen

El uso masivo de las Tecnologías de la Información y Comunicaciones (TIC), han ocasionado la interdependencia de la sociedad respecto de estas; no obstante, la ausencia de controles y normativas legales que regulen la utilización del ciberespacio aumentan la exposición ante ataques o amenazas informáticas, incrementando las vulnerabilidades en los activos de información de las organizaciones. La seguridad de los datos en la actualidad es el principal motivante para que las organizaciones generen entornos en cuanto a los nuevos desafíos en el campo de la Seguridad de la información, aplicando técnicas y herramientas del ecosistema de Big Data para coadyuvar en la prevención y detección de amenazas informáticas, mejorando los sistemas de identificación, integración y correlación de eventos en los Centros de Operaciones y Monitoreo de Seguridad de la información (SOC).

La arquitectura basada en herramientas del ecosistema de Big Data y propuesta en esta investigación, integra componentes de Elastic Stack (Elasticsearch, Logstash, Kibana) y tecnologías como Filebeat y Wazuh (NIPS / HIDS), gestionado la seguridad en equipos de comunicaciones, servidores de datos y aplicaciones, motores de bases de datos, terminales de usuario final, entre otros. Su implementación permitirá la supervisión en tiempo real e histórica para obtener una respuesta ágil y efectiva, personalizando búsquedas de correlaciones de eventos, alertas de seguridad e informes de estado, visualizando los datos para incrementar la capacidad de detección y optimización de la respuesta ante incidentes, evidenciando las actividades asociadas a posibles amenazas informáticas.

Palabras clave: Inteligencia de Negocios, Big Data, seguridad de la información, arquitectura tecnológica, amenazas informáticas.

Abstract

The massive use of Information and Communication Technologies (ICT) has caused the interdependence of society with respect to these; however, the absence of controls and legal regulations on the use of cyberspace increase exposure to attacks or cyber threats, and vulnerabilities in the organization's information assets. Data security is currently the main motivator for organizations to generate environments in terms of new challenges in the field of Information security, applying techniques and tools of Big Data's ecosystem to assist in the prevention and detection of threats, improving systems for identification, integration and correlation of events in the Security Operations and Information Monitoring Centers (SOC).

The tools-based architecture of Big Data's ecosystem and proposed in this research, includes Elastic Stack's components (Elasticsearch, Logstash, Kibana) and technologies such as Filebeat and Wazuh (NIPS / HIDS), managed security in communications equipment, data servers and applications, database engines, endpoints, among others. This implementation will allow real-time and historical monitoring to enable an agile and effective response, customizing event correlation searches, security alerts and status reports, visualizing data to increase the ability to detect and optimize incident response, revealing the activities associated with possible cyber threats.

Keywords: Business Intelligence, Big Data, information security, technological architecture, cyber threats.

Índice de contenido

Introducción 1

- Antecedentes. 2
- Descripción del problema. 3
- Pregunta problémica. 5
- Idea a defender. 6
- Objetivos de la investigación. 6
  - Objetivo general. 6
  - Objetivos específicos. 6
- Justificación. 7
- Procedimiento metodológico. 8
- Métodos de investigación. 9
- Marco legal y normativo. 10

Capítulo 1 Marco Teórico 14

1.1. Big Data. 15

1.1.1. Conceptos. 17

1.1.2. Aplicaciones del Big Data. 19

1.2. Fases de Big Data. 22

1.2.1. Ingesta de datos. 23

1.2.2. Agregación de datos y procesamiento. 23

1.2.3. Indexación y almacenamiento. 23

1.2.4. Visualización de datos. 24

1.3. Seguridad de la información. 24

1.3.1. Ciberseguridad y ciberdefensa. 25
1.3.2. ¿Cómo el Big Data ayuda a la ciberseguridad? 27
1.3.3. ¿Qué relación existe entre Big Data y ciberseguridad? 27
1.3.4. Tipos de amenazas informáticas. 29
1.3.5. Evaluación del impacto de una amenaza. 32
1.3.6. Nuevos desafíos. 33
1.4. Gestión de eventos de seguridad (Event Management). 35
1.5. Security Information and Event Management Systems (SIEM). 37
1.5.1. Características. 37
1.5.2. Funcionalidades claves. 38
1.5.3. Detección y alerta de amenazas informáticas. 40
1.5.4. Marco de ciberseguridad NIST. 40
1.5.5. Arquitectura referencial. 42
Capítulo 2 Solución propuesta 44
2.1. Security Operation Center (SOC). 44
2.1.1. Definición y misión. 44
2.1.2. Instrumentación. 46
2.1.3. Personas, habilidades y competencias. 47
2.2. Diseños de la solución propuesta. 49
2.2.1. Arquitectura de procesos. 51
2.2.2. Arquitectura de infraestructura tecnológica. 53
2.2.3. Arquitectura de software. 55
2.2.4. Arquitectura del negocio. 58
Capítulo 3 Validación de resultados 60

3.1. Hardware. 62
3.2. Software. 63
3.2.1. VMware vSphere 6.7 de 64 bits. 63
3.2.2. Sistemas operativos implementados. 64
3.3. Consolidado de infraestructura virtual. 65
3.3.1. Componentes de Elastic Stack. 66
3.4. Construcción del entorno de identificación de amenazas. 67
3.4.1. Interfaz gráfica de Wazuh Server. 68
3.4.2. Integración API con fuentes de información externa. 70
3.5. Caso de Uso para validación de resultados. 72
3.5.1. Caso de Uso No. 01. 72
3.5.2. Caso de Uso No. 02. 74
3.5.3. Caso de Uso No. 03. 76
3.5.4. Caso de Uso No. 04. 78
3.5.5. Caso de Uso No. 05. 80
3.5.6. Caso de Uso No. 06. 82
3.6. Impacto derivado del proyecto. 84
Capítulo 4 Conclusiones y Recomendaciones 85
4.1. Conclusiones. 85
4.2. Recomendaciones. 88
Referencias bibliográficas 89
Anexos 95
Vita 111

Índice de tablas

Tabla 1. Componentes de hardware. 62

Tabla 2. Consolidado de infraestructura virtual implementada. 65

Tabla 3. Caso de Uso No. 01. 72

Tabla 4. Caso de Uso No. 02. 74

Tabla 5. Caso de Uso No. 03. 76

Tabla 6. Caso de Uso No. 04. 78

Tabla 7. Caso de Uso No. 05. 80

Tabla 8. Caso de Uso No. 06. 82

Índice de figuras

Figura 1. Infecciones de malware por país. 4
Figura 2. Acceso al servicio de Internet en Ecuador. 11
Figura 3. Internet en un minuto, 2019. 16
Figura 4. 6V de Big Data. 17
Figura 5. El entorno de la Industria 4.0. 20
Figura 6. Fases de Big Data. 22
Figura 7. Triada de la Seguridad de la información. 25
Figura 8. Ciberseguridad y ciberdefensa. 27
Figura 9. Marco de referencia de ciberseguridad NIST. 41
Figura 10. Arquitectura referencial de un SIEM. 43
Figura 11. Modelo referencial de un SOC. 45
Figura 12. Consolidado de perspectivas arquitectónicas de la solución propuesta. 50
Figura 13. Arquitectura de procesos. 52
Figura 14. Arquitectura de infraestructura tecnológica. 54
Figura 15. Arquitectura de software. 57
Figura 16. Arquitectura del negocio. 59
Figura 17. Plataforma de procesamiento empresarial Mid – Range x86. 62
Figura 18. Arquitectura VMware vSphere. 64
Figura 19. Interfaz gráfica, Gestión de eventos de seguridad (Logs). 67
Figura 20. Interfaz gráfica, Gestión de Agentes desplegados. 68
Figura 21. Interfaz gráfica, Perspectiva general para identificación de amenazas. 69
Figura 22. Interfaz gráfica, Dashboard de seguridad. 69

Figura 23. Integración API con VirusTotal. 70
Figura 24. Análisis de inteligencia con VirusTotal. 71
Figura 25. Análisis de inteligencia con VirusTotal Graph, Modelo de red. 71
Figura 26. Visualización de evolución de alertas, Top 5 de agentes. 73
Figura 27. Lista resumen de alertas de seguridad. 73
Figura 28. Visualización de grupos por reglas de seguridad. 75
Figura 29. Análisis de auditoria de sistemas operativos Microsoft. 77
Figura 30. Ejecución de un ataque dirigido con UFONet. 79
Figura 31. Análisis de usuario y credenciales de acceso en activos de información. 79
Figura 32. Explotaciones de vulnerabilidades con Kali Linux. 81
Figura 33. Ataque dirigido por denegación de servicio dinámico DDoS. 81
Figura 34. Ataque de enumeración de activos de información. 83
Figura 35. Identificación de activos de información y cuentas de usuarios. 83

Índice de anexos

Anexo A – Consolidado de infraestructura virtual. 95

Anexo B – Plan de direccionamiento de infraestructura virtual. 96

Anexo C – Instalación de Elastic Stack. 97

Anexo D – Instalación de Wazuh Server. 103

Anexo E – Agentes Wazuh. 110

Introducción

La gestión y la seguridad de los datos en la actualidad se han convertido en la principal preocupación de las empresas y organizaciones, presentándose nuevos desafíos en el campo de la Seguridad de la información en la era del Big Data.

El almacenamiento, procesamiento y análisis de datos a través de Big Data, considera la aplicación de técnicas modernas para la detección y prevención de amenazas informáticas mediante datos de seguridad de fuentes internas o externas, que permitan mejorar los sistemas de identificación, integración y correlación de eventos en los Centros de Operaciones y Monitoreo de Seguridad de la información (SOC).

Hervé Lambert (2018) afirma: Big Data permite incrementar y adaptar la prevención y respuesta ante cualquier tipo de amenaza; acortar los tiempos de reacción y defensa, además de visibilizar tanto el histórico como la actividad en tiempo real de los endpoints, mejorar la capacidad analítica y los procesos, clasificándolos automáticamente y realizando análisis forenses de amenazas y ataques.

La investigación objeto de este estudio, se focaliza en los Centros de Operaciones y Monitoreo de Seguridad de la información (SOC), pertenecientes al sector de empresas que brindan servicios tecnológicos especializados en Seguridad de la información en el Ecuador.

- **Antecedentes.**

El Big Data es una de las tendencias más actuales dentro de la industria tecnológica, la aplicación de ecosistemas basadas en Big Data está transformando la sociedad. Así como lo hace en áreas de Marketing, Investigación, Economía y Medicina, en Seguridad de la información, también se apunta a ser un aliado muy importante, como lo es en la identificación de amenazas informáticas y vulnerabilidades, como por ejemplo en la información de identidad de usuarios, redes de datos corporativas, terminales de usuario o servidores, accesos malintencionados, malware, entre otros, dado que los ataques informáticos se están sofisticando y aumentando. Sin duda, el ecosistema de Big Data permite cambiar y mejorar los aspectos de la Seguridad de la información para crear plataformas inteligentes de ciberseguridad concebidas para erradicar las amenazas informáticas.

Las empresas de servicios en el ámbito de la Seguridad de la Información orientados a la identificación de amenazas informáticas y vulnerabilidades por medio de herramientas del entorno de Big Data en la actualidad en el Ecuador son escasas, sin embargo, el vertiginoso avance tecnológico entorno al manejo de grandes volúmenes de información ha motivado una profesionalización y modernización tecnológica de las empresas del ramo.

Con la aplicación de herramientas del ecosistema de Big Data, los Centros de Operaciones y Monitoreo de Seguridad de la información (SOC) potenciarán sus esquemas de identificación de amenazas utilizando análisis de patrones, análisis basado en comportamientos y modelos de aprendizaje automático para agilizar la tarea de monitoreo de los activos de información e infraestructura tecnológica, aplicaciones, bases de datos y

procesos empresariales, mejorando la identificación de amenazas informáticas desconocidas. Las herramientas del ecosistema de Big Data y Big Data Analytics, análisis cuantitativo y aprendizaje automático permiten que los equipos de respuesta a incidentes (IRT, Incident Response Team) identifiquen no solo amenazas informáticas, sino que además de una amplia gama de riesgos empresariales que afectan y comprometen las operaciones de las organizaciones.

- **Descripción del problema.**

Según información de más de 4500 ejecutivos, técnicos y gerentes que laboran en más de 2500 empresas de 15 países de Latinoamérica, evidenciaron que al menos tres de cada cinco organizaciones en Latinoamérica durante el año 2018 sufrieron por lo menos un incidente de seguridad, ubicándose en primer lugar la infección con códigos maliciosos con el 45 por ciento y siendo Ecuador el que tiene un mayor índice de infecciones de ransomware con el 22 por ciento (ESET Inc., 2018), como se observa en la **Figura 1**.

Una de las tendencias actuales para la identificación de estas anomalías, se enfoca en la aplicación de técnicas de Inteligencia de Negocios y específicamente, en la aplicación de herramientas del ecosistema de Big Data, que permitan que las organizaciones logren estándares aceptables a nivel de su seguridad de la información, a pesar del impredecible y cambiante ambiente de las amenazas informáticas actuales.

Porcentaje de infecciones de malware en Latinoamérica.



Figura 1. *Infecciones de malware por país.*

Fuente: Laboratorio de Investigación de ESET Inc.

Por lo tanto, resulta crítica la identificación, detección y respuesta ante amenazas informáticas para una organización:

1. La identificación de amenazas informáticas basadas en técnicas de Inteligencia de Negocios se fundamenta en una visibilidad completa de los activos críticos de la organización y en la aplicación de herramientas avanzadas de analítica de datos para descubrir los incidentes de seguridad.

2. La respuesta ante la ocurrencia de incidentes de seguridad debido a la presencia de amenazas informáticas es gestionada por personal especializado de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), que cuenta con la ayuda de herramientas avanzadas de análisis de seguridad.

3. Aumento significativo en la velocidad y precisión de las investigaciones de seguridad de la información, ofreciendo un contexto sobre los incidentes identificados y asignando prioridades a los posibles problemas para su posterior evaluación.

4. La implementación de herramientas para la supervisión en tiempo real, continua e histórica, permiten una respuesta rápida por parte de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), personalizando búsquedas de correlaciones de eventos, alertas de seguridad e informes de estado, visualizando los datos para incrementar la capacidad de detección y optimizar la respuesta a incidentes, para un análisis de ataques e investigaciones con el objetivo de encontrar las actividades asociadas a amenazas avanzadas.

- **Pregunta problémica.**

¿Como mejorar la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC)?

- **Idea a defender.**

Si se crea una arquitectura tecnológica utilizando herramientas del ecosistema de Big Data, se agilizará la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

- **Objetivos de la investigación.**
  - **Objetivo general.**

Desarrollar una arquitectura tecnológica utilizando herramientas del ecosistema de Big Data para mejorar la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

  - **Objetivos específicos.**

a. Conceptualizar el estado del arte en referencia al entorno de la Seguridad de la información y las tecnologías del ecosistema de Big Data.

b. Diagnosticar el estado actual de la identificación de las amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

c. Diseñar una arquitectura tecnológica que permita la implementación de herramientas del ecosistema de Big Data para la identificación de amenazas informáticas.

d. Integrar los componentes de la arquitectura tecnológica planteada utilizando herramientas del ecosistema de Big Data.

e. Validar la arquitectura propuesta en un escenario real.

- **Justificación.**

Debido al crecimiento de los incidentes de seguridad de la información, inicialmente dirigidos a grandes empresas y organizaciones, entidades gubernamentales e instituciones financieras, estas implementaron sus propios Centros de Operaciones y Monitoreo de Seguridad de la información (SOC) enfocados en identificar y prevenir amenazas digitales.

En la actualidad, todas las organizaciones y personas están expuestas a sufrir un ataque informático, dado que los criminales informáticos están mejor organizados y las amenazas son cada día más sofisticadas, siendo imperativo contar con capacidades para realizar inteligencia de amenazas informáticas.

No obstante, es posible disminuir el nivel de exposición ante incidentes de seguridad de forma significativa y con ello la materialización de las amenazas informáticas, así como reducir el impacto sin necesidad de incurrir en elevadas inversiones ni contar con una gran estructura de personal técnico. Para concretar esto, es necesario conocer y gestionar de manera ordenada las amenazas informáticas a las que están expuestos los activos de información, considerando procedimientos y controles de seguridad, planificando e implantando estrategias de seguridad apoyadas en nuevas tecnologías de información, como Big Data, Big Data Analytics o Machine Learning (aprendizaje automático), que para Ecuador todavía son catalogadas como muy recientes.

Con el diseño de una arquitectura tecnológica de Inteligencia de negocios enmarcada en una plataforma de gestión para los Centros de Operaciones y Monitoreo de Seguridad de la información (SOC), se permitirá el procesamiento del gran volumen de información que generan los componentes tecnológicos monitoreados; estos datos pueden ser analizados en un menor tiempo, mejorando la identificación de las posibles amenazas de seguridad utilizando herramientas del ecosistema de Big Data.

La investigación objeto de estudio, plantea que dentro del ciclo de vida del aseguramiento tradicional de la información frente amenazas de informáticas, las herramientas del ecosistema de Big Data contribuirán en la generación de modelos de predicción más rápidos y precisos facilitando el aprendizaje automático, que hoy en día, utilizan los grandes fabricantes de soluciones de seguridad para detección y prevención de amenazas, mismos que son aplicados en sistemas de gestión de eventos e información de seguridad.

- **Procedimiento metodológico.**

La misión de un Centro de Operaciones de Seguridad de la información (SOC) típicamente se ha centrado en la coordinación de una defensa basada en múltiples capas de seguridad para detectar, prevenir y gestionar amenazas informáticas que pueden comprometer la integridad de la infraestructura tecnológica, los servicios empresariales o los datos de una organización.

La aplicación de técnicas de Inteligencia de negocios y a su vez de herramientas del ecosistema de Big Data, establecen correlaciones entre datos que permiten detectar amenazas informáticas y anticiparse a los posibles eventos de seguridad, sea para detectar

conductas inusuales de usuarios de la organización o para determinar el patrón de comportamiento de un atacante o criminal informático. El Big Data puede representar un recurso valioso para el personal de seguridad de la información, para automatizar procesos y detectar anomalías o eventos de seguridad, que normalmente pasarían desapercibidos debido al volumen de datos procesados.

Se plantea la construcción de una arquitectura tecnológica que permita la identificación de amenazas informáticas utilizan la lógica contextual para revelar patrones de comportamiento malicioso y generar acciones de defensa informática avanzada contra amenazas conocidas y desconocidas; así también, analiza, categoriza y correlaciona todos los datos que obtiene sobre las amenazas informáticas para llevar a cabo tareas de prevención, detección, respuesta y remediación dentro de en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), aportando valor en las tareas de identificación de amenazas informáticas por parte de los especialistas de seguridad de la información.

- **Métodos de investigación.**

La investigación inicia con la revisión documental de la Seguridad de la información, su definición, conceptos, categorías y los desafíos enfrentados, para en posterior abordar tópicos de Big Data, descripción del análisis de datos, correlación de eventos de seguridad y su aplicabilidad para fortalecer la operatividad de los Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

Además, se mantendrá un alcance fundamentalmente de carácter exploratorio, diagnóstico y correlacional durante la ejecución de la investigación, generando valor junto con la experiencia y conocimiento de Expertos especializados en Seguridad de la información y Análisis de datos, residiendo su aplicabilidad en el entorno de desarrollo de arquitecturas tecnológicas utilizando herramientas del ecosistema de Big Data para mejorar la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

Una vez concluida la fase de investigación se validarán las arquitecturas propuestas en un escenario real, ejecutando pruebas de las configuraciones necesarias para dar cumplimiento con los objetivos planteados en el proyecto entorno a la identificación de amenazas de informáticas actuales. Se finalizará con una discusión de los resultados entorno a la arquitectura tecnológica propuesta.

- **Marco legal y normativo.**

Como se observa en la **Figura 2**, en Ecuador el acceso a las Tecnologías de la Información y la Comunicación (TIC) ha crecido considerablemente en los últimos años. En el año 2008, solo el siete por ciento de la población ecuatoriana tenía accesos a Internet y en el año 2018 se incrementó el uso de este servicio al 46,1 por ciento, de acuerdo con la información de la Agencia de Regulación y Control de las Telecomunicaciones, dicho crecimiento está influenciado tanto por la innovación y desarrollo tecnológico, como por las políticas y estrategias gubernamentales de conectividad y prestación de servicios implementadas en los últimos años (ARCOTEL, 2019).

Cuentas de Internet fijo a nivel Nacional (2010 – 2018).

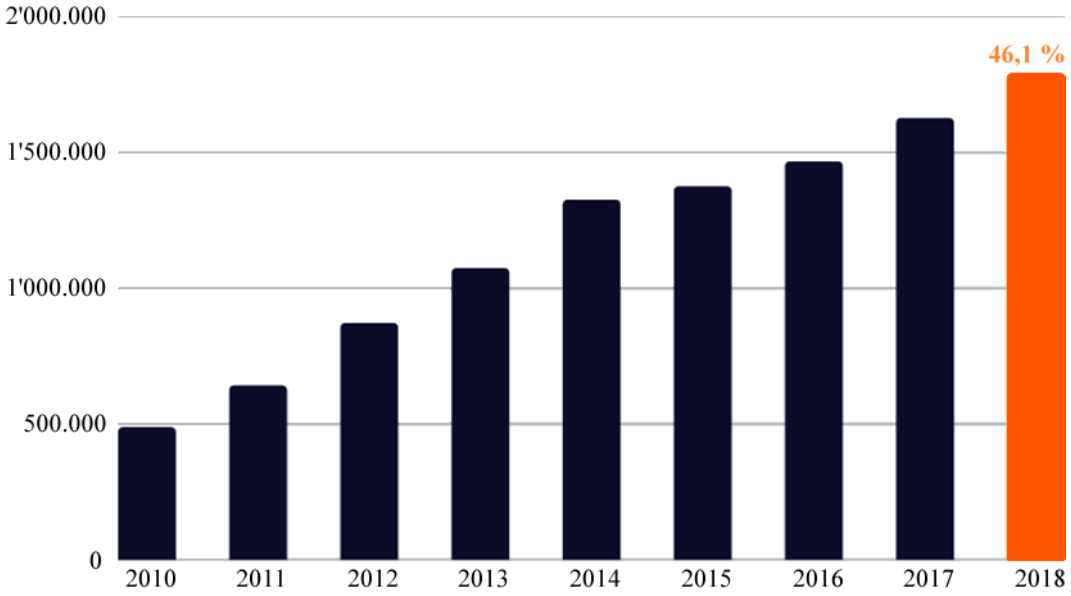


***Figura 2**. Acceso al servicio de Internet en Ecuador.*

Fuente: Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

Este factor, además de considerarse en la actualidad como una herramienta de trabajo, conlleva implicaciones de carácter delictivo, en este ámbito, en el país se alertó del hackeo de páginas del Gobierno y la revisión de correos privados de altas autoridades durante el año 2019 debido a eventos de carácter político (MINTEL, 2019). Por otro lado, las denuncias registradas por delitos de carácter informático crecen, de estas el 93 por ciento fueron presentadas ante la Fiscalía General del Estado, el cuatro por ciento ante dependencias de la Policía Nacional y el tres por ciento a través de la herramienta 1-800 DELITO; imputaciones que van desde la interceptación ilícita, suplantación de identidad, secuestro digital, ataques a la integridad de datos y sistemas, abuso de dispositivos, falsificación y fraude informático, pornografía infantil y delitos contra la propiedad intelectual.

De esta manera, los delitos informáticos son enfrentados con importantes estructuras del Estado ecuatoriano, disponiendo de al menos 200 miembros de la Policía Judicial que están involucrados directa y exclusivamente en la investigación e inteligencia antidelincuencial de los cibercrímenes desde el 2016.

En otro frente, el Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador (MINTEL) durante el año 2018 entregó el documento denominado Libro Blanco de la Sociedad de la Información y del Conocimiento (LBSIC) (MINTEL L. , 2018), en el que delinean las directrices para la construcción de la Sociedad de la Información y del Conocimiento en beneficio de la población ecuatoriana bajo el criterio de equidad, inclusión y acceso a la información por parte de los ciudadanos, así como efectivizando las labores de la administración pública. Su elaboración es el resultado de un trabajo colaborativo de las personas, academia, así como organizaciones privadas y gubernamentales. Dicho documento se alinea con el Plan Nacional de Desarrollo 2017 – 2021, que es el principal instrumento del Sistema Nacional Descentralizado de Planificación Participativa (SNDPP) (República del Ecuador, 2017), y su objetivo es contribuir al cumplimiento progresivo de los derechos constitucionales, los objetivos y disposiciones del régimen de desarrollo (a través de la implementación de políticas públicas), y los programas, proyectos e intervenciones que de allí se desprenden, el cual impulsa la productividad y la competitividad para el crecimiento económico sostenible. El Libro Blanco de la Sociedad de la Información y del Conocimiento (LBSIC), se centra en cinco ejes principales de acción, a saber:

1. **Infraestructura y conectividad**, impulsando el despliegue de la infraestructura, permitiendo ampliar la cobertura de telecomunicaciones en zonas aún desatendidas, con énfasis en disminuir la brecha digital en el Ecuador.

2. **Gobierno electrónico**, bajo la meta de acercar cada vez más al Gobierno y a los ciudadanos, mediante el uso de las tecnologías de información y comunicaciones (TIC), aportando a la eficiencia y eficacia del Estado.

3. **Inclusión y habilidades digitales**, permitiendo a los ciudadanos acceder a oportunidades de empleabilidad por medio del desarrollo de habilidades digitales básicas y específicas, fortaleciendo la inclusión digital, con iniciativas como la tele–educación, tele–trabajo, entre otras.

4. **Seguridad de la información y protección de datos personales**, posicionando al Ecuador como referente regional en Seguridad de la información y fortaleciendo los mecanismos de ciberseguridad; así como, fomentando una cultura de protección de datos personales en la sociedad para garantizar los derechos de los ciudadanos.

5. **Economía digital y tecnologías emergentes**, para promover la transición hacia una economía digital a través de la digitalización de las empresas y organizaciones, como paso previo a la Transformación Digital, que permita caminar al Ecuador hacia una industria 4.0 y fomentar el uso de tecnologías emergentes para aprovechar sus beneficios en el gobierno, industria, academia y sociedad civil.

Capítulo 1

Marco Teórico

La gestión de grandes volúmenes de datos o también conocida como Big Data, hace referencia a sacar el mayor provecho de una enorme cantidad de datos generados por ejemplo por plataformas tecnológicas, sistemas o usuarios. En temáticas de seguridad de la información, existe la necesidad de obtener, analizar e interpretar una gran cantidad de datos que se generan diariamente en cientos de miles de registros de eventos (Logs) en los activos de información de una organización.

Bajo esta premisa, todo ataque informático queda asentado en los registros de eventos o bitácoras; sin embargo, ¿si todo evento malicioso genera una huella (marca distintiva) en los registros de eventos de los activos de información, por qué a menudo pasan desapercibidos? o en el mejor de los casos se desconoce el haber sido objeto de un ataque informático. La respuesta es evidente puesto que son demasiados datos para analizar en tiempo real (Pérez Marqués, 2015).

Para comprender esta problemática, es imprescindible utilizar una herramienta de software que recolecte todos estos datos, los procese bajo reglas definidas que se haya proporcionado y permita su visualización para la interpretación, como por ejemplo un correlacionador de eventos de seguridad (Mujawar & Kulkarni, 2015). La visualización de la seguridad se refiere a observar los datos recopilados de una manera diferente, es decir, gráficamente, generar modelos que representen infinidad de datos que resultarían incomprensibles, a primera vista.

1.1. Big Data.

La gestión de datos masivos, datos a gran escala o Big Data, es un término que hace referencia al concepto relativo a conjuntos de datos tan grandes y complejos como para que hagan falta aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente (Pérez Marqués, 2015). Por tal motivo, los procedimientos usados para encontrar patrones repetitivos dentro de esos datos son más sofisticados y requieren software especializado (Mayer-Schönberger & Cukier, 2013).

En la actualidad, el uso del término Big Data, tiende a referirse al análisis del comportamiento del usuario, otorgando valor a los datos almacenados y formulando predicciones a través de los patrones de comportamiento observados; la disciplina dedicada al estudio de los datos masivos se enmarca en el sector de las Tecnologías de la información y comunicación (TICs) (Chalmers, Picot-Clémente, & Bothorel, 2013). Esta disciplina se ocupa de todas las actividades relacionadas con los sistemas que manipulan ingentes conjuntos de datos, siendo las dificultades más comunes las vinculadas a la gestión de estas cantidades de datos que se centran en la recolección y el almacenamiento, búsqueda, compartición, análisis, y visualización (Hashem, et al., 2015).

La tendencia a manipular tales cantidades de datos se debe a la necesidad de incluir dicha información para la creación de informes estadísticos y modelos predictivos utilizados por los Directivos de las organizaciones para el análisis de rendimiento de un negocio, marketing y fidelización de clientes, datos de enfermedades infecto – contagiosas, espionaje industrial y seguimiento a los ciudadanos, o en la lucha contra la delincuencia organizada, entre otras actividades.

No obstante, como se observa en la **Figura 3**, Internet ha cambiado en la última década tanto que, por ejemplo, hace siete años se enviaban cada minuto 11 millones de mensajes a través de aplicaciones de mensajería instantánea, y en el año 2019 sobrepasan los 41,6 millones de mensajes, Google soporta 3,8 millones de consultas cada minuto, se visualizan en YouTube 4,5 millones de vídeos y se envían más de 87500 tuits en Twitter (Trecebits, 2019).

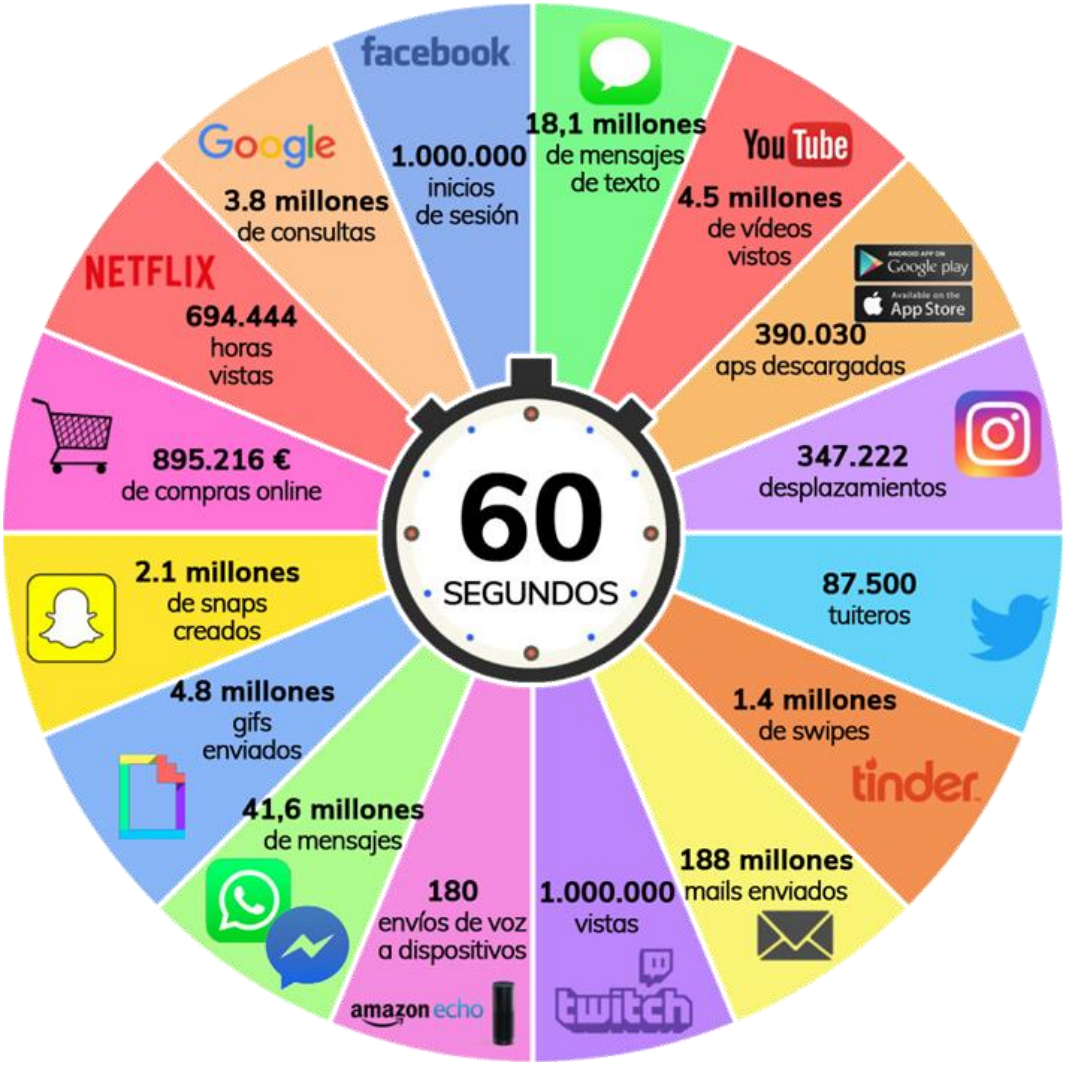


***Figura 3**. Internet en un minuto, 2019.*

Fuente: Trecebits, https://www.trecebits.com/2019/04/03/minuto-internet-infografia

1.1.1. Conceptos.

El concepto de Big Data se aplica para toda aquella información que no puede ser procesada o analizada, utilizando procesos o herramientas tradicionales; de acuerdo con la **Figura 4**, se consideran seis características claves que definen la información relativa al Big Data en referencia a la Seguridad de la información (Lněnička, Máchová, Komárková, & Čermáková, 2017).

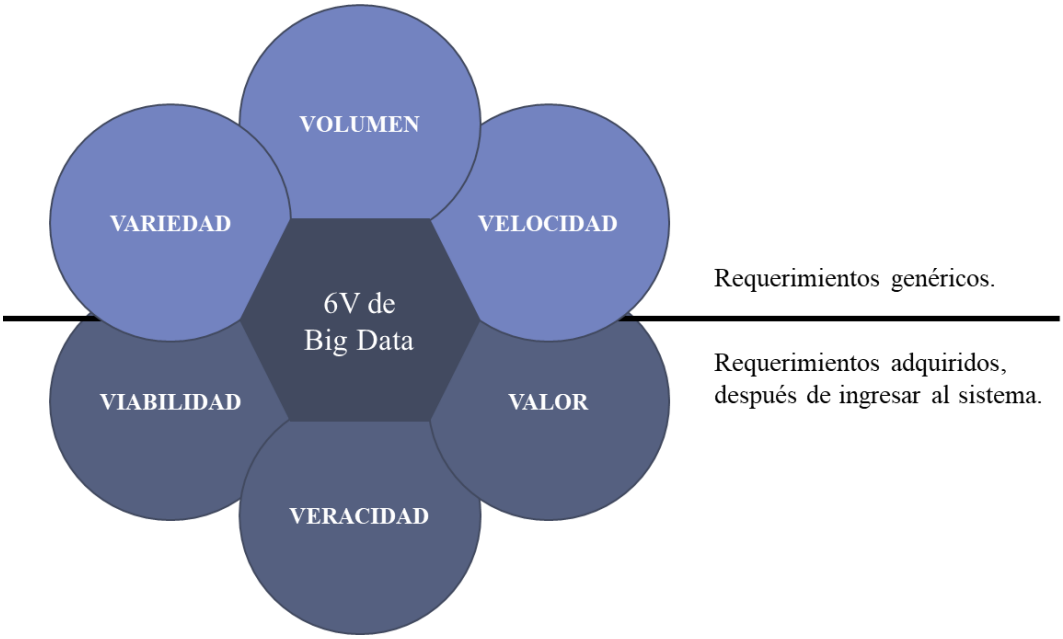


Figura 4. *6V de Big Data.*

Fuente: Lněnička, Máchová, Komárková, & Čermáková, 2017.

1. **Variedad**, una de las principales características de Big Data, son las distintas tipologías y estructuras de los datos procediendo de fuentes muy diversas. El éxito de una organización dependerá en gran medida de resaltar el conocimiento que le propician los distintos tipos de datos de los que dispone. La clasificación más tradicional divide los datos en: estructurados, no estructurados y semiestructurados.

2. **Volumen**, los datos relativos a Big Data se producen en mayores cantidades que los datos tradicionales; por ejemplo, en un Aeropuerto con más de 25000 vuelos de aerolíneas por día, el volumen diario de esta única fuente de datos se contabiliza en el orden de Petabytes, lo que empeora el problema.

3. **Velocidad**, en la toma de decisiones en momentos críticos, el tiempo de respuesta es primordial; en Big Data ocurre algo similar, el procesamiento de los datos debe hacerse en el menor tiempo posible e incluso en el tiempo real para acceder a los datos, con el objetivo de facilitar el análisis y procesamiento. Para el año 2020 se estima que más de 25 mil millones de dispositivos estarán conectados a Internet generando datos en tiempo real; a nivel de los medios sociales, Twitter proporciona alrededor de 8 Terabytes por día, a pesar de que cada tweet solo tiene 140 caracteres.

4. **Valor**, el rédito económico o valor de los diferentes datos varía conforme a su contenido; existe información de gran interés para las organizaciones contenida en conjuntos de datos no estructurados, el desafío esencial es identificar la información valiosa, transformarla y extraer los datos para su posterior análisis. A partir de los datos extraídos y procesados, se puede evaluar el conocimiento contenido en los mismos.

5. **Veracidad**, en Big Data es primordial controlar la integridad de los datos, ya que de esto dependerá el acierto en la toma de decisiones, por lo que es mandatorio el otorgar un alto nivel de fiabilidad a la información recopilada y eliminando posibles eventos

de inexactitud o incertidumbre, esta característica se enlaza con el tratamiento de los datos o limpieza de estos (depuración).

6. **Viabilidad**, se relaciona con la capacidad de las organizaciones para utilizar de manera eficaz el gran volumen de datos que manejan. De esto se derivan conceptos como el de la Inteligencia competitiva, que no es sino la innovación de los equipos de trabajo y el uso de las tecnologías; una organización inteligente analiza, selecciona y monitoriza los datos, con el único objetivo de conocer el mercado en el que opera, sus competidores y clientes, a fin de diseñar estrategias eficaces.

1.1.2. Aplicaciones del Big Data.

Como se describe en la **Figura 5**, Big Data se relaciona con las áreas de conocimiento de Seguridad Informática, Seguridad de red de datos y Seguridad de la información, dentro del entorno de la denominada Industria 4.0, dado que los datos generados por las distintas fuentes de información (internas o externas) deben estar protegidos ante eventos de carácter malicioso o mal intencionado, como son los ataques o amenazas informáticas (Prajakta & Nitin, 2016). En este contexto, este vínculo permite mantener la información de manera segura en el entorno digital. Así también, Big Data y las herramientas de su ecosistema son aplicadas en el análisis, gestión y predicción de eventos de seguridad, detectando y pronosticando posibles amenazas en tiempo real o de manera histórica (Ynzunza Cortés, Izar Landeta, Bocarando Chacón, Aguilar Pereyra, & Larios Osorio, 2017).

El entorno de la Industria 4.0: implicaciones y perspectivas futuras.

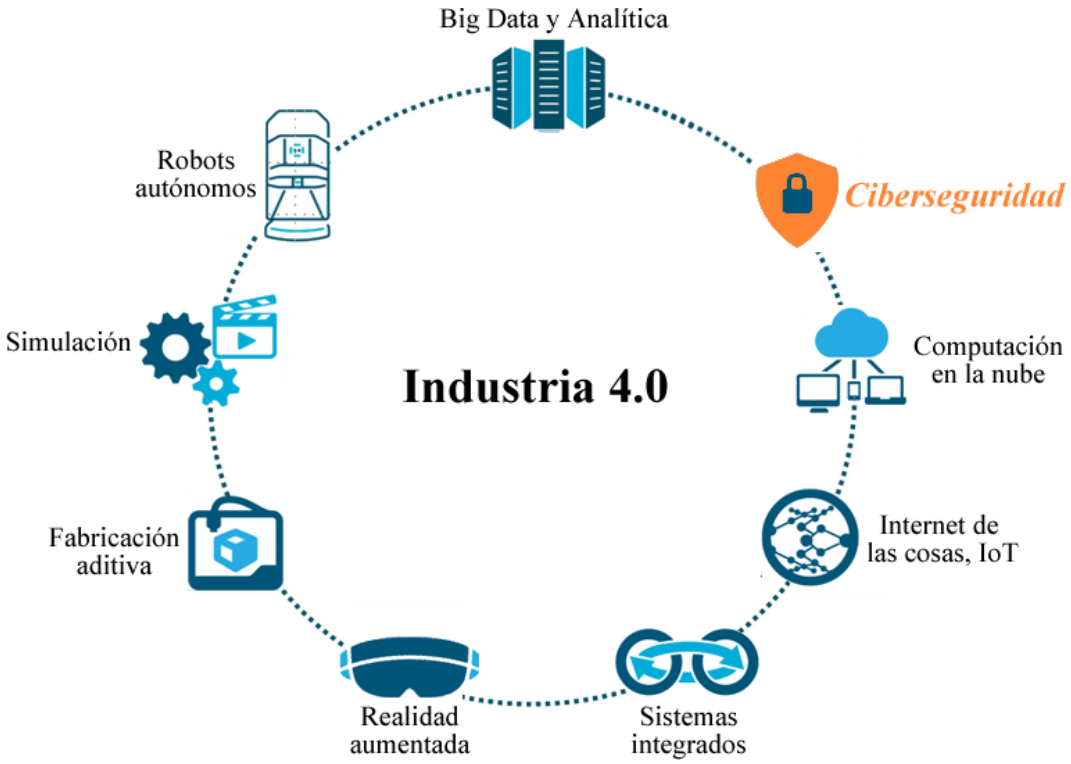


***Figura 5**. El entorno de la Industria 4.0.*

Fuente: Ynzunza Cortés, et al., 2017

La protección y la conservación de la integridad de las fuentes de datos masivas, requiere de Expertos especializados en Seguridad de la información y Análisis de datos, dado que las amenazas informáticas continuamente se diversifican y hacen cada vez más compleja la tarea de mantener una seguridad de extremo a extremo (Sharma & Roji, 2019).

En el entorno de la inteligencia operacional, es necesario gestionar e incrementar servicios claves que permitan a la organización disponer de la capacidad de análisis dinámico de negocios, en tiempo real, ya que esto aporta a una mayor visibilidad y compresión del sentido de las operaciones del negocio, empleando predicciones que integran datos estructurados o

no estructurados con el análisis en comportamientos, sentimientos, ubicación u otros datos (Bajpai, Arya, & Dayanand, 2018).

1. **Análisis predictivo de seguridad**, permiten predecir y prevenir posibles amenazas basándose en el análisis contextual de los datos recopilados de múltiples dispositivos y sistemas de seguridad en Big Data. Al utilizar esta colección y mediante el uso de análisis predictivos, los datos se transforman en conocimientos críticos y percepciones procesables. Sin embargo, el procesamiento analítico predictivo requiere de un alto nivel de recursos tecnológicos, como son grandes espacios de almacenamiento y una gran potencia de procesamiento, así como de personal especializado en Seguridad de la información.

2. **Análisis de decisiones de seguridad**, considerando una metodología que aborda las decisiones importantes de manera formal, lo que ayuda a identificar, representar y evaluar los aspectos importantes de las decisiones y su correspondiente recomendación a los Directivos de las organizaciones para la toma de decisiones, con el objetivo de utilizar los conocimientos para modelar cuantitativamente aspectos importantes de un problema, como su estructura e incertidumbre.

3. **Análisis de diagnóstico de seguridad**, se emplean en el descubrimiento o determinación de eventos inesperados. Además, se relaciona con las herramientas de descubrimiento y visualización de datos para determinar el comportamiento de las tendencias, identificando los factores que afectan directa o indirectamente en el resultado esperado.

4. **Análisis de seguridad del comportamiento del usuario**, se centra en el seguimiento, adquisición y evaluación de los datos basados en las actividades de los usuarios de una organización, permitiendo la identificación de los patrones de información para evidenciar la presencia de criminales informáticos, ciberdelincuentes o intrusos, así como amenazas internas y comportamientos riesgosos en los activos de la información de una organización (Patgiri & Majhi, 2018).

1.2. Fases de Big Data.

Los diferentes tipos de Análisis de seguridad para la identificación de amenazas informáticas siguen un conjunto de fases comunes que permiten la toma de decisiones. Las fases de procesamiento de Big Data se consideran como una serie de pasos que deben seguir las organizaciones durante la gestión de la información (Vallejo Martínez, 2015), como se observa en la **Figura 6**.

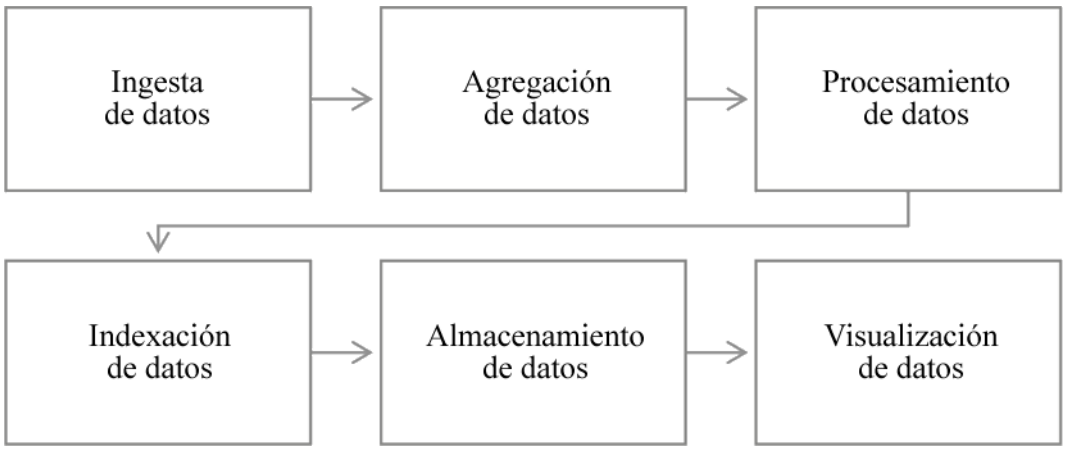


***Figura 6**. Fases de Big Data.*

Fuente: Ynzunza Cortés, et al., 2017

1.2.1. Ingesta de datos.

Se encarga de la recopilación de datos (ingesta) y se considera como elemento de abastecimiento de datos con información potencialmente útil para el análisis de un proceso de negocio, por ejemplo, servidores de datos o aplicaciones, terminales de usuarios, equipos de seguridad, equipos de comunicaciones, entre otros, dicho de otra manera, constituye todos los datos relacionados a eventos o comportamientos en los activos de información de una organización (Berman, 2013).

1.2.2. Agregación de datos y procesamiento.

Su principal función se basa en el procesamiento y transformación de los datos, que se puede almacenar y mostrar de manera más humana. La agregación de datos puede realizarse de forma manualmente o a través de un software especializado.

1.2.3. Indexación y almacenamiento.

Se consideran las tecnologías del ecosistema de Big Data que se refieren al conjunto de aplicaciones, componentes y normas que procesan grandes cantidades de datos, siendo sus resultados elementos, claves para la toma de decisiones. Por otro lado, la indexación y almacenamiento de datos son gestionados por el componente que se encarga del almacenamiento y ejecución de búsquedas sobre la información almacenada de manera ágil y distribuida, en la que toda información se encuentra en nodos de procesamiento, y por tanto, es tolerante a fallos y eventualmente puede disponer de alta disponibilidad (Liu, Li, Li, & Juhnyoung, 2014).

1.2.4. Visualización de datos.

La inteligencia de la arquitectura para identificación de amenazas se apalanca en la aplicación de colectores de información o denominados Agentes, mismos que se tornan en componentes ligeros de software que se integran en las aplicaciones o servicios para enviar la información de eventos de seguridad, por ejemplo, Logs de eventos, métricas, redes de datos, disponibilidad, entre otros. Adicionalmente, para la gestión de datos o visualización de información, se empleará un Dashboard o consola de monitoreo, que se encarga de mostrar toda la información que se tiene almacenada e indexada como datos no estructurados (Lněnička, Máchová, Komárková, & Čermáková, 2017).

1.3. Seguridad de la información.

La información de una organización tiene un gran valor económico, por lo que la gestión de la información corporativa es una disciplina cada vez más importante; esta gestión tiene por objeto maximizar el valor de la información, así como reducir el costo de obtenerla y el riesgo implícito que conlleva.

Como se describe en la **Figura 7**, el valor de la información de una organización está relacionado con la calidad de esta, y la integridad es uno de los componentes que se ubican en la conjunción entre la relevancia, usabilidad y fiabilidad de la información, que junto con la confidencialidad y la disponibilidad forman parte de la tradicional Triada de la seguridad de la información (Figueroa, Rodríguez, Bone, & Saltos, 2017).

Triada de la Seguridad de la información.

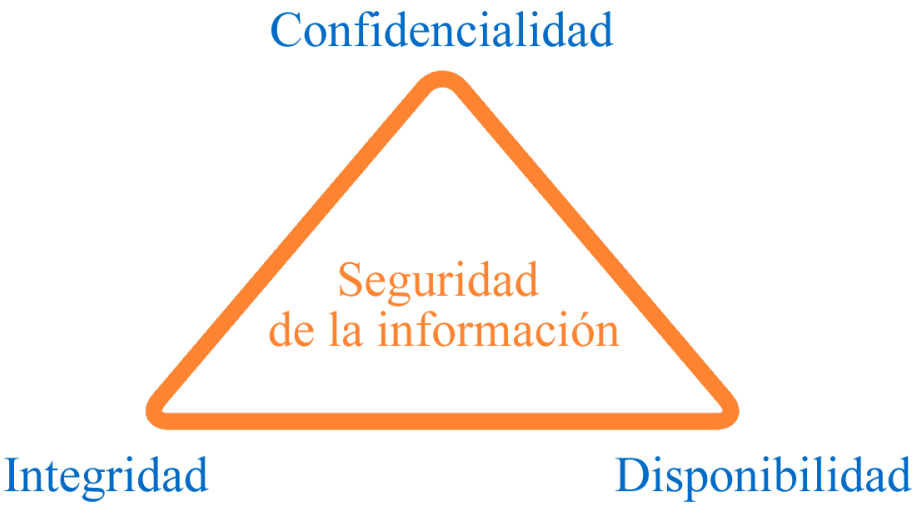


***Figura 7**. Triada de la Seguridad de la información.*

Fuente: Elaboración del autor.

1.3.1. Ciberseguridad y ciberdefensa.

El ciberespacio se define como el ámbito operacional virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y explotación de información digital, a través de redes interdependientes e interconectadas (vinculadas al Internet o no) y el software y firmware de dispositivos asociados a ellas, siendo su carácter distintivo el empleo excluyente de las Tecnologías de Información y Comunicaciones (TIC) y la interacción permanente con los otros ámbitos operacionales (Lucero, 2015).

Se delimita un escenario de conflicto no convencional caracterizado por una libertad de actuación absoluta en el uso de recursos tecnológicos, una presencia sin barreras de tiempo y espacio, y técnicas de acción silenciosas e invisibles. En este escenario se torna compleja la identificación de un criminal o delincuente informático, por cuanto es imperativo un cambio de paradigma, donde debe primar la adaptación permanente a los cambios

tecnológicos para enfrentar nuevas metodologías de ataque con estrategias y medios no habituales, denominada ciberseguridad.

Debido a las amenazas informáticas que surgen de la difusión, uso y aplicación de las nuevas Tecnologías de Información y Comunicaciones (TIC), se deben platear estrategias de ciberdefensa que garanticen las características de confidencialidad, integridad, disponibilidad, autenticidad, duplicidad y no repudio de la información, para permitir la continuidad de las operaciones de los activos de información de misión crítica de las organizaciones (Figueroa, Rodríguez, Bone, & Saltos, 2017).

La ciberdefensa por su lado se representa como una nueva dimensión de conflicto, que origina la necesidad de establecer nuevos modos de acción, estrategias y acuerdos a nivel internacional. Las personas, organizaciones privadas y públicas, no pueden estar ajenos a esta realidad y deben tomar las medidas adecuadas para precautelar los bienes, recursos y el normal funcionamiento de la sociedad. La implementación de una estrategia de ciberdefensa se muestra como la forma idónea de mitigar el impacto de las nuevas amenazas informáticas (Sorrentino, 2018), como se observa en la **Figura 8**.

Ciberseguridad y ciberdefensa.

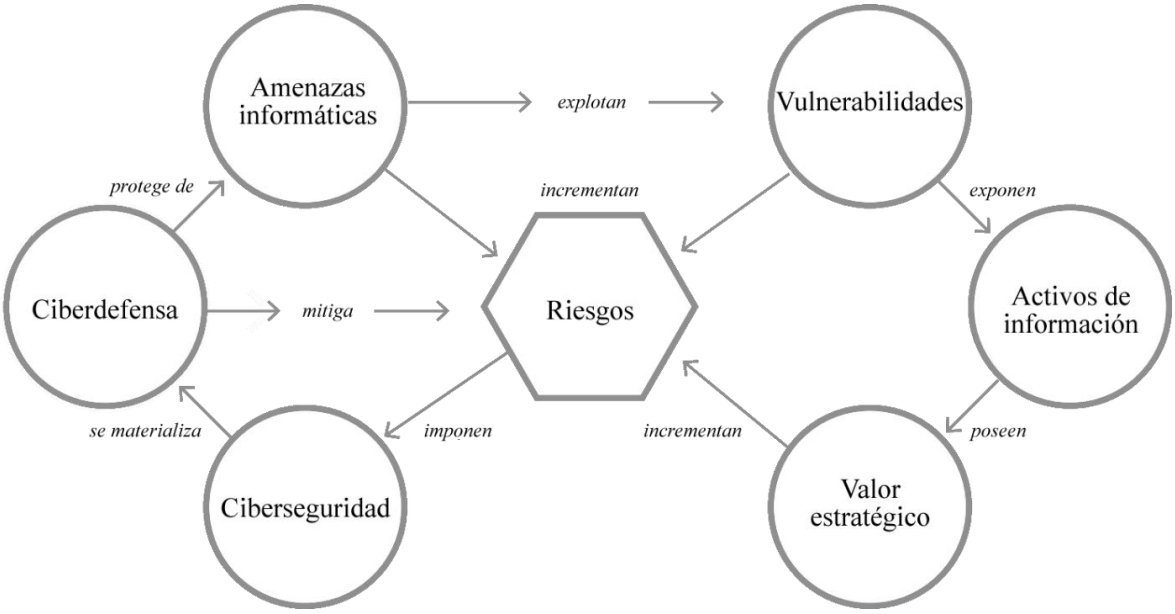


Figura 8. *Ciberseguridad y ciberdefensa.*

Fuente: Sorrentino, Pablo, 2018.

1.3.2. ¿Cómo el Big Data ayuda a la ciberseguridad?

Existe una gran relación entre el Big Data y la ciberseguridad, una tecnología que cada vez se está utilizando más debido al desarrollo constante que está experimentando el mundo digital. Debido a esto, cada vez se precisa de más profesionales que sean capaces de mantener la seguridad de todo el entorno digital y de ofrecer los recursos necesarios para que las personas y las organizaciones tengan la certeza que sus datos están a buen resguardo.

1.3.3. ¿Qué relación existe entre Big Data y ciberseguridad?

Las amenazas y ataques informáticos son habituales hoy en día; el 99 por ciento de los terminales de usuario final que existen en el mundo, son vulnerables a los ataques

informáticos. Por esta razón, Big Data y la ciberseguridad son muy importantes para garantizar que se mantiene la seguridad de los datos que pertenecen a las organizaciones.

Big Data ayuda a pronosticar y anticipar lo que está por venir, realizando un análisis de toda la información que se tiene para poder detectar y evitar posibles ataques informáticos. Esta tecnología también permite identificar irregularidades y posibles violaciones de la seguridad de la red de datos corporativa. Bajo este criterio, Tounsi & Rais (2018) afirma:

La tecnología Big Data, aparte de ofrecer una gran capacidad operativa a la hora de procesar grandes volúmenes de datos y analizarlos, también permite identificar a personas mal intencionadas u organizaciones delictivas que actúen en contra de la integridad de los mismos. Esto implica que las personas con intenciones de vulnerar la privacidad de los datos, piensen dos veces antes de cometer alguna acción que ponga en peligro la información de otras personas u organizaciones.

Big Data puede proteger a las organizaciones, logrando que sea más complejo que los datos importantes del funcionamiento interno del negocio se filtren; todo apunta que, en un futuro no muy lejano la mayoría de las organizaciones tendrán que utilizar la ciberseguridad que aporta la tecnología Big Data. Esta tecnología permitirá que la gestión de tareas y operaciones internas que se realizan en la organización sean plenamente aseguradas.

1.3.4. Tipos de amenazas informáticas.

La Inteligencia de Negocios (BI, Business Intelligence) aplicando herramientas del ecosistema de Big Data, permiten a las organizaciones el reforzar sus tres niveles de protección tecnológica (Masabo, Swaib, & Sansa-Otim, 2018):

1. **Amenazas conocidas**, corresponden a las amenazas o fallos en infraestructura tecnológica que crean debilidades en la seguridad global de una organización. Las vulnerabilidades también pueden producirse por configuraciones inadecuadas software o de la seguridad; los criminales informáticos explotan estas debilidades, causando daños a la infraestructura o la información.

    a. **Botnet**, es un programa que le permite a un criminal informático o ciberdelincuente, tomar el control de un terminal de usuario infectado. Por lo general, son parte una red de equipos afectadas denominados botnets. Los equipos infectados son conocidos como zombies y pueden usarse para llevar a cabo un ataque masivo de denegación de servicio (DDoS).

    b. **Phishing**, amenaza generada cuando un usuario recibe un correo electrónico y accede a una página web fraudulenta que simula ser un sitio legítimo, creando copias similares de sitios web e incluso usando imágenes corporativas originales. Dentro de los usos que se le da a este tipo de amenazas, están la obtención de credenciales privadas a diferentes sitios (bancos, tiendas en línea, entre otros), así como engañar a la persona para infectar dispositivos con algún tipo de malware o robar identidades (secuestro digital) para cometer delitos.

c. **Virus**, se presentan como un programa aparentemente legítimo e inofensivo, que al ejecutar puede ocasionar daños severos a la infraestructura tecnológica; tiene por objeto alterar el normal funcionamiento un dispositivo sin el permiso o conocimiento del usuario.

d. **Gusanos**, son amenazas capaces de copiarse a sí mismos una y otra vez incluso infectando otros dispositivos enviando copias de sí mismos; no se apropian del control de un terminal de usuario, sino que influyen tanto en su funcionamiento como en el de la red de datos corporativos.

e. **Keylogger**, existen dos tipos de ataques y su función es capturar las pulsaciones del teclado ya sean estos físicos o digitales; los primeros consisten en dispositivos que se instalan entre el teclado y el terminal del usuario, mientras que otro puede ser un programa que se ejecuta sin conocimiento del usuario. Se enfoca principalmente en conseguir datos o credenciales sensibles para la seguridad.

f. **Exploits**, es una amenaza informática que ataca una vulnerabilidad de sistema informático o de un software determinado; se instalan en equipos corporativos como en servidores o terminales de usuario con el fin de acceder a información específica. En muchos casos los exploits dependen de que el usuario atacado realice una acción determinada como por ejemplo abrir un archivo o dar click en un enlace (link).

g. **Backdoor**, como su nombre lo indica es una puerta trasera que existe en algunos sistemas informáticos que permiten el acceso remoto a la infraestructura tecnológica. En ocasiones se acceden a los datos sin que las protecciones de los sistemas las identifiquen.

2. **Amenazas desconocidas**, el riesgo de sufrir un ataque por un virus, spyware, troyanos y otros programas maliciosos, se incrementa diariamente, sin embargo, las vulnerabilidades de los sistemas informáticos e infraestructura tecnológica frente a ataques de amenazas nuevas y desconocidas se incrementa exponencialmente.

   a. **Amenazas persistentes avanzadas (ATP, Advanced Persistent Threat)**, son amenazas nuevas que aparecen antes de que los proveedores de soluciones de seguridad publiquen la protección específica para su mitigación. Los programas maliciosos pueden aprovechar vulnerabilidades de los sistemas informáticos y de las aplicaciones para sus ataques.

   b. **Ransomware**, es uno de los más sofisticados y modernos ataques informáticos, el cual secuestra los datos de una organización y los encripta, con la finalidad de pedir un rescate por ellos. Normalmente, se solicita una transferencia en dinero electrónico (bitcoins), para evitar el rastreo y localización del atacante. Este tipo de amenaza va en aumento y es uno de los más temidos por las organizaciones, en la actualidad.

c. **Ataques de día cero (Zero-day)**, las amenazas nuevas que aparecen antes de que los proveedores de seguridad publiquen protección específica se denominan amenazas de día cero. Los programas maliciosos pueden aprovechar vulnerabilidades de los sistemas y de las aplicaciones para sus ataques. Cuando se identifica un agujero de seguridad en algún programa, el proveedor suele desarrollar un parche para protegerlo contra posibles ataques.

1.3.5. Evaluación del impacto de una amenaza.

Análisis de impacto y factores de riesgos informáticos, se determina el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad (Oseku-Afful, 2016). Se pueden considerar los siguientes aspectos:

1. **Consecuencias de tipo financiero**, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias de que este activo no funcione, y afecte la operación de la organización.

2. **La importancia crítica de los datos y el sistema informático**, considerando la importancia para la organización, así como la sensibilidad de los datos y el sistema afectado.

3. **Evaluación de riesgo, se identifican las amenazas, vulnerabilidades y riesgos**, sobre la infraestructura tecnológica de una organización, con el fin de generar un Plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad (*Triada de*

la Seguridad de la información). Para el efecto se deben consideran los siguientes puntos:

a. La probabilidad de explotación de una amenaza.
b. La magnitud del impacto sobre el sistema informático.

Su integración en la organización y en la arquitectura global de Seguridad de la información, permitirá desarrollar nuevas herramientas y marcos de trabajo que no solamente lleguen hasta el origen de la amenaza, sino que también acercar y coordinar a las diferentes técnicas de mitigación global de los riesgos por parte de los equipos de respuesta a incidentes (IRT, Incident Response Team).

1.3.6. Nuevos desafíos.

En la actualidad, las organizaciones recopilan de forma rutinaria grandes volúmenes de datos de gran importancia para la seguridad de la información a nivel de sus activos de información de misión crítica, por ejemplo: eventos de la red de datos, eventos de aplicaciones de software o eventos del actuar de sus colaboradores sobre las plataformas corporativas, lo que supone un problema para almacenar la información de manera conveniente. Según indica Cloud Security Alliance: “una empresa como Hewlett Packard puede generar un trillón de eventos por día, y al menos 12 millones de eventos por segundo” (Cloud Security Alliance, 2013).

Con la intención de incluir el mayor número de líneas de investigación, Cloud Security Alliance señaló las áreas de investigación a nivel de la Seguridad de la información aplicando técnicas de Big Data:

a. Aseguramiento y validación de cálculos basados en programación distribuida, métricas y monitoreo del rendimiento de los sistemas informáticos.

b. Aplicación de las mejores prácticas a nivel de la Seguridad de la información para motores de bases de datos no estructuradas.

c. Almacenamiento seguro de datos y registros de transacciones de gran tamaño, desarrollo de herramientas de protección, diagnóstico de daños y contingencia.

d. Monitoreo de seguridad en tiempo real para amenazas persistentes avanzadas (APT) aplicando técnicas de lenguaje de máquina (Machine Learning).

e. Minería y análisis de datos escalables para preservar la privacidad, investigación en estrategias y mecanismos de protección de la privacidad.

f. Seguridad de la información centrada en la encripción de los datos, aplicando tecnologías basadas en la experiencia del usuario y su interacción.

g. Control de acceso granular para colaboradores de las organizaciones, gestión de la identidad basada en controles de acceso, contraseñas y sistemas de seguridad adaptados a patrones de uso.

h. Análisis forenses a gran escala sobre los activos de la información de misión crítica, estudio del software malicioso y búsqueda de su origen.

1.4. Gestión de eventos de seguridad (Event Management).

Se aplica generalmente en sistemas de monitoreo donde los registros de eventos son detectados por los sensores o colectores de información. La gestión de eventos de seguridad consiste en la investigación, interpretación y procesamiento posterior de los datos obtenidos.

Las razones más habituales para el análisis de los eventos de seguridad se deben a aspectos, tales como:

a. Seguridad.
b. Regulación o normativa.
c. Solución de problemas.
d. Investigación.
e. Respuesta automática de incidentes.

Existen tipos básicos de registros de eventos que son utilizados por los servicios de los componentes de infraestructura; estos pueden variar según el tipo de componente de infraestructura, su versión, o el evento presentado (Ezzikouri, Erritali, & Oukessou, 2015).

También existen múltiples registros de eventos generados en función de su evento de activación, contenido y lógica, algunos ejemplos son:

1. **Registros de errores**.

```
Sat Apr 20 13:41:49 2019 [error] [client 192.168.1.] SoftException in Application.cpp:601: Directory “/home/userdemo/public_html is writeable by group.
```

2. **Registros de acceso**.

```
Sat Apr 20 17:53:12 centos nagios3: Caught SIGTERM, shuttingdown...! Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from 169.223.1.130 port 2039 ssh2
```

3. **Registros de seguridad**.

```
Sat Apr 20 17:37:12 ids4 snort [776]: [1:1156:13] WEB-MISC apache directory disclosure attempt [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} 10.2.1.99:41337 -> 192.168.1.1:80
```

4. **Registros canalizados**.

```
Apr 20 04:40:11.788 SERVER: %SEC-6-IPACCESSLOGP: list 100 deniedtcp79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet!Sep 1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from consoleby pr on vty0 (203.200.80.75)!%CI-3-TEMP: Overtemperaturewarning!Mar 1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changedstateto down!
```

Los formatos de registro de eventos típicos son estandarizados por la NCSA (National Certer for Supercomputing Applications), los cuales se basan en el servicio HTTPd de NCSA y se aplica principalmente como estándar para los contenidos de registro de servidores aplicaciones Web (HTTP).

También existen tipos específicos de formatos NCSA, como son:

a. **NCSA Common (también conocido como registro de acceso)**, contiene solo información básica de acceso HTTP.

b. **Formato de registro combinado de NCSA**, es una extensión del formato NCSA común ya que contiene la misma información con campos adicionales (referente, agente de usuario y campo de cookie).

1.5. Security Information and Event Management Systems (SIEM).

1.5.1. Características.

En la actualidad, resulta compleja la tarea de identificar los ataques informáticos que se presentan en las organizaciones; sin embargo, los Sistemas de seguridad de la información y gestión de eventos (SIEM) permiten la automatización de la gestión de la seguridad de la red de datos corporativa.

Hoy en día, la gestión y el tratamiento de las amenazas informáticas es uno de los aspectos más importantes a considerar por parte de las organizaciones modernas, dedicando los recursos necesarios para poder responder a cualquier incidente de seguridad que surja. Los

Sistemas de seguridad de la información y gestión de eventos (SIEM) actúan como un repositorio o contenedor de datos, registrando todos los eventos de los activos de información, que se relacionan con la seguridad, usándolos para monitorear, identificar, documentar e incluso responder a dichos incidentes de seguridad (Lobo & Flórez, 2017).

Algunos de los incidentes de seguridad son claros y su identificación podría ser sencilla, pero una gran parte de los incidentes de seguridad, aunque puedan ser obvios, se esconden detrás de la gran cantidad de eventos por segundo que se producen en los activos de información de la organización, y que sin un Sistemas de seguridad de la información y gestión de eventos (SIEM) serían completa o parcialmente inadvertidos.

Una de las grandes propiedades de Sistemas de seguridad de la información y gestión de eventos (SIEM), se basa en la reducción de falsas alertas o falsos positivos, frecuentemente producidos, por ejemplo, a través de sistemas de detección de intrusiones (IDS). La reducción de falsas alertas viene de la mano de la filtración y correlación de eventos de seguridad producidas por el Sistemas de seguridad de la información y gestión de eventos (SIEM), discriminando con precisión aquellas situaciones que los sensores las catalogan de incidentes de seguridad, sin realmente serlo en muchos de los casos.

1.5.2. Funcionalidades claves.

Las Sistemas de seguridad de la información y gestión de eventos (SIEM), tanto comerciales como Open source, comparten puntos en común que son relevantes para su operación:

1. Visualización centralizada de amenazas informáticas potenciales.

2. Indagación de qué amenazas informáticas requieren resolución y cuáles se consideran falsos positivos.

3. Procedimientos de escalamiento ante eventos de carácter malicioso a los Expertos de Seguridad de la información para que puedan accionar de manera oportuna.

4. Inserción del contexto de los eventos de seguridad, con la finalidad de elaborar un marco de resolución de incidentes estructurado y detallado.

5. Establecimiento de procesos documentales durante y después de las actividades de identificación de amenazas informáticas, así como de los distintos registros de auditoría, eventos detectados y cómo fueron resueltos.

6. Cumplimiento con las normativas o regulaciones de la industria, en un formato de reporte comprensible, por ejemplo: el Estándar de Seguridad de datos para la Industria de Tarjeta de Pago (PCI DSS), el Reglamento General de Protección de Datos de la Unión Europea (RGPD), la Ley Sarbanes Oxley de los Estados Unidos (SOX), la Ley de Portabilidad y Responsabilidad del seguro médico (HIPAA), entre otras normativas).

1.5.3. Detección y alerta de amenazas informáticas.

La Seguridad de la información aplicando herramientas del ecosistema de Big Data ayuda a las organizaciones a contrarrestar las amenazas informáticas y ataques antes de que generen eventos de seguridad, aplicando estrategias con capacidades de:

a. **Visibilidad**, completa para los activos de información de la organización, permitiendo capturar y analizar grandes volúmenes de datos de seguridad relevantes.

b. **Analítica de datos sofisticada para procesar los datos**, identificando posibles amenazas informáticas y alertando a las organizaciones sobre posibles eventos vinculados con los activos críticos de información.

c. **Activación de procesos de respuesta ante incidentes (IR)**, aumentando la eficacia y eficiencia durante la investigación y mitigación de las amenazas informáticas.

1.5.4. Marco de ciberseguridad NIST.

El marco de referencia de ciberseguridad NIST correspondiente al Instituto Nacional de Estándares y Tecnología de los Estados Unidos de Norteamérica (NIST, por sus siglas en inglés, National Institute of Standards and Technology) fue concebido bajo el Decreto Ejecutiva 13636 y cuyo objetivo es mejorar la seguridad de la infraestructura de misión crítica de la Nación frente a los ataques cibernéticos o informáticos (NIST, 2019).

Aunque está orientado a las organizaciones que disponen infraestructura crítica, el marco de referencia en mención es una guía muy útil para cualquier organización que desee mejorar su gestión a nivel de Seguridad de la información, como se observa en la **Figura 9**.

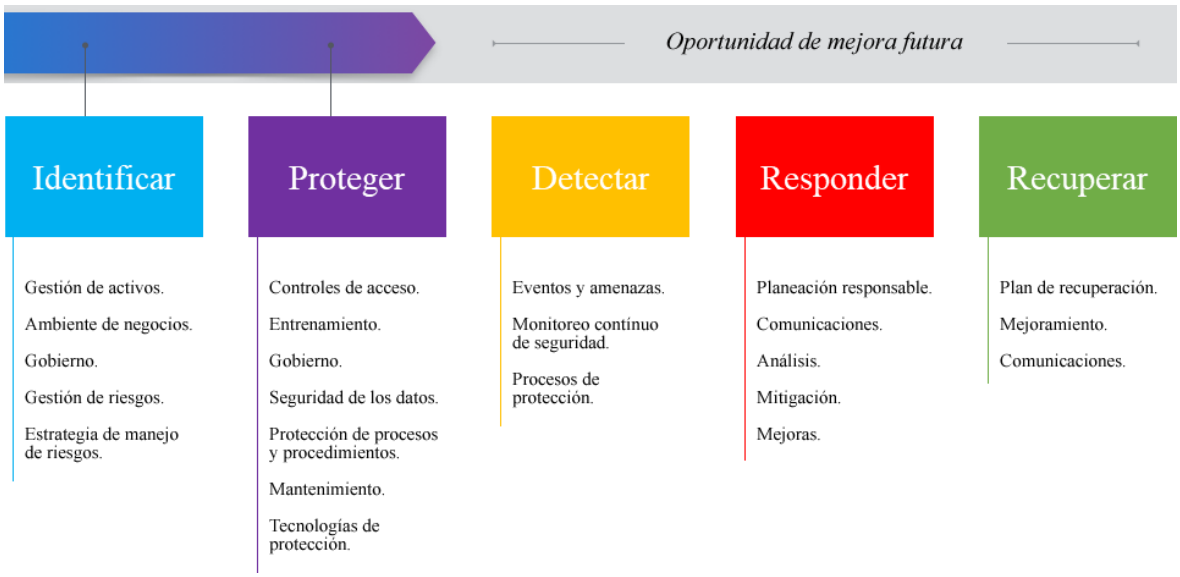


***Figura 9**. Marco de referencia de ciberseguridad NIST.*

Fuente: NIST, 2019.

El marco de referencia de ciberseguridad NIST, se compone de:

a. **Marco básico de referencia (Framework Core)**, describe las funciones de un Programa de Seguridad de la información, que corresponde a la *identificación*, *protección*, *detección*, *respuesta* y *recuperación* ante la presencia de una amenaza informática; así también, el marco de referencia no se contrapone ni excluye a otros estándares, marcos de referencia o manuales de buenas prácticas de la industria como NIST 800-53 y COBIT 5 / COBIT 2019.

b. **Niveles de implementación del marco (Framework Implementation Tiers)**, permiten a la organización clasificarse en función de las prácticas actuales de gestión de riesgo, el entorno de las amenazas informáticas, los requerimientos legales y normativos, los objetivos y misión del negocio, y las restricciones de la organización, siendo los niveles definidos como parcial, riesgos informados, repetible y adaptativo.

c. **Perfiles del marco de referencia (Framework Profiles)**, se utilizan para interpretar el estado actual (Current Profile) y el estado objetivo (Target profile) de las actividades específicas de la Seguridad de la información.

1.5.5. Arquitectura referencial.

Un Sistema de seguridad de la información y gestión de eventos (SIEM) representa una estructura tecnológica compleja, con componentes que se interconectan de forma física y lógica.

A continuación, en la **Figura 10** se ilustra la arquitectura referencial de un Sistemas de seguridad de la información y gestión de eventos (SIEM) con sus funcionalidades claves; no obstante, no es imprescindible que todas las funcionalidades descritas se encuentren en el sistema, pero si es aconsejable su integración por motivos de complemento operativo de la plataforma de seguridad de la información.

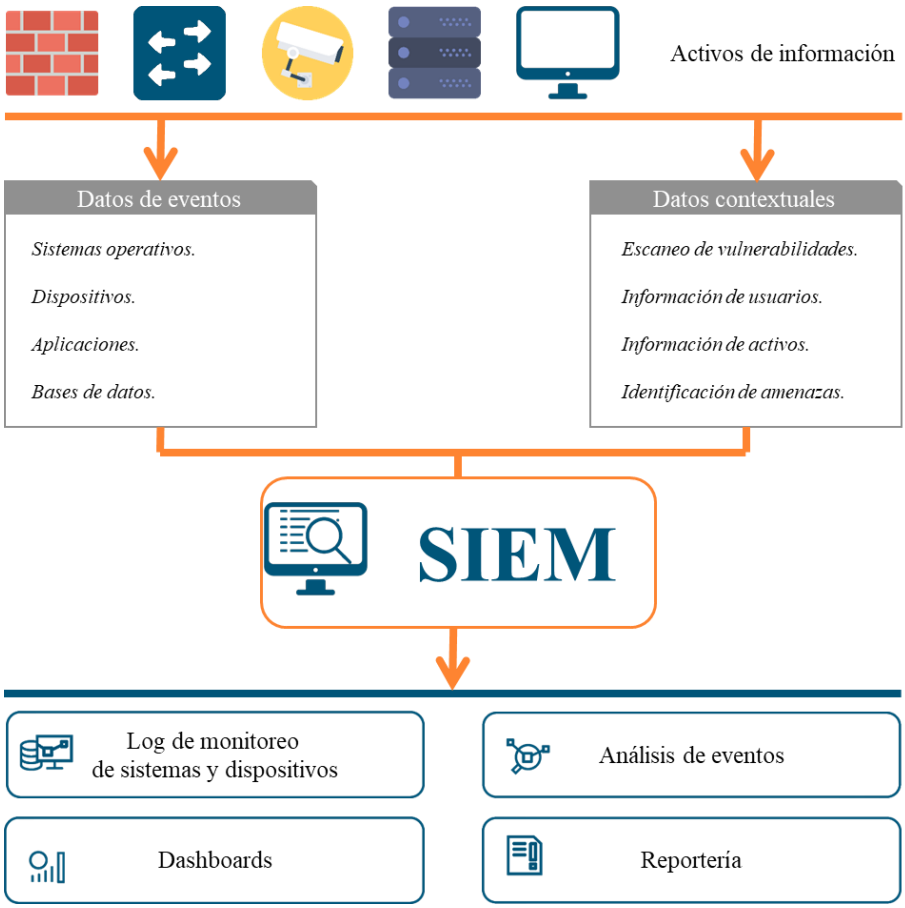


***Figura 10**. Arquitectura referencial de un SIEM.*

Fuente: Elaboración del autor.

Capítulo 2

Solución propuesta

2.1. Security Operation Center (SOC).

2.1.1. Definición y misión.

En los Centros de Operaciones y Monitoreo de Seguridad de la información (SOC), destacan las actividades de seguimiento y análisis de la actividad en equipos de comunicaciones (switch, router, firewall, NAC, IPS / IDS, entre otros), servidores de aplicaciones y bases de datos, terminales de usuario final, y otros activos de información, en búsqueda de actividades anómalas que indiquen de un posible evento o compromiso de seguridad (Netsecurity, 2018).

Miloslavskaya (2018) afirma que un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) es responsable de garantizar que los eventos de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente, conforme al Modelo referencial descrito en la **Figura 11**.

Sus objetivos principales se centran en:

1. Incrementar la capacidad de vigilancia y detección ante amenazas informáticas conocidas o no, en las actividades rutinarias de los activos de información.

2. Analizar los ataques o potenciales amenazas informáticas.

3. Recuperar información perdida o comprometida de la organización por consecuencia de las amenazas informáticas.

4. Incrementar la capacidad de respuesta ante incidentes ocasionados por la presencia de amenazas informáticas.



Figura 11. *Modelo referencial de un SOC.*

Fuente: Netsecurity, 2018.

2.1.2. Instrumentación.

Conforme al planteamiento de la gestión cíclica de la Seguridad de la información para las organizaciones aplicando la estrategia de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), se identifican las fases clave que conforman las bases de su instrumentación:

1. **Métricas e indicadores de compromiso de seguridad**, se plantea la valoración selectiva y cualitativa de los activos de información de la organización, que son vigilados a nivel del Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

2. **Recopilación de datos**, comprende el despliegue de los sensores o agentes de monitoreo para obtener una cantidad suficiente de datos relevantes de las fuentes de información.

3. **Detección de amenazas informáticas**, conforme con un estudio de valoración de los activos de información y clasificación de las potenciales amenazas informáticas, se platean los criterios que involucran el cálculo del índice de riesgo de la organización y sus activos.

4. **Análisis de incidentes de seguridad**, por medio de la correlación cruzada de las fuentes de información, los eventos almacenados y los datos procesados, se aplican técnicas de Inteligencia de Negocios para determinar incidentes de seguridad.

5. **Acción y mitigación**, bajo la intervención de un operador humana o automatizado, se direccionan los incidentes evaluados al equipo de Expertos y Analistas de Seguridad de la información para su mitigación; bajo esta premisa se obtienen acciones de remediación y se comunican los siguientes pasos para la mitigación del evento.

6. **Respuesta ante incidentes de seguridad**, se centra en la toma de decisiones informadas para la minimización del impacto y riesgo potencial; en ciertos casos esta respuesta puede ser drástica para mitigar la amenaza informática identificada o permisiva de acuerdo con los lineamientos de la organización según el marco de referencia aplicado (NIST, ISO 27001, ISO 27002).

2.1.3. Personas, habilidades y competencias.

De acuerdo a la estructura orgánica – funcional, se presenta la estructura de roles para un equipo de trabajo multidisciplinario de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC):

1. **Gerente del Centro de Operaciones de Seguridad (SOC)**, con formación de nivel superior y especialización en Seguridad de la información, así como también en servicios de Consultoría en Seguridad Informática.

2. **Líder del equipo**, gestión coordinada de las actividades y funciones del equipo del Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), con

formación, entrenamiento y desarrollo de habilidades necesarias para dirigir el equipo a cargo.

3. **Investigador Líder**, recopila y analiza toda la evidencia, a fin de determinar la causa raíz de un incidente de seguridad crítico, dirige a otros analistas de seguridad e implementa de manera eficiente estrategias de recuperación del servicio.

4. **Analistas de seguridad**, realiza el análisis de los incidentes presentados en los activos de información de una organización. Identifica, evalúa y aplica herramientas que permitan el análisis de vulnerabilidades, así como elabora reportes e informes de carácter técnico, que permitan aportar a los Planes estratégicos de seguridad de la información de los clientes.

5. **Operadores de monitoreo y control**, personal delegado al monitoreo de las consolas de identificación de amenazas informáticas, a fin de identificar y notificar posibles eventos de seguridad a los Analistas de seguridad. Aplican políticas y procedimientos según estándares internacionales y buenas prácticas de la industria, mientras ejecutan el seguimiento de los incidentes presentados.

6. **Ejecutivo de calidad**, coordinación y registro de actividades diarias de personal del Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), además de mantener una comunicación efectiva con el cliente, permitiendo evaluar el grado de satisfacción por el servicio brindado.

2.2. Diseños de la solución propuesta.

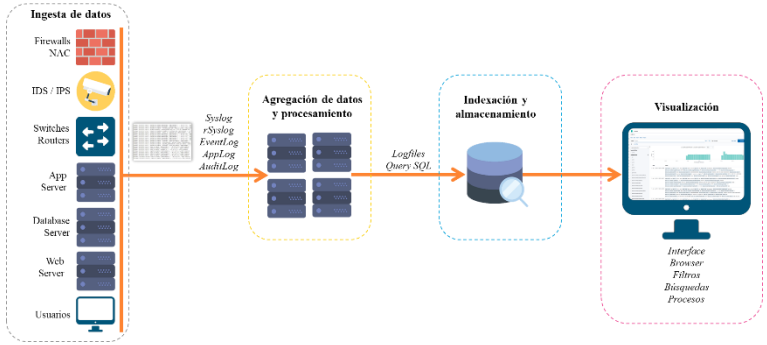
El diseño de una arquitectura tecnológica se basa en la especificación de uno o varios objetos creados por el Autor del desarrollo del proyecto, buscando alcanzar los objetivos planteados en la investigación, a través de un entorno particular y usando un conjunto de componentes básicos que satisfagan los requerimientos funcionales que se ciñan con restricciones específicas.

Derivado de la generación del inventario de datos a analizar y en conformidad con la investigación, la evaluación de brechas de Seguridad de la Información aplicando una arquitectura tecnológica – empresarial que permita la implementación de herramientas del ecosistema de Big Data para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), puede evaluarse desde las siguientes perspectivas arquitectónicas, a saber:

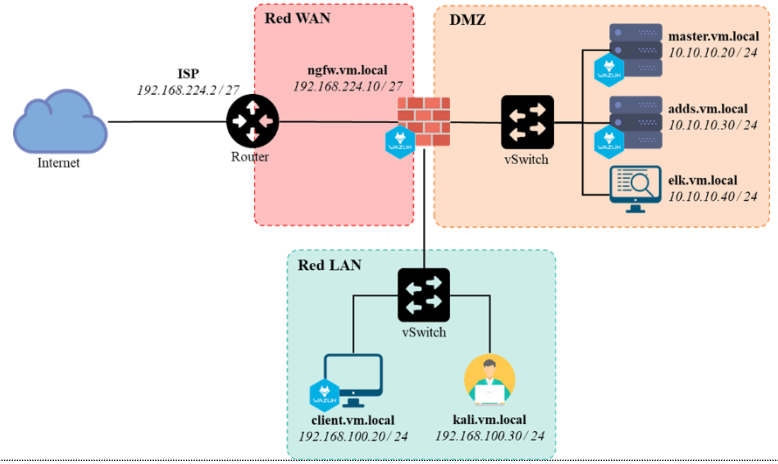
a. Arquitectura de procesos.
b. Arquitectura de infraestructura tecnológica
c. Arquitectura de software.
d. Arquitectura del negocio.

Para la comprensión y entendimiento de la solución propuesta, se propone en la **Figura 12**, el diagrama consolidado de perspectivas arquitectónicas establecidas en la investigación.

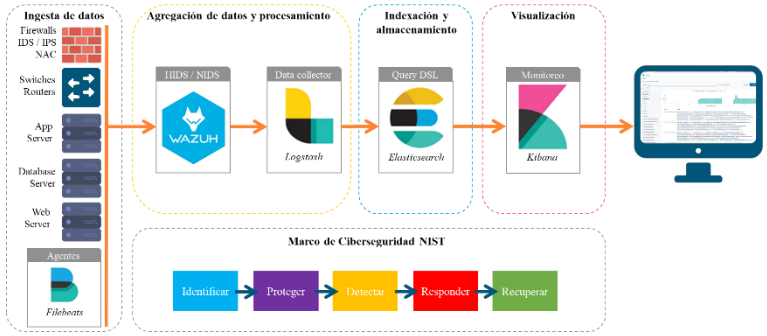
a. Arquitectura de procesos.



b. Arquitectura de infraestructura tecnológica.



c. Arquitectura de software.



d. Arquitectura del negocio.

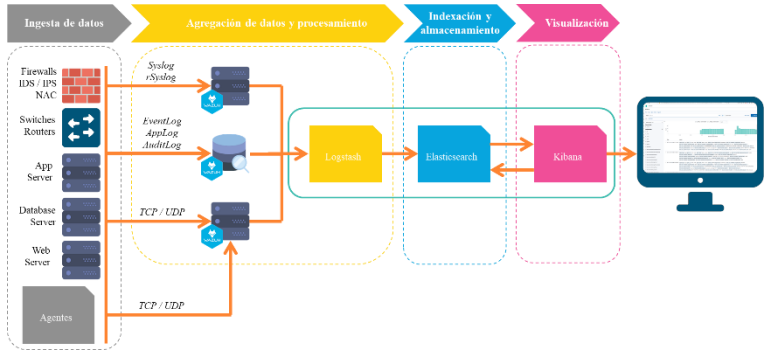


Figura 12. *Consolidado de perspectivas arquitectónicas de la solución propuesta.*

Fuente: Elaboración del autor.

2.2.1. Arquitectura de procesos.

Se plantea garantizar que una organización automatice sus procesos de negocio, considerándose como la definición global de un sistema de procesos orientados a la Seguridad de la información. En la **Figura 13**, se definen los lineamientos estructurales que delinearán los procesos subyacentes que conforma la arquitectura planteada:

a. **Ingesta de datos**, se recopilan los datos con información potencialmente útil para el análisis de eventos de seguridad de la información, desde los activos de información como servidores de datos o aplicaciones, terminales de usuarios, equipos de seguridad, equipos de comunicaciones, entre otros, en formato de eventos (Logs).

b. **Agregación de datos**, una vez procesados y transformados los datos, estos son almacenados de manera entendible para el ser humano.

c. **Indexación y almacenamiento**, este proceso se gestiona por el componente encargado de la ejecución de las búsquedas sobre la información almacenada en el nodo de almacenamiento distribuido.

d. **Visualización**, la arquitectura para identificación de amenazas informáticas, para la gestión de datos o visualización de la información, emplea un Dashboard que se encarga de mostrar toda la información que se tiene almacenada e indexada como datos no estructurados.

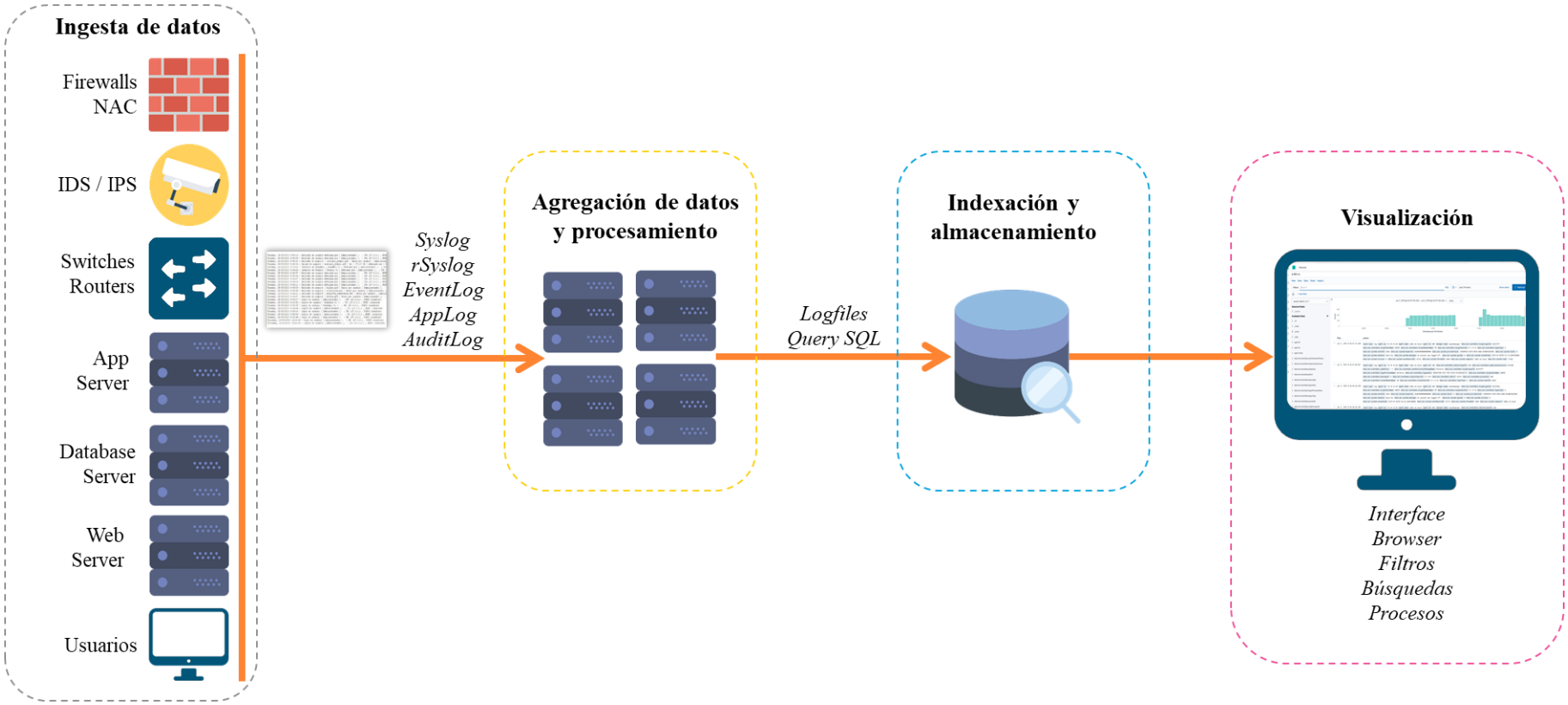


Figura 13. *Arquitectura de procesos.*

Fuente: Elaboración del autor.

2.2.2. Arquitectura de infraestructura tecnológica.

Se considera al conjunto de hardware y software sobre el que se implementan los diferentes servicios tecnológicos que una organización precisa tener en funcionamiento, para llevar a cabo toda su actividad, tanto de negocio como de gestión interna orientada a la Seguridad de la información. En la **Figura 14**, se plantea la arquitectura de infraestructura tecnológica que servirá de modelo para la identificación de ataques o amenazas informáticas.

La arquitectura propuesta permite establecer un marco para la especificación de los componentes físicos y lógicos de una red de datos corporativa, su distribución funcional y configuración, así como sus procedimientos y principios operacionales, que junto con los formatos de los datos utilizados intervienen en su funcionamiento.

La especificación de la arquitectura de infraestructura tecnológica propuesta incluye una descripción detallada de los componentes y servicios entregados a través de una red de datos corporativa, segmentada en redes funcionales según las mejores prácticas:

a. **Red WAN (RED)**, por sus siglas en inglés de Wide Area Network o Red de Área Extendida, que permite el servicio de acceso a Internet por parte de un proveedor.

b. **Red DMZ (ORANGE)**, Zona Desmilitarizada o red de servidores.

c. **Red LAN (GREEN)**, por sus siglas en inglés de Local Area Network o Red de Área Local, cuyo propósito es la interconexión de los usuarios corporativos.

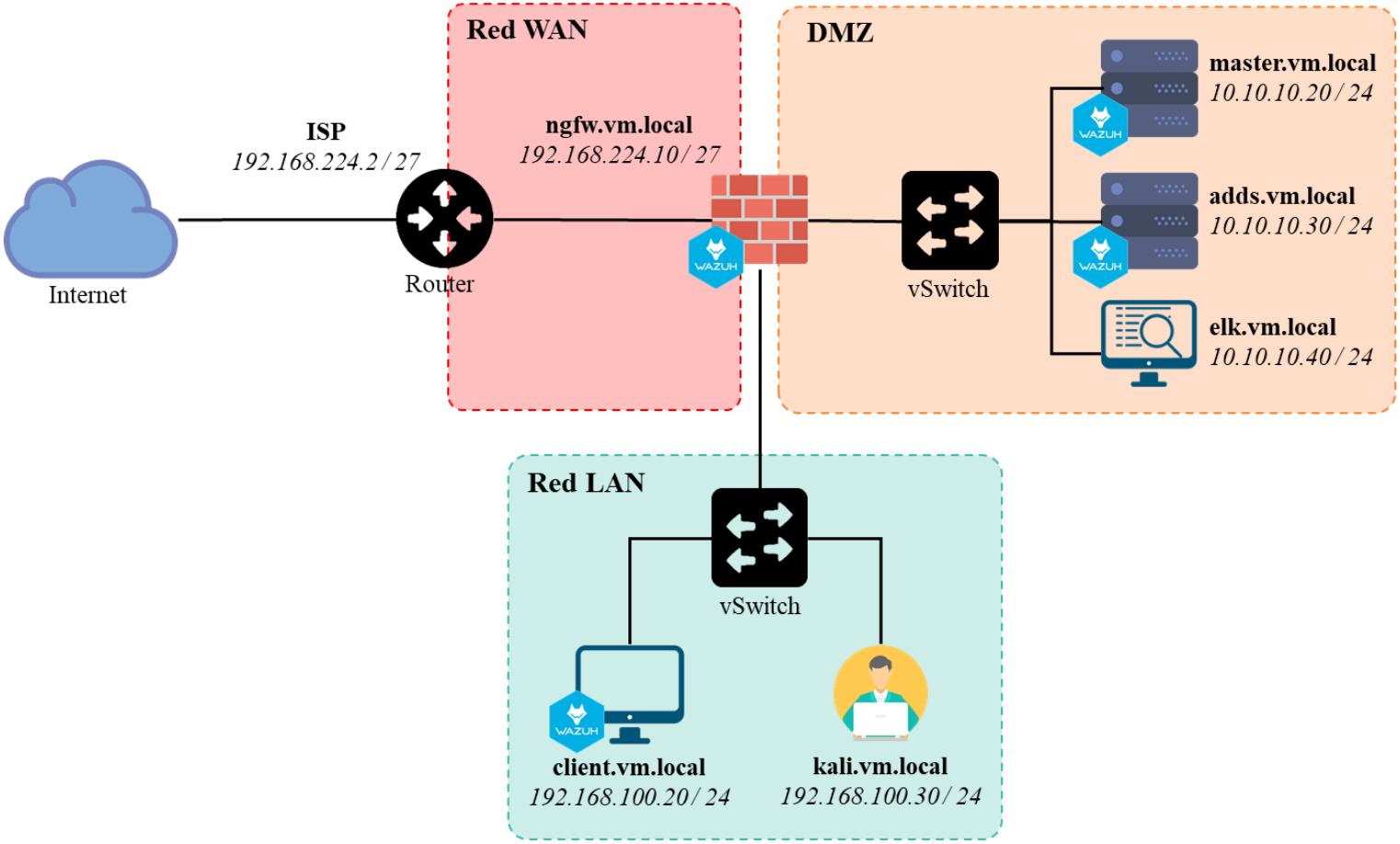


Figura 14. *Arquitectura de infraestructura tecnológica.*

Fuente: Elaboración del autor.

2.2.3. Arquitectura de software.

Es un conjunto de elementos que proporcionan un marco de referencia necesario para dirigir la construcción del aplicativo de software, que a su vez permite al equipo de Desarrolladores y Analistas de software compartir y colaborar en una misma línea de trabajo.

En la **Figura 15**, se describe el diseño a un alto nivel correspondiente a la estructura de solución para identificación de amenazas informáticas. Esta arquitectura de software se fundamenta en un conjunto de patrones y abstracciones coherentes que proporcionan un marco definido y claro para interactuar con los componentes de Elastic Stack, conforme a los lineamientos propuestos inicialmente en la arquitectura de procesos.

Elastic Stack es un conjunto de herramientas de gran potencial, con orientación de código abierto y que se combinan para crear una plataforma de administración de registros de eventos (Logs), permitiendo la monitorización, consolidación y análisis de datos generados en múltiples fuentes o activos de información de una organización. Las herramientas clave de Elastic Stack son ElasticSearch, Logstash y Kibana.

a. **Agentes Filebeats**, contempla la plataforma para los gestores de datos para el envío de datos desde los activos de información hacia procesos posteriores (Logstash y Elasticsearch).

b. **Wazuh**, comúnmente desplegado con Elastic Stack, permite la detección de intrusos basado en un host de código abierto (HIDS), proporcionando el análisis de registros, supervisión de integridad de archivos de sistema operativo, detección de rootkits y

vulnerabilidades, evaluación de configuraciones y capacidad de respuesta ante incidentes de seguridad de la información.

c. **Logstash**, es un canal de procesamiento de datos de código abierto en el lado del servidor de Big Data, que ingiere datos de una multitud de fuentes simultáneamente, los transforma y envía para su almacenamiento.

d. **Elasticsearch**, es un motor de búsqueda y análisis distribuido basado en RESTful y JSON, capaz de adaptarse a un número creciente de casos de uso. Considerado como el corazón del Elastic Stack, almacena los datos de forma centralizada y distribuida, permitiendo ejecutar búsquedas avanzadas.

e. **Kibana**, permite visualizar los datos de búsquedas ejecutadas en Elasticsearch y navegar por el Elastic Stack a nivel de Dashboards generados, permitiendo desde el seguimiento de la carga de consultas hasta la comprensión de solicitudes de trabajo que fluyen a través de las aplicaciones. El núcleo de Kibana consta de estructuras gráficas de nivel profesional, como histogramas, gráficos de líneas y barras, diagramas circulares, mapas de calor, tablas de contenido, entre otros.

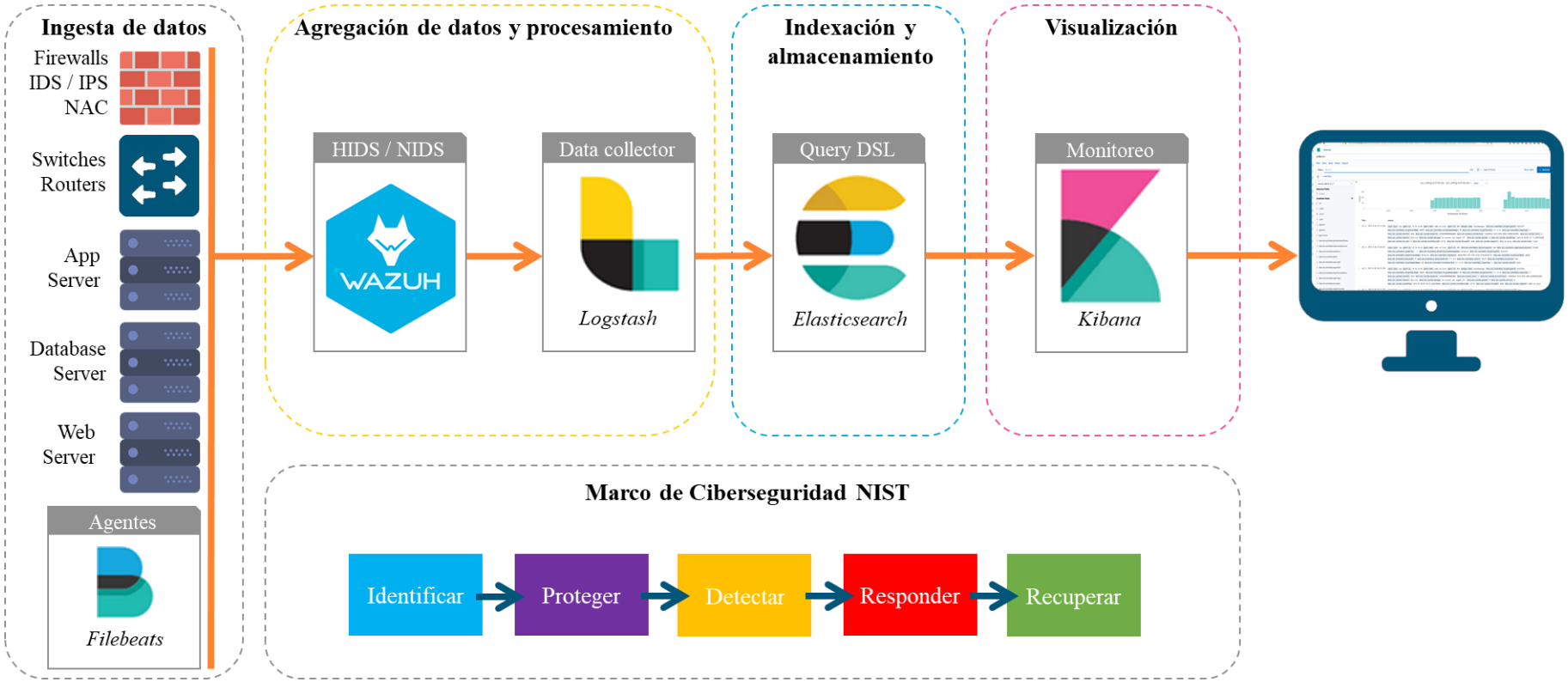


***Figura 15**. Arquitectura de software.*

Fuente: Elaboración del autor.

2.2.4. Arquitectura del negocio.

Consta del diseño de la operación del negocio, descrito en términos de capacidades empresariales y de tecnologías. Esta arquitectura a menudo puede ser de índole conceptual y determina cómo una organización debe acoplarse para empujar una estrategia establecida, en este caso orientado a la Seguridad de la información.

En la **Figura 16**, se plantea la arquitectura del negocio para el establecimiento de las estrategias de seguridad de la información (procesos, procedimientos e infraestructura tecnológica) que apoyen las actividades del negocio y que están alineadas con los objetivos de la organización, bajo el enfoque de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC).

La arquitectura planteada permitirá la identificación, aseguramiento, segregación, resistencia, correlación, monitoreo y respuesta ante de posibles ataques o amenazas informáticas, los cuales están enfocados en garantizar tanto la visibilidad como el control de los activos de información crítica de la organización, proporcionando un modelo para cambiar del modo reactivo tradicional de tratar los incidentes de seguridad de la información a un modo proactivo, apoyando y generando valor para la organización con el fin de dar cumplimiento a los objetivos organizacionales.

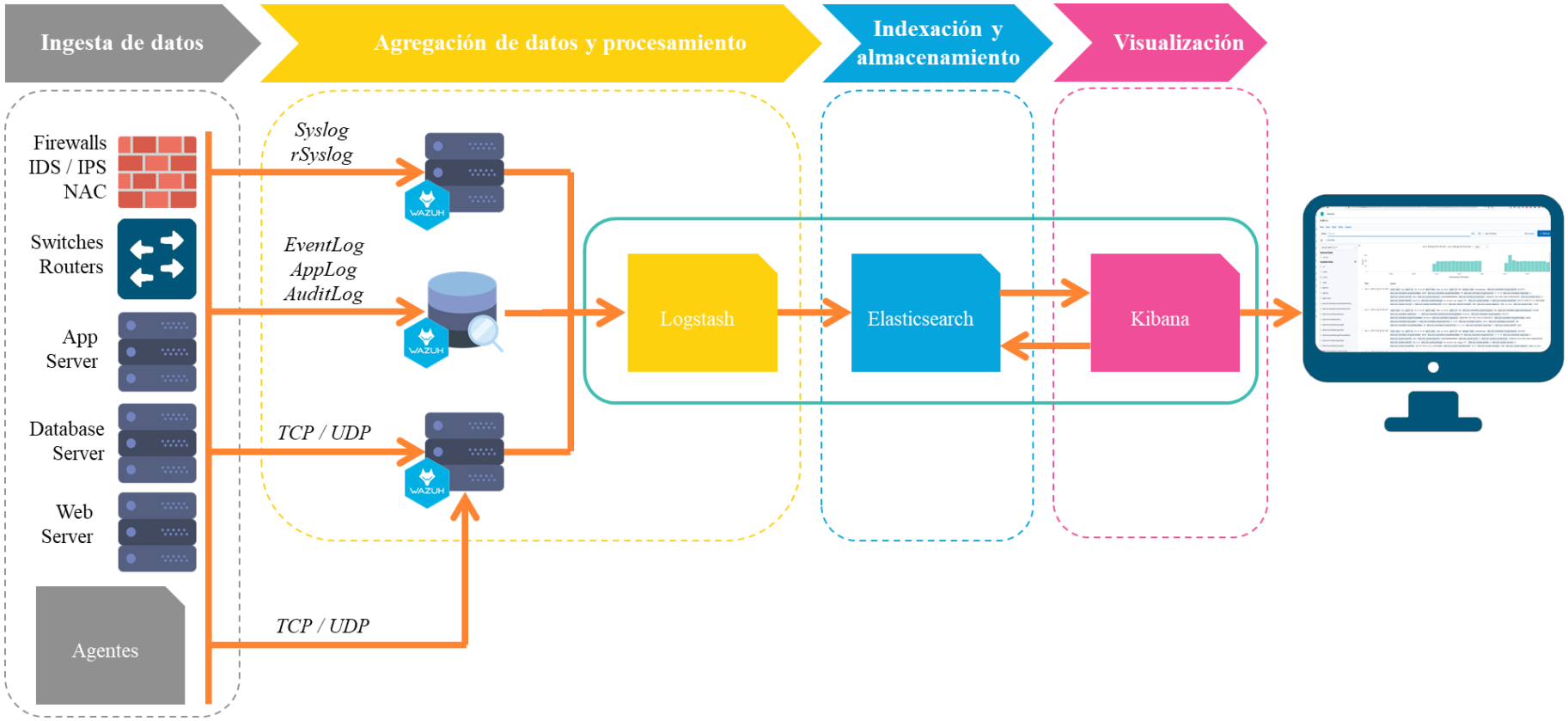


Figura 16. *Arquitectura del negocio.*

Fuente: Elaboración del autor.

Capítulo 3

Validación de resultados

Para efecto de la ejecución de las pruebas de validación se aplicarán Casos de Uso de ataques informáticos simulados bajo un ambiente de infraestructura tecnológica controlada, desplegada como parte del presente proyecto y expuesto en los **Anexos A** y **B**, los cuales se desarrollaron para la explotación de las vulnerabilidades informáticas más comunes.

El análisis y monitoreo de eventos constituye la etapa de consumo de la información obtenida mediante la gestión de los activos de información de la organización o fuentes generadoras de información en relación a eventos de seguridad (Logs). En los puntos subsiguientes, se presentan los Casos de Uso específicos que permiten evaluar la solución Elastic Stack como parte medular del diseño de una arquitectura para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data, alineándose con las siguientes estrategias planteadas:

1. Detección de la presencia o inminencia de errores en dispositivos de comunicaciones de datos y seguridad de red, sistemas operativos y aplicaciones.

2. Detección de accesos e intentos de acceso no autorizados de administración a los activos de la información o infraestructura tecnológica de la organización.

3. Detección de accesos e intentos de acceso no autorizados a los equipos de comunicaciones de red de datos.

4. Detección de accesos e intentos de acceso no autorizados a las sesiones de red Microsoft Windows, por parte de los usuarios corporativos.

5. Detección de accesos e intentos de acceso no autorizados a los servicios de Intranet de la organización.

6. Identificación de posibles amenazas informáticas sobre los activos de la información o infraestructura tecnológica de la organización.

7. Visualización de la distribución del consumo de la conexión de Internet por parte de los usuarios corporativos.

8. Visualización de eventos de carácter malicioso o que involucre compromiso a nivel operativo en los activos de la información monitoreados dentro de la organización.

Bajo el entorno desplegado, se implementó la infraestructura tecnológica de acuerdo con la **Tabla 2**, que permite la ejecución de los distintos Casos de Uso propuestos además de la integración de componentes tecnológicos empleados como parte de la solución y que no son específicamente parte del ecosistema de Big Data, sino que interactúan o influyen en la implementación y en la configuración de estos.

3.1. Hardware.

Como se describe en la **Figura 17** y **Tabla 1**, el proyecto fue implementado con tecnología de la familia de procesadores escalables Intel®'s Core i7® y Chipset de Intel®, ofrece potencia de computación optimizada y capacidad de virtualización en un factor de forma compacto de 1U con un socket para CPU, 2 slots para módulos de red (NIC) y memoria de sistema DDR4 de hasta 48GB, y tiene un costo estimado de USD$ 960,00.

Appliance para procesamiento de datos.



***Figura 17**. Plataforma de procesamiento empresarial Mid – Range x86.*

***Tabla 1**. Componentes de hardware.*

Plataforma	
Procesador	Familia de procesadores Intel® Core i7®.
Chipset	Intel®.
Memoria RAM	Cuatro DIMM DDR4 2666 MHz de 8 GB.
Almacenamiento	
Disco duro	Una bahía interna de 2,5 pulgadas.
Capacidad	1 TB SSD.
Interfaces E/S	
Puertos LAN	2 puertos Gigathernet RJ45.
Salida de video	VGA.

USB 3.0	4 puertos Tipo A.
Alimentación eléctrica	
Entrada de energía	Entrada de alimentación de CA en la fuente de poder.
Tipo / Watt	Fuente de poder ATX de 850 Watts.
Características físicas y ambientales	
Temperatura	0°C a 40°C
Humedad	5% a 95% (sin condensación).
Dimensiones	610 mm. x 44 mm. x 438 mm.
Peso	18 kg. (39,6 lb.).

3.2. Software.

3.2.1. VMware vSphere 6.7 de 64 bits.

Es una plataforma de virtualización a nivel de centro de datos producido por VMware, Inc. Es el componente de su producto VMware Infraestructure que se encuentra al nivel inferior de la capa de virtualización, el hipervisor posee herramientas y servicios de gestión autónomos e independientes, como se observa en la **Figura 18**.

Está compuesto de un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software hipervisor, los servicios y servidores que permiten la interacción con el software de gestión y administración de las máquinas virtuales (VMware Inc., 2019).

Plataforma de virtualización.

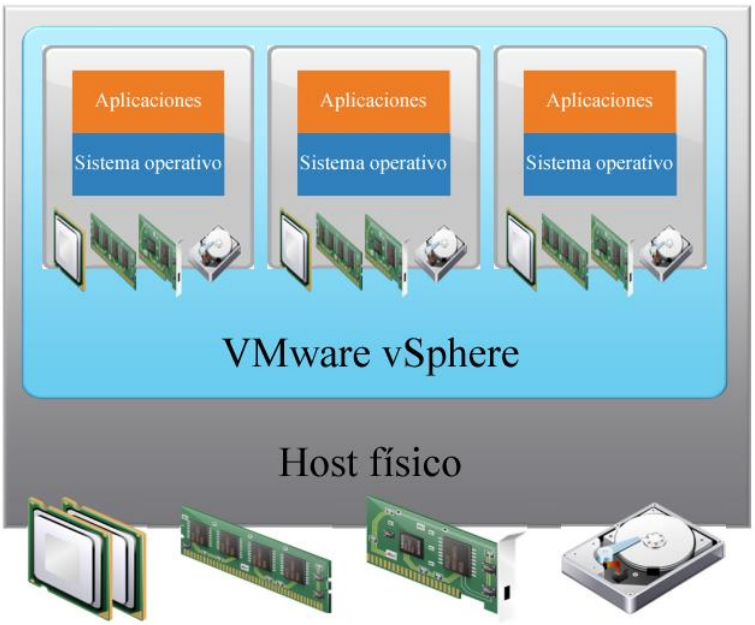


***Figura 18**. Arquitectura VMware vSphere.*

Fuente: VMware Inc., 2019

3.2.2. Sistemas operativos implementados.

La plataforma para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data, será implementada sobre las siguientes plataformas de software:

1. Microsoft Windows 2012 R2 de 64 bits.
2. Microsoft Windows 7 de 32 bits.
3. GNU / Linux CentOS 7.6.1810.
4. GNU / Linux FreeBSD IPFire 2.23 - Core Update 134.
5. GNU / Linux Kali Linux 2019.2.04 de 64 bits.

3.3. Consolidado de infraestructura virtual.

Conforme a la información recabada en la **Tabla 2**, como parte de las arquitecturas planteadas para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data, adjunto se describe la distribución consolidada de la infraestructura virtual desplegada. El detalle técnico del consolidado de infraestructura virtual se especifica en el **Anexo A** y **B**.

***Tabla 2**. Consolidado de infraestructura virtual implementada.*

Host	Máquinas virtuales	Nombre del servidor	Descripción
Host 1	VM1	ngfw.vm.local	Next–gen firewall, DNS, DHCP, filtro de URL, filtro de contenido, IDS/IPS.
	VM2	master.vm.local	DNS, servidor Web, servidor DB, servidor FTP, servidor NTP.
	VM3	adds.vm.local	Servidor de autenticación (ADDS), servidor DB, servidor DLP.
	VM4	elk.vm.local	Elasticsearch, Logstash, Kibana, Wazuh Manager.
	VM5	client.vm.local	Cliente de dominio.
	VM6	kali.vm.local	Monitor de explotación de vulnerabilidades.

3.3.1. Componentes de Elastic Stack.

Elastic Stack es un motor de búsqueda y analítica de tipo Open source basado en Apache Lucene, considerado como un motor de búsqueda de texto completo, distribuido y con capacidad de multi-tenencia con una interfaz web RESTful y con documentos JSON, diseñado para permitir una escalabilidad horizontal, fiabilidad y de fácil gestión.

En el entorno de la inteligencia operacional, es necesario gestionar e incrementar servicios claves que permitan a la organización disponer de la capacidad de análisis dinámico de negocios, en tiempo real, ya que esto aporta a una mayor visibilidad y compresión del sentido de las operaciones del negocio.

Los componentes claves de Elastic Stack en su versión 7.3.0 (Elastic Stack, 2019), liberados el 31 de julio de 2019, a saber:

1. GNU / Linux CentOS 7.6.1810
2. Elasticsearch 7.3.0 (Elasticsearch, 2019)
3. Logstash 7.3.0 (Logstash, 2019)
4. Filebeat 7.3.0 (Filebeat, 2019)
5. Kibana 7.3.0 (Kibana, 2019)
6. Wazuh Manager 3.9.5 (Wazuh Security Detection, 2019)
7. Wazuh API 3.9.5
8. Wazuh App 3.9.5 – 7.3.0

3.4. Construcción del entorno de identificación de amenazas.

La interfaz gráfica de usuario a nivel de eventos de seguridad (Logs), como se observa en la **Figura 19**, proporcionando seguimiento de registros en tiempo real en una pantalla unificada y personalizable; los datos de registros se correlacionan con las métricas de la interfaz de usuario de infraestructura, lo que facilita el diagnóstico de los posibles incidentes. Los registros de eventos se pueden transmitir en tiempo real o cargar de forma manualmente, siendo visualizados de arriba hacia abajo, lo que facilita su exploración en tiempo real y la visualización de una vista histórica de los registros de eventos de seguridad.

Interfaz gráfica de Elastic Stack.

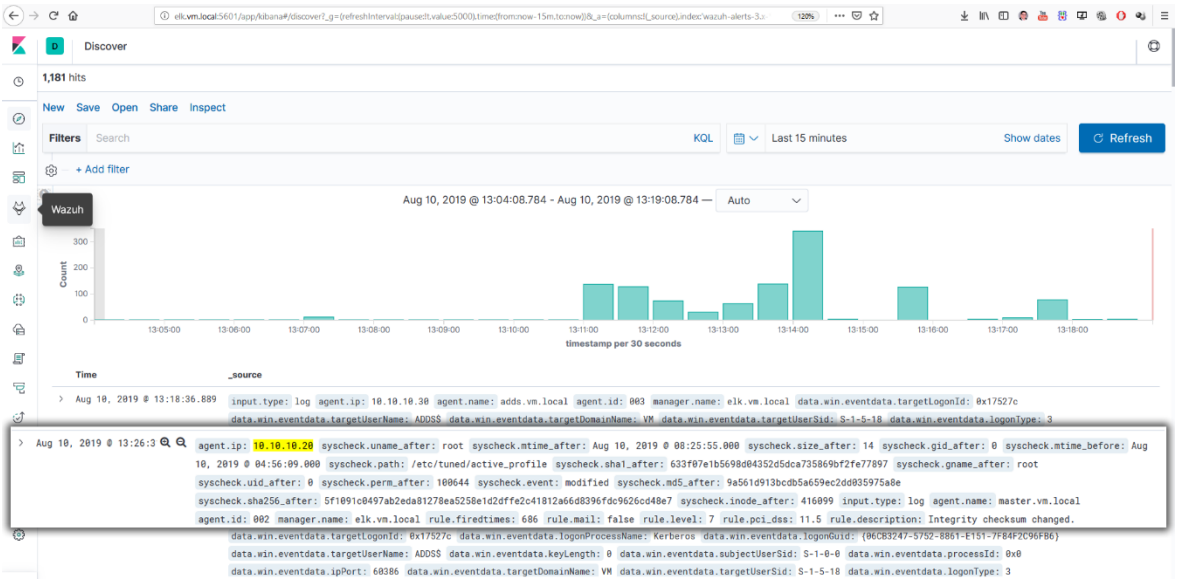


***Figura 19**. Interfaz gráfica, Gestión de eventos de seguridad (Logs).*

3.4.1. Interfaz gráfica de Wazuh Server.

Wazuh Server es un proyecto de código abierto que proporciona visibilidad de seguridad, cumplimiento y capacidad de supervisión a la infraestructura de misión crítica de una organización. El proyecto Wazuh nació como una alternativa de OSSEC HIDS (Host Intrusion Detection System, Sistemas de Detección de Intrusos basado en Host) y ha evolucionado hasta convertirse en una solución integral mediante la implementación de nuevas funcionalidades y la integración de herramientas adicionales como OpenSCAP y Elasticsearch, de acuerdo con la **Figura 20**, **Figura 21** y **Figura 22**.

Interfaz gráfica de Wazuh Server.

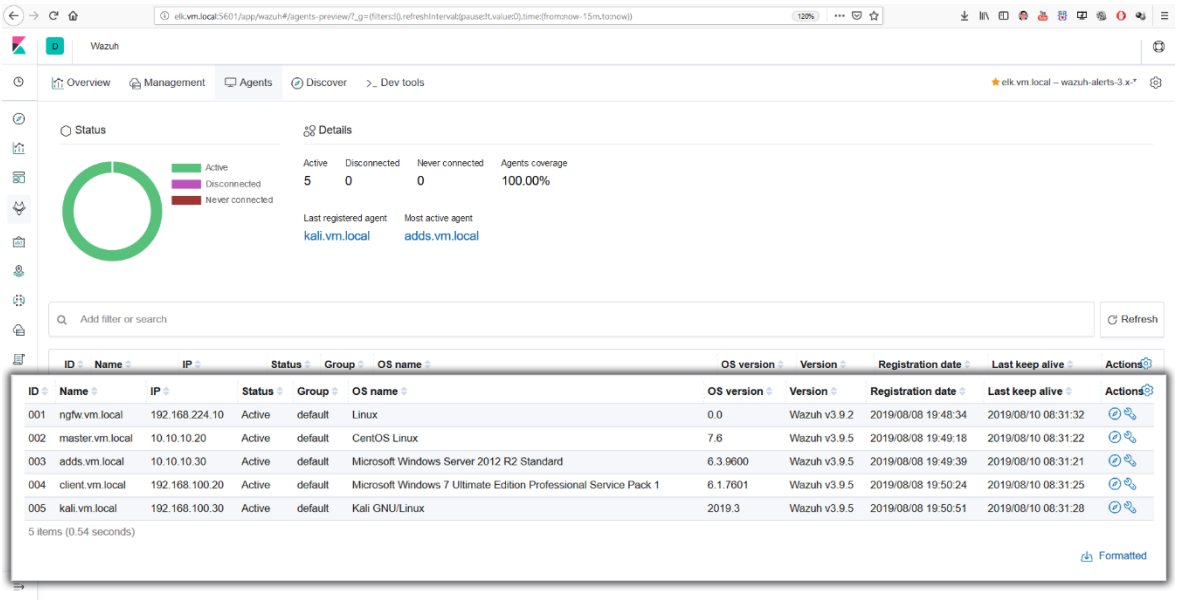


***Figura 20**. Interfaz gráfica, Gestión de Agentes desplegados.*

Interfaz gráfica para identificación de amenazas.

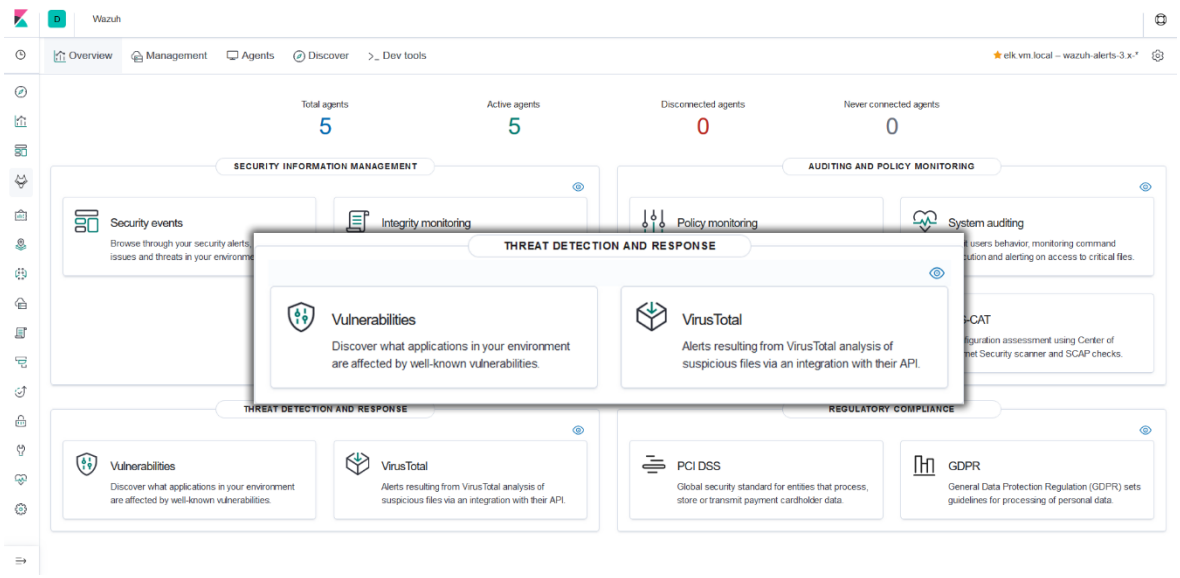


Figura 21. *Interfaz gráfica, Perspectiva general para identificación de amenazas.*

Interfaz gráfica para identificación de amenazas.

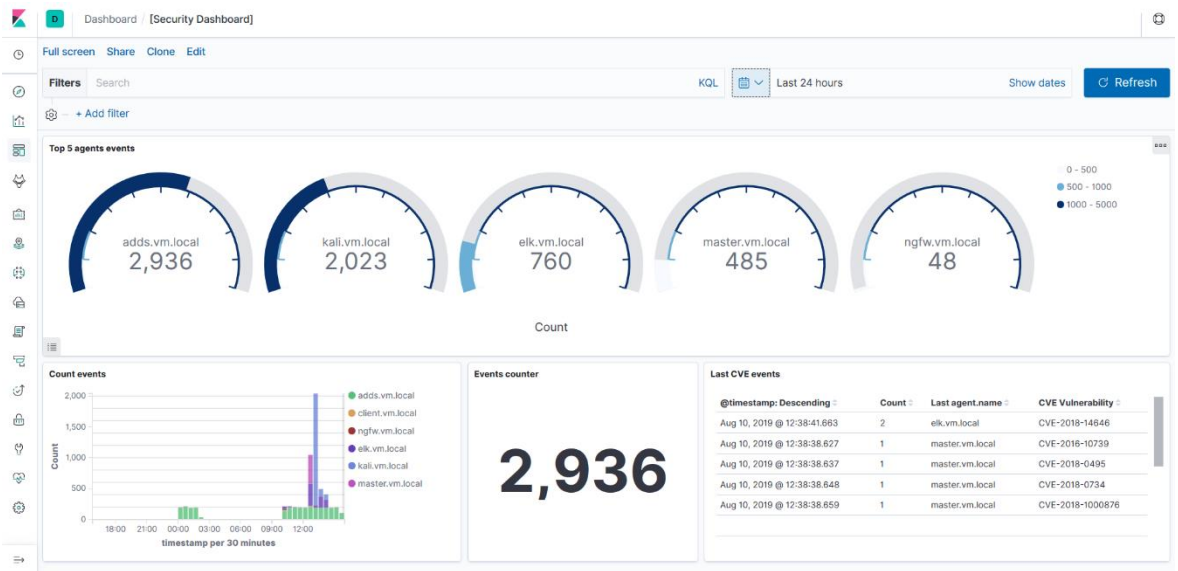


Figura 22. *Interfaz gráfica, Dashboard de seguridad.*

3.4.2. Integración API con fuentes de información externa.

Wazuh Server junto con Elastic Stack pueden en conjunto escanear archivos de sistema operativo y de datos, en busca de contenido malicioso insertado en ellos, a través de su motor de análisis de integridad de archivos (FIM) o en inglés File Integrity Management, como se observa en la **Figura 23**.

Integración API con plataformas de seguridad.

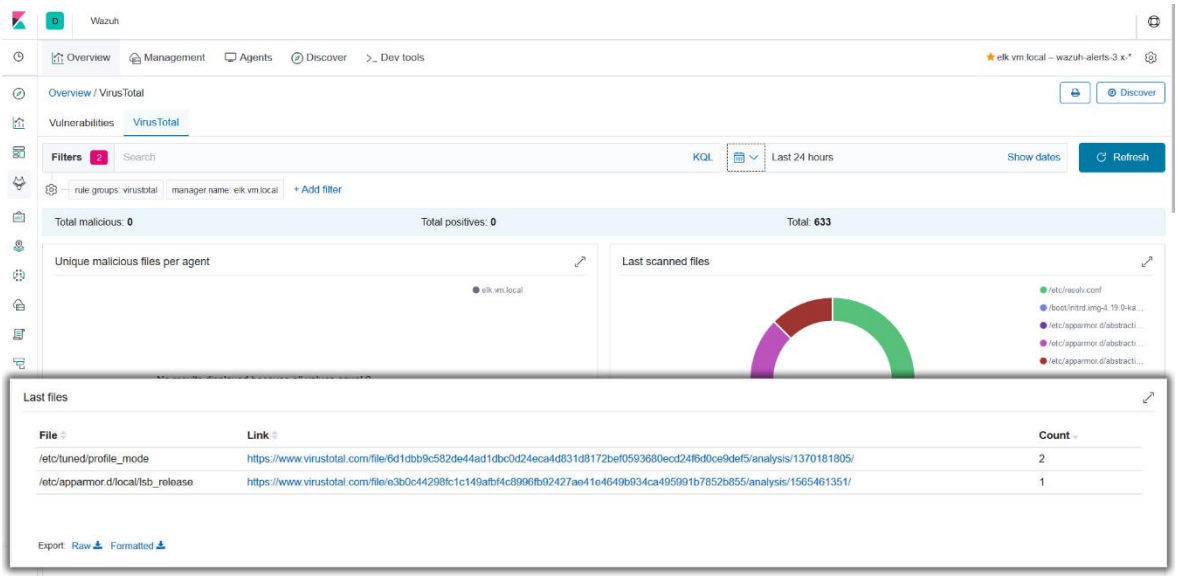


***Figura 23**. Integración API con VirusTotal.*

Esto es posible a través de una integración con VirusTotal, que es una potente plataforma que agrega múltiples productos antivirus junto con un motor de escaneo en línea; la combinación de esta herramienta con el motor FIM proporciona un medio sencillo de escanear los archivos que se supervisan para inspeccionarlos en busca de contenido malicioso, como se describe en la **Figura 24** y **Figura 25**.

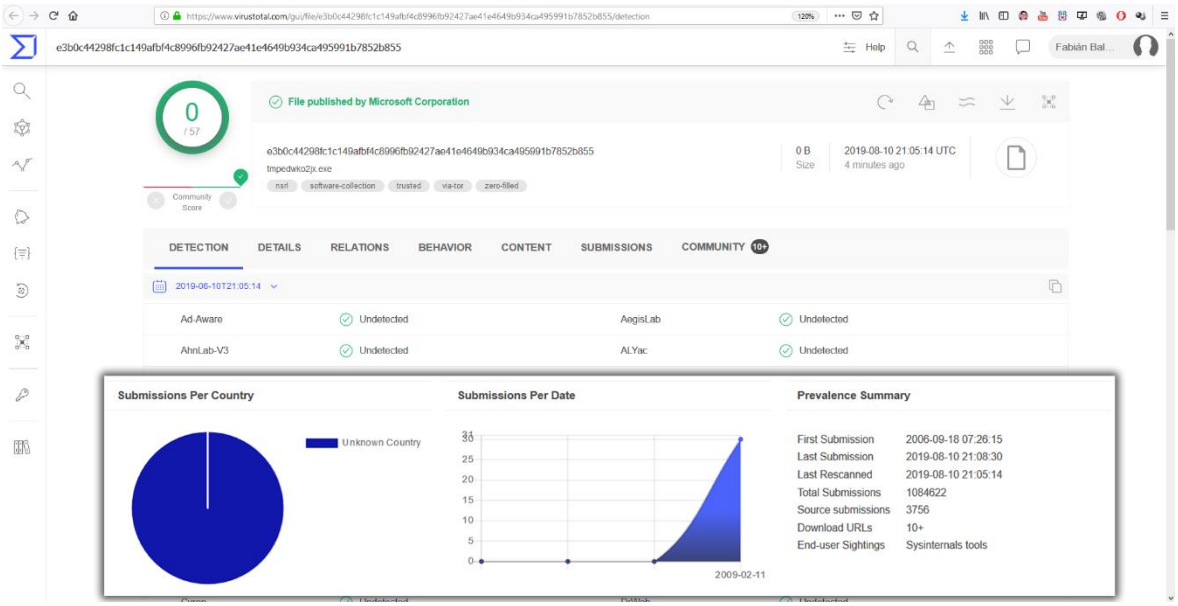


***Figura 24**. Análisis de inteligencia con VirusTotal.*

Integración API con plataformas de seguridad.

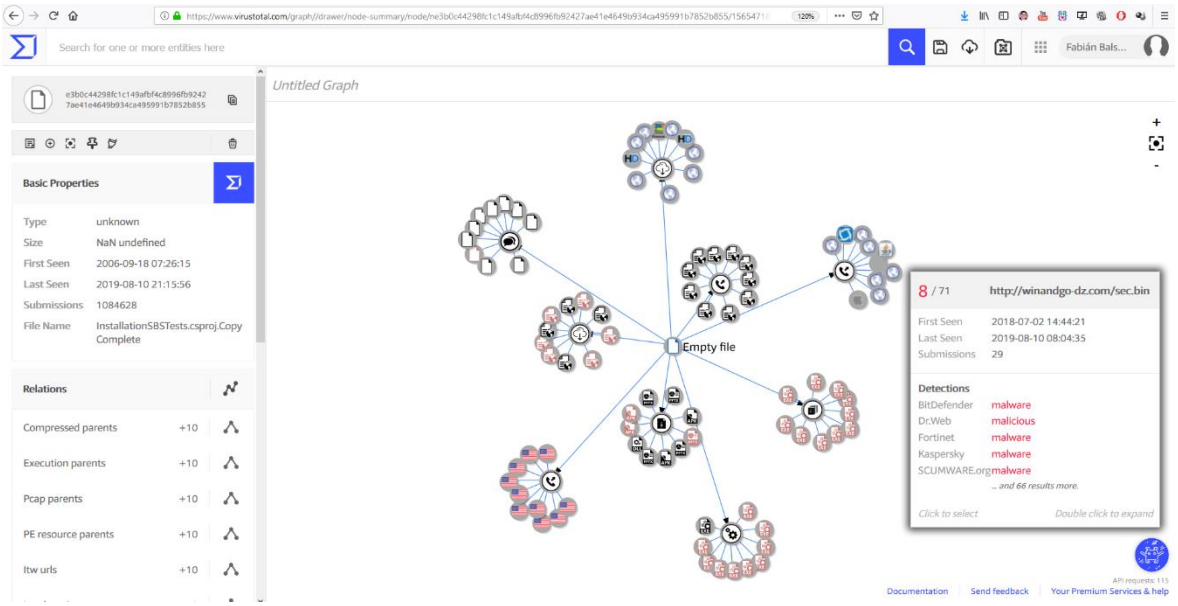


***Figura 25**. Análisis de inteligencia con VirusTotal Graph, Modelo de red.*

3.5. Caso de Uso para validación de resultados.

3.5.1. Caso de Uso No. 01.

El usuario promedio emplea al menos 5 contraseñas diferentes que va intercambiando entre las distintas aplicaciones corporativas, dispositivos electrónicos (terminal o laptop de usuario final, Tablet o dispositivo móvil) y cuentas transaccionales, como se describe en la **Tabla 3**.

***Tabla 3**. Caso de Uso No. 01.*

CUSEG No. 01	**Violación de políticas de acceso y uso de credenciales de acceso.**
Descripción	Controlar el acceso autorizado a los sistemas y aplicaciones de la organización desde una o varias ubicaciones geográficas.
Objetivo	Detectar incumplimiento de políticas de control de acceso de usuarios.
Condiciones de alerta	a. Alertar sobre múltiples autenticaciones simultáneas de un mismo usuario. b. Inicio de sesión desde ubicaciones geográficas no autorizadas. c. Alertar sobre intentos fallidos de autenticación o conexión.
Fuentes de datos	Logs del sistema de autenticación de usuarios (ADDS). Next–gen Firewall. Sistema de detección de intrusos (IPS / HIDS). Proxy Server.

En la **Figura 26**, se visualizan los agentes desplegados en la infraestructura tecnológica implementada durante la investigación, identificando que el servidor ngfw.vm.local (192.168.224.10) presenta alertas de seguridad por utilización recurrente de credenciales de acceso a los servicios corporativos. Además, la **Figura 27** presenta un resumen descriptivo de las alertas de seguridad presentadas a la fecha.

Top 5 de los agentes en base a la evolución de alertas.

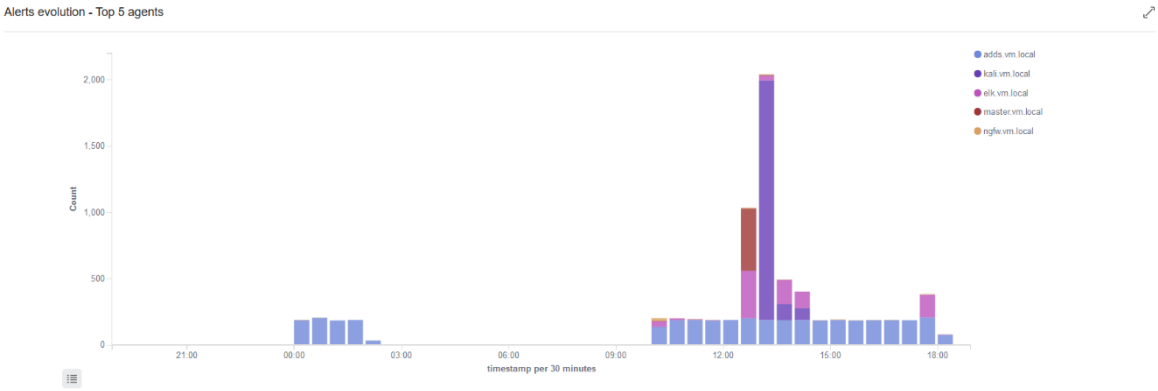


***Figura 26**. Visualización de evolución de alertas, Top 5 de agentes.*

Resumen de alertas de seguridad.

Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	1,927
60137	Windows User Logoff	3	1,913
550	Integrity checksum changed.	7	741
2904	Dpkg (Debian Package) half configured.	7	711
87101	VirusTotal: Error: Public API request rate limit reached	3	371
2902	New dpkg (Debian Package) installed.	7	359
87103	VirusTotal: Alert - No records in VirusTotal database	3	227
533	Listened ports status (netstat) changed (new port opened or closed).	7	45
23505	kernel: lack of check for mmap minimum address in expand_downwards in mm/mmap.c leads to NULL pointer dereferences exploit on non-SMAP platforms	10	19
23505	kernel: insufficient input validation in kernel mode driver in Intel i915 graphics leads to privilege escalation	10	19

Export: Raw Formatted

***Figura 27**. Lista resumen de alertas de seguridad.*

3.5.2. Caso de Uso No. 02.

En el campo de la seguridad de la información, la infraestructura de centro de comando y control (Command and control, usualmente abreviado C&C o C2), consta de servidores de procesamiento y otros elementos que son usados para controlar los malware y botnet, como se describe en la **Tabla 4**.

***Tabla 4**. Caso de Uso No. 02.*

CUSEG No. 02	**Detección eventos salida Internet (Comando de centro y control).**
Descripción	Cuando un equipo interno (terminal de usuario) de la organización genere un alto número de peticiones hacia Internet, este indicará en el equipo de seguridad perimetral y de prevención de intrusos (IPS) que es posible que una máquina este contaminada con malware o esté enviando ataques hacia fuentes externas.
Objetivo	Detectar incumplimiento de políticas de control de acceso de usuarios.
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea: a. Múltiples conexiones hacia redes externas. b. Detección de firma que involucre la misma dirección IP destino.
Fuentes de datos	Next–gen Firewall. Sistema de detección de intrusos (IPS / HIDS).

Los Analistas y Expertos de seguridad de la organización necesitan encontrar una manera eficiente de detectar y controlar aspectos relevantes a las conexiones desde y hacia Internet para mantener un entorno en seguro y accesible. Como se observa en la **Figura 28**, una de las formas de obtener el control por parte de los atacantes es a través del protocolo DNS, siendo las brechas de seguridad de Windows el principal medio de utilización para este tipo de ataque o amenaza informática. Aplicando las contramedidas y contención través de estos servicios se puede interrumpir la transmisión de paquetes de un malware hacia el punto de conexión o servidor de comando y control (C&C).

Visualizador de eventos de seguridad.

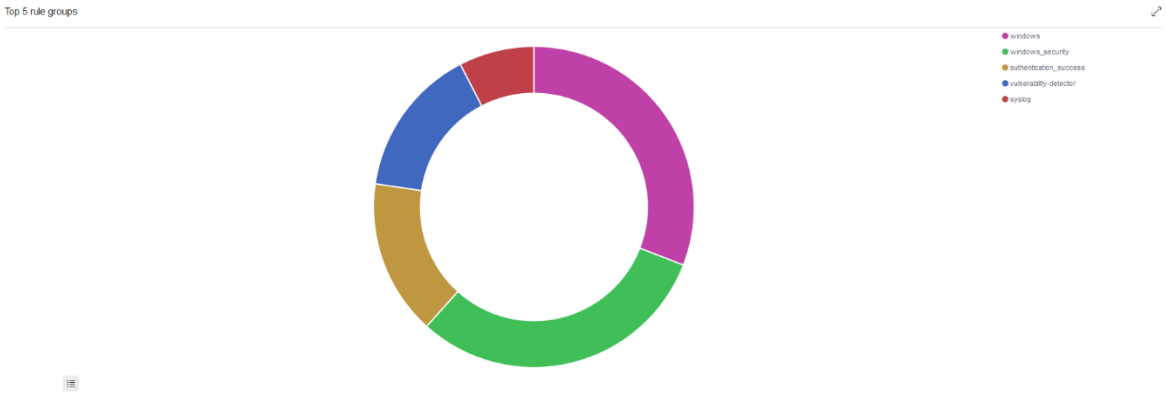


***Figura 28**. Visualización de grupos por reglas de seguridad.*

3.5.3. Caso de Uso No. 03.

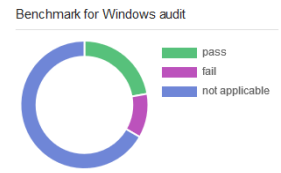
Además de los ataques de código malicioso (virus, troyanos, spyware, malware, entre otros), es posible que los activos de información de una organización sean objetivo de diversos ataques de red de datos, uno de los más comunes es el de reconocimiento, detección y esquematización no autorizadas de sistemas, servicios o vulnerabilidades, como se describe en la **Tabla 5**.

***Tabla 5**. Caso de Uso No. 03.*

CUSEG No. 03	**Detección reconocimiento objetivos.**
Descripción	Reconocimiento de servicios críticos.
Objetivo	Detectar un posible ataque interno de reconocimiento de puertos a los servidores principales de la red de datos organizacional.
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea: a. Detecta conexiones fallidas y satisfactorias hacia los diferentes servidores corporativos. b. Se detectan firmas relacionadas con reconocimiento hacia la granja de servidores con destino de direcciones críticas para la organización.
Fuentes de datos	Logs del sistema de autenticación de usuarios (ADDS). Next–gen Firewall. Sistema de detección de intrusos (IPS / HIDS). Topología de la infraestructura de red de datos corporativa.

El escaneo de activos intenta encontrar potenciales incidentes de seguridad usando ataques conocidos contra objetivos seleccionados. Como se observa en la **Figura 29**, se verifica el escaneo de activos de información sobre los objetivos identificados, que para la investigación corresponde a la infraestructura tecnológica desplegada. Cabe notar que el escaneo de activos solo puede encontrar ciertos tipos de incidentes de seguridad y vulnerabilidades lógicas, tales como un control de acceso defectuoso. Además de un escaneo de activos, se verifica la ejecución de una prueba de penetración automática para encontrar incidentes de seguridad relacionados con los cumplimientos normativos de los activos de información de la organización.

Prueba de rendimiento para equipos Microsoft Windows.



Policy	Description	Last scan	Pass	Fail	Not applicable	Score
Benchmark for Windows audit	This document provides a way of ensuring the security of the Windows systems.	2019/08/10 12:46:04	2	1	6	66%

***Figura 29**. Análisis de auditoria de sistemas operativos Microsoft.*

3.5.4. Caso de Uso No. 04.

Un ataque dirigido es un proceso a largo plazo que pueden comprometer la seguridad y dar acceso no autorizado a los criminales cibernéticos; algunos de estos ataques utilizan amenazas persistentes (APT) o pueden usar técnicas como malware avanzado o exploits de día cero (Zero – day), como se describe en la **Tabla 6**.

***Tabla 6**. Caso de Uso No. 04.*

CUSEG No. 04	**Detección de ataques específicos o ataques dirigidos.**
Descripción	Alto número de conexiones hacia un servicio especifico
Objetivo	Identificar ataques internos realizados hacia los servidores principales de la organización.
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea: a. Detecta conexiones satisfactorias hacia los servidores críticos de la organización. b. Se detecta una firma de un servicio Web, consola remota SSH, E-mail, base de datos, etc., con destinos de direcciones críticas para la organización.
Fuentes de datos	Next–gen Firewall. Sistema de detección de intrusos (IPS / HIDS). Topología de la infraestructura de red de datos corporativa.

Para la ejecución de ataques dirigidos se propone la utilización de la herramienta UFOnet junto con GNU / Linux Kali, como se observa en la **Figura 30** y **Figura 31**. UFONet es una

herramienta de código abierto con licencia GPLv3, escrita por Lord Epsylon (psy) en python, html5 y javascript, para realizar ataques de denegación distribuídos (DDoS) aprovechando fallos de redirecciones abiertas (Open redirect) en aplicaciones web a modo de botnet.

Explotaciones de vulnerabilidades con Kali Linux.

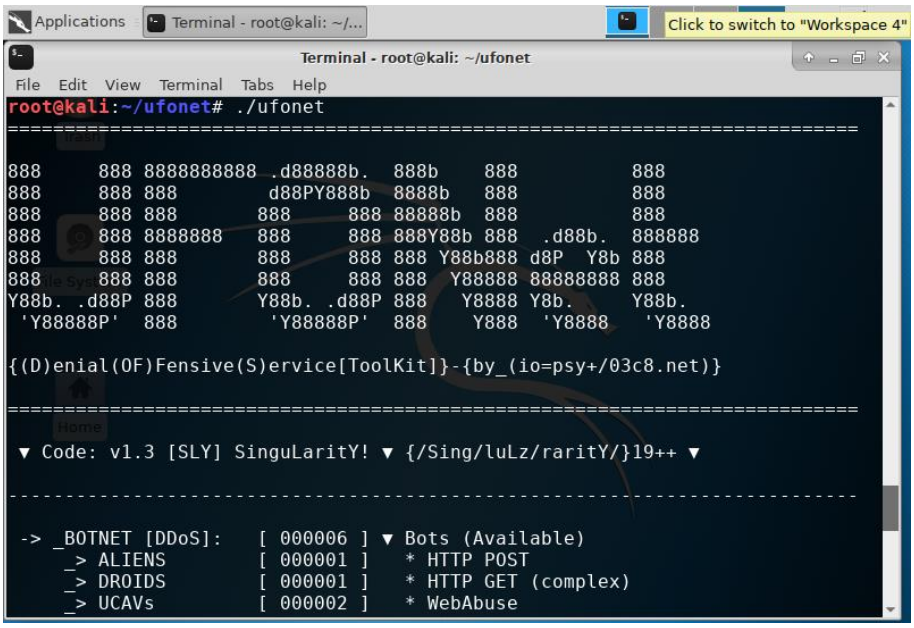


***Figura 30**. Ejecución de un ataque dirigido con UFONet.*

Identificación de credenciales de acceso.

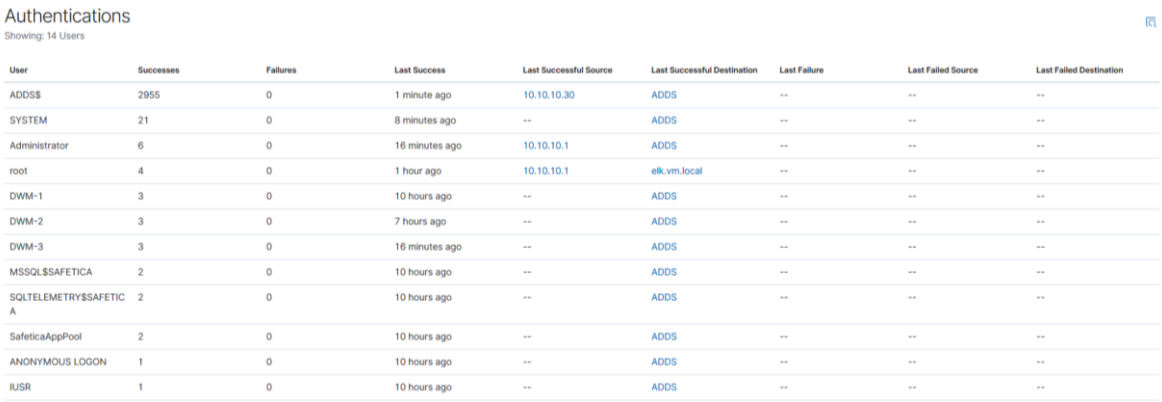


***Figura 31**. Análisis de usuario y credenciales de acceso en activos de información.*

3.5.5. Caso de Uso No. 05.

Los ataques de denegación de servicio (DoS) son la forma más común de ataque a nivel de comunicaciones de datos, así también pueden usar diversos protocolos de comunicaciones a fin de no ser identificados, en este caso se denominan ataques de denegación dinámica de servicio (DDoS), como se describe en la **Tabla 7**.

Tabla 7*. Caso de Uso No. 05.*

CUSEG No. 05	**Denegación dinámica de servicio (DDoS).**
Descripción	Denegación de servicios hacia servidores internos de la organización.
Objetivo	Detectar ataques que puedan llegar a afectar la disponibilidad del servicio.
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea: a. Detecta un alto número de conexiones permitidas hacia redes de datos internas. b. Detecta firmas relacionadas con ataques de denegación de servicios dinámica (DDoS) con destino de direcciones críticas para la organización.
Fuentes de datos	Next–gen Firewall. Sistema de detección de intrusos (IPS / HIDS).

Una ampliación del ataque de denegación de servicio distribuido, también llamado DDoS (por sus siglas en inglés, Distributed Denial of Service) el cual se lleva a cabo generando un

gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino o activo de información. Como se observa en la **Figura 32** y **Figura 33**, se aplica la técnica denominada Ping de la muerte, con repercusión en el estado operativo del activo de información objetivo del ataque informático.

Explotaciones de vulnerabilidades con Kali Linux.

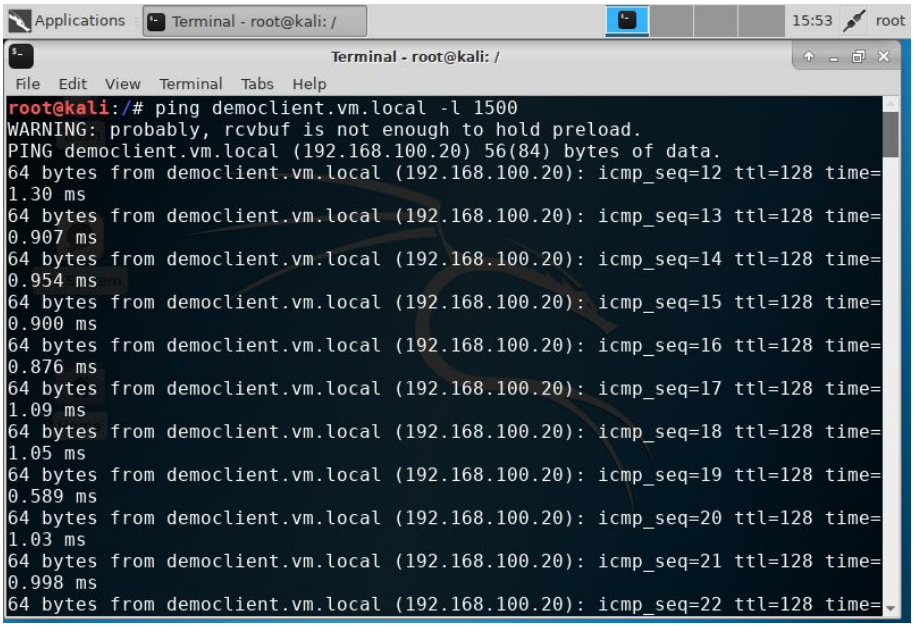


***Figura 32**. Explotaciones de vulnerabilidades con Kali Linux.*

Ataque dirigido por denegación de servicio dinámico DDoS.

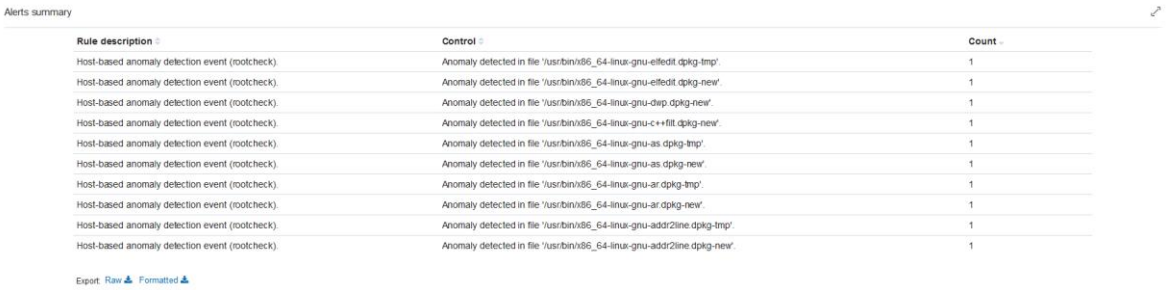


***Figura 33**. Ataque dirigido por denegación de servicio dinámico DDoS.*

3.5.6. Caso de Uso No. 06.

Las amenazas que se originan de afuera de la red de datos corporativa, al no tener información certera de la topología de la red interna de la organización, permiten que el criminal cibernético debe realizar varias acciones para conocer la estructura y encontrar la manera de atacar los activos de información, como se describe en la **Tabla 8**.

***Tabla 8**. Caso de Uso No. 06.*

CUSEG No. 06	**Detección de amenazas externas sobre infraestructura crítica.**
Descripción	Detectar actividades anómalas provenientes de fuentes externas que puedan afectar la disponibilidad de las aplicaciones críticas de la organización.
Objetivo	Identificar ataques que puedan afectar la disponibilidad de las aplicaciones críticas.
Condiciones de alerta	a. Flujos de tráfico desde una misma dirección IP, desde o hacia uno o varios puertos de servicios. b. Alto número de peticiones originadas desde una misma dirección IP origen, hacia un puerto de servicio específico, como por ejemplo 80 (HTTP) o 443 (HTTPS).
Fuentes de datos	Next–gen Firewall. Sistema de detección de intrusos (IPS / HIDS). Topología de la infraestructura de red de datos corporativa.

Un inventario de activos se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, entre otros) que contengan valor

para la organización y necesiten por tanto ser protegidos de potenciales amenazas informáticas. Como se observa en la **Figura 34** y **Figura 35**, se aplican técnicas de enumeración de activos de información, para que permite la identificación de los activos de información expuestos sobre la infraestructura tecnológica empleada en la investigación.

Ataque de enumeración de activos de información.

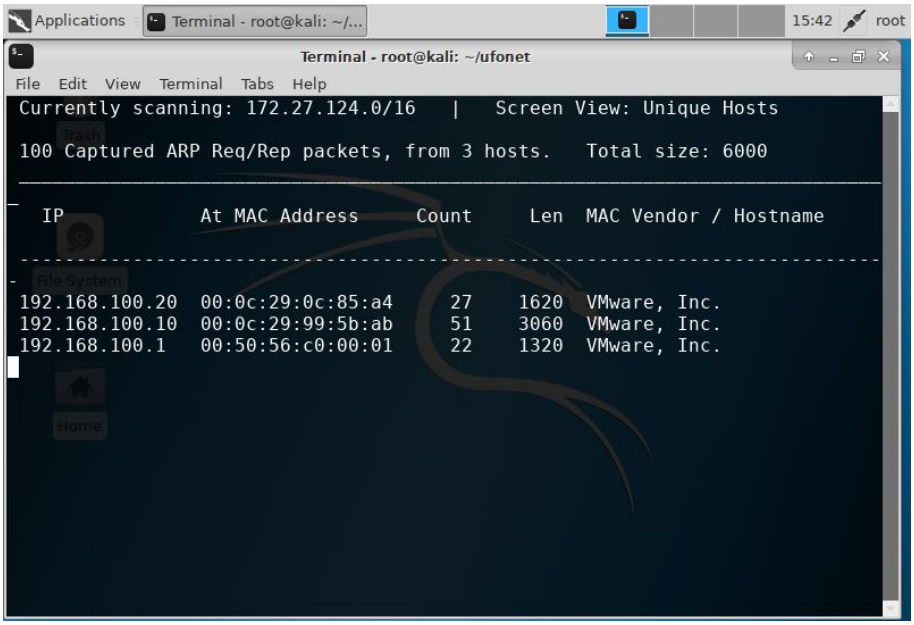


***Figura 34**. Ataque de enumeración de activos de información.*

Identificación de activos de información y cuentas de usuarios.

Top 5 users

Agent ID	Agent name	Top user	Count
005	kali.vm.local	root	691
001	ngfw.vm.local	root	10
000	elk.vm.local	root	6

Export: Raw Formatted

***Figura 35**. Identificación de activos de información y cuentas de usuarios.*

3.6. Impacto derivado del proyecto.

El monitoreo de eventos o incidentes de seguridad para asegurar el cumplimiento tanto de normativa interna como externa en materia de seguridad de la información es un servicio que puede ser asignado a un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) aplicando herramientas del ecosistema de Big Data, contribuyendo tanto a la disminución del riesgo inminente como también a la prevención de los activos de información de la organización, y por el ende el impacto financiero y de reputación que podría conllevar.

El personal de Expertos y Analistas de seguridad de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), puede colaborar en pro de la concientización para la educación en materia de seguridad de la información de los usuarios de la organización; estas actividades son en extremo útiles para capacitar a los usuarios sobre la detección de potenciales incidentes de seguridad informática, cómo reportarlos y cómo reaccionar ante una situación de riesgo.

Conforme a lo mencionado, la investigación forense que utiliza herramientas del ecosistema de Big Data se constituye como un servicio otorgado por el Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), actuando como referente técnico ante eventuales temas de índole legal, por lo tanto el personal del Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) debe estar capacitado para actuar en todos los casos, utilizando tecnología avanzada de análisis de datos, dedicada y preservando al mismo tiempo la cadena de custodia de la información.

Capítulo 4

Conclusiones y Recomendaciones

4.1. Conclusiones.

1. La tecnología continuará evolucionando, las organizaciones seguirán siendo cada vez más dependientes de las Tecnologías de la Información y Comunicaciones (TIC), y por ende las amenazas relacionadas a la tecnología se mantendrán e inclusive podrán aumentar debido a configuraciones técnicas deficientes, inadecuada gestión o falta de capacidades y competencias técnicas de los proveedores de las tecnologías.

2. El análisis de grandes cantidades de datos en el área de la Seguridad de la información es considerado como un área de trabajo reciente y requiere de una amplia investigación, así como establecer un nuevo modelo conceptual o arquitectura tecnológica que ofrezca una alta capacidad de almacenamiento, flexibilidad técnica y con una inversión de capital menos costosa para hacer frente a las amenazas informáticas con el apoyo del análisis de datos con herramientas del ecosistema de Big Data.

3. Durante la investigación fue necesario conceptualizar como se producen los datos en los activos de información de una organización y cuál es el ciclo de vida de estos, que permitió presentar una propuesta para la recopilación, almacenamiento y procesamiento eficaz de grandes volúmenes de datos de seguridad en tiempo real, así como flujo de datos históricos.

4. Adicionalmente, es importante tener en cuenta el rendimiento y recursos tecnológicos necesarios, para que la plataforma de identificación de amenazas informáticas no sólo opere bajo un esquema de laboratorio de pruebas y ambiente controlado, sino que también se permita su operación en un entorno de producción real. El uso de las tecnologías emergentes, como el Internet de las cosas (IoT), la Analítica de datos y la generación de nuevos algoritmos de Inteligencia artificial, en nuestro medio pueden desarrollarse bajo esquemas más flexibles en cuanto al costo – beneficio, en este sentido incorporar tecnologías en modelos como servicio es una alternativa idónea a nivel organizacional.

5. Para la validación de una arquitectura tecnológica que permita la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC), es necesario definir una guía de recursos de hardware y software, así como el dimensionamiento de un sistema de almacenamiento distribuido, clústers de Elastic Stack, capacitación del personal de Especialistas de Seguridad de la información, además del uso de herramientas del ecosistema de Big Data. Uno de los principales resultados que se persigue, es establecer la carga transaccional óptima de la infraestructura tecnológica; bajo este contexto, los modelos de infraestructura como servicio (IaaS) y plataforma como servicio (PaaS) son válidos para sustentar el crecimiento horizontal proyectado, incluso para organizaciones de tipo pequeñas y medianas empresas (PyMES).

6. En el presente trabajo de titulación, implementó y probó las arquitecturas propuestas, pasando por cuatro perspectivas de arquitectura que se superponen en diferentes capas de abstracción, a saber:

    a. Arquitectura de procesos.
    b. Arquitectura de infraestructura tecnológica
    c. Arquitectura de software.
    d. Arquitectura del negocio.

7. Se evidenció la validez de la arquitectura para la identificación de amenazas informáticas en un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) utilizando herramientas del ecosistema de Big Data, especificando cada uno de los componentes y módulos que intervinieron en cada una de las fases. En virtud del estudio efectuado, se puede concluir que es imperativo que las organizaciones sigan trabajando en procura de madurar sus modelos de Seguridad de la información, fortaleciendo sus equipos de Especialistas e implementando nuevos esquemas para la identificación de amenazas informáticas aplicando modelos predictivos.

4.2. Recomendaciones.

La aplicación de buenas prácticas en la gestión de eventos de seguridad, a nivel de la conformación de un Centro de Operaciones y Monitoreo de Seguridad de la información (SOC) como en la gestión de los eventos de seguridad (Log and Event Management), aporta distintos beneficios, tanto a nivel de funcionamiento de las aplicaciones como de los objetivos de la organización:

1. Aplicación de diversas técnicas de Inteligencia de Negocios, como por ejemplo Machine Learning, permite detectar patrones que ayuden a tomar decisiones de negocio, como son trazas relativas a sistemas de seguridad de la información, entre otros.

2. Mejoramiento en la gestión y el control de la información, facilitando el acceso y la explotación de estos datos contenidos en los activos de la información.

3. Detección de amenazas informáticas, conocidas o desconocidas, permitiendo actuar en consecuencia con rapidez, eficiencia y eficacia.

4. Prevención de fugas y extracción de información, así como comportamientos inadecuados que ocasionen incidentes que repercutan en pérdidas económicas para la organización.

Referencias bibliográficas

ARCOTEL. (2019). *Servicio de acceso a Internet, Boletín estadístico Mayo 2019.* Quito: Agencia de Regulación y Control de las Telecomunicaciones del Ecuador.

Bajpai, A., Arya, A., & Dayanand. (2018). Big Data Analytics in Cyber Security. *International Journal of Computer Sciences and Engineering*, 5.

Berman, J. (2013). *Principles of Big Data: Preparing, Sharing, and Analyzing.* Massachusetts: Elsevier Inc.

Chalmers, S., Picot-Clémente, R., & Bothorel, C. (2013). Big Data - State of the Art. 24.

Cloud Security Alliance. (2013). *Big Data Analytics for Security Intelligence.* Cloud Security Alliance Org.

Elastic Stack. (junio de 2019). *Elastic Stack*. Obtenido de https://www.elastic.co/guide/index.html

Elasticsearch. (junio de 2019). *Elasticsearch, search and analytics engine*. Obtenido de https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html

ESET Inc. (2018). *ESET Security Report Latinoamérica 2018.* Obtenido de https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region

Ezzikouri, H., Erritali, M., & Oukessou, M. (2015). Pretreatment of web log files. *Journal of Information Sciences and Computing Technologies*, 15.

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2017). La seguridad informática y la seguridad de la información. *Polo de conocimiento*, 11.

Filebeat. (junio de 2019). *Filebeat, centralizing log data*. Obtenido de https://www.elastic.co/guide/en/beats/filebeat/current/index.html

Hashem, I., Yaqoob, I., Anuar, N., Mokhtar, S., Gani, A., & Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. *University of Malaya*, 29.

Kibana. (junio de 2019). *Kibana, open source analytics and visualization platform*. Obtenido de https://www.elastic.co/guide/en/kibana/current/index.html

Liu, R., Li, Q., Li, F., & Juhnyoung, L. (2014). Big Data architecture for IT incident management. (I. d. IEEE, Ed.) *International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 5.

Lněnička, M., Máchová, R., Komárková, J., & Čermáková, I. (2017). Components of Big Data Analytics for Strategic Management of Enterprise Architecture. 9.

Lobo, A., & Flórez, A. (2017). *Análisis del proceso de implantación de los sistemas de detección de intrusos basados en big data de código abierto para la detección temprana de incidentes informáticos.* Universidad Pontificia Bolivariana Seccional Bucaramanga.

Logstash. (2019). *Logstash*. Obtenido de https://www.elastic.co/guide/en/logstash/current/index.html

Lucero, J. (2015). La dimensión desconocida. 7.

Masabo, E., Swaib, K., & Sansa-Otim, J. (2018). Big Data: Deep Learning for detecting Malware. *ACM/IEEE Symposium on Software Engineering*, 8.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think.* Boston: Houghton Mifflin Harcourt.

Miloslavskaya, N. (2018). *Security Operations Centers for Information Security Incident Management.* National Research Nuclear University MEPhI, Moscow Engineering Physics Institute, Moscú.

MINTEL. (28 de marzo de 2019). *Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador*. Obtenido de Ecuador trabaja en la Estrategia Nacional de Ciberseguridad: https://www.telecomunicaciones.gob.ec/ecuador-trabaja-en-la-estrategia-nacional-de-ciberseguridad

MINTEL, L. (2018). *Libro Blanco de la Sociedad de la Información y del Conocimento.* Quito: Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Mujawar, S., & Kulkarni, S. (2015). Big Data: Toolsand Applications. *nternational Journal of Computer Applications*, 5.

Netsecurity, I. (abril de 2018). *Security Operations Center*. Obtenido de https://nextsecurity.co/security-operations-center/

NIST, N. (20 de junio de 2019). *National Institute of Standards and Technology*. Obtenido de Cybersecurity Framework NIST: https://www.nist.gov/cyberframework

Oseku-Afful, T. (2016). *The use of Big Data Analytics to protect Critical Information Infrastructures from Cyber-attacks.* Tesis, Luleå University of Technology, Luleå, Suecia.

Patgiri, R., & Majhi, U. (2018). Big Data Security Analytics: Key Challenges. *14th Int. Conference on Data Science (ICDATA'18)* (pág. 5). Las Vegas, Nevada, USA: CSREA Press.

Pérez Marqués, M. (2015). *Big Data. Técnicas, herramientas y aplicaciones.* Madrid: Alfaomega Grupo Editor.

Prajakta, J., & Nitin, P. (2016). Solving Cyber Security Challenges using Big Data. *International Journal of Computer Applications*, 4.

República del Ecuador, P. (2017). *Plan Nacional para el Buen Vivir 2017 - 2021*. Quito: Consejo de Planificación Nacional del Ecuador.

Sharma, G., & Roji, K. (2019). Cyber Security Challenges and Big Data Analytics. *COJ Technical & Scientific Research*, 4.

Sorrentino, P. (2018). Ciberespacio, ciberseguridad y ciberdefensa. *Boletín del Centro Naval de Argentina*, 10.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 21.

Trecebits. (03 de Abril de 2019). *¿Qué ocurre en un minuto en Internet en 2019?* Obtenido de Trecebits: https://www.trecebits.com/2019/04/03/minuto-internet-infografia

Vallejo Martínez, A. (2015). *Arquitectura lambda aplicada a clustering de documentos en contextos Big Data.* Universidad Nacional de Educación a Distancia.

VMware Inc. (2019). *VMware vSphere Hypervisor*. Obtenido de https://www.vmware.com/latam/products/vsphere-hypervisor.html

Wazuh Security Detection. (junio de 2019). *Wazuh Security Detection*. Obtenido de https://documentation.wazuh.com/3.x/getting-started/index.html

Ynzunza Cortés, C., Izar Landeta, J., Bocarando Chacón, J., Aguilar Pereyra, F., & Larios Osorio, M. (2017). El entorno de la Industria 4.0: implicaciones y perspectivas futuras. *Conciencia Tecnológica*, 23.

Anexos

Anexo A – Consolidado de infraestructura virtual.

		TOTAL, RECURSOS	7680	8	---	200		
Host	**Máquinas virtuales**	**Nombre del servidor**	**RAM [MB]**	**CPU [vCores]**	**Compartición CPU**	**HDD 1 [GB]**	**S.O.**	**Disponibilidad**
Host 1	VM1	ngfw.vm.local	768	1	1-1	20	GNU / Linux IPFire 2.23 - Core Update 134	Alta 99,8%
	VM2	master.vm.local	768	1	1-1	20	GNU / Linux CentOS 7.6.1810	Alta 99,8%
	VM3	adds.vm.local	2048	2	1-1	60	Microsoft Windows 2012 R2 de 64 bits	Alta 99,8%
	VM4	elk.vm.local	2048	2	1-1	20	GNU / Linux CentOS 7.6.1810	Alta 99,8%
	VM5	client.vm.local	1024	1	2-1	60	Microsoft Windows 7 de 32 bits	Baja 99,4%
	VM6	kali.vm.local	1024	1	2-1	20	GNU / Linux Kali Linux 2019.2.04	Baja 99,4%

Anexo B – Plan de direccionamiento de infraestructura virtual.

Host	Máquinas virtuales	Nombre del servidor	vEthernet [virtuales]	IP Address	Default Gateway	VLAN	MAC Address
Host 1	VM1	ngfw.vm.local	3	192.168.224.10 10.10.10.10 192.168.100.10	192.168.224.2	WAN DMZ VLAN 10	00-0C-29-99-5B-A1 00-0C-29-99-5B-B5 00-0C-29-99-5B-AB
	VM2	master.vm.local	1	10.10.10.20	10.10.10.10	DMZ	00-0C-29-4A-56-E5
	VM3	adds.vm.local	1	10.10.10.30	10.10.10.10	DMZ	00-0C-29-FF-9D-6C
	VM4	elk.vm.local	1	10.10.10.40	10.10.10.10	DMZ	00-0C-29-9B-6E-5C
	VM5	client.vm.local	1	192.168.100.20	192.168.100.10	VLAN 10	00-0C-29-0C-85-A4
	VM6	kali.vm.local	1	192.168.100.30	192.168.100.10	VLNA 10	00-0C-29-62-F9-77

Anexo C – Instalación de Elastic Stack.

Esta guía describe la instalación de un servidor Elastic Stack, compuesto por Elasticsearch, Logstash, Kibana y Filebeat. Se describe la instalación basada en los paquetes de software de estos componentes.

- **Preparación.**

1. Posterior a la instalación del sistema operativo GNU / Linux CentOS 7.6.1810, verifique si no existen actualizaciones disponibles.

```
# yum update
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.espoch.edu.ec
 * extras: mirror.espoch.edu.ec
 * updates: mirror.espoch.edu.ec
No packages marked for update
```

2. Verifique la correcta configuración de los parámetros de nombre del servidor FQDN (Fully Qualified Domain Name) y la definición de los servidores a desplegar.

```
# hostname
elk.vm.local


# cat /etc/hosts
10.10.10.10    ngfw      ngfw.vm.local
10.10.10.20    master    master.vm.local
10.10.10.30    adds      adds.vm.local
```

```
10.10.10.40    elk       elk.vm.local

192.168.100.20 client    client.vm.local

192.168.100.30 kali      kali.vm.local
```

3. Valide la sincronización del reloj del sistema, a través del servicio NTP (*Network Time Protocol*).

```
# date

Sun Jul 28 04:56:00 -05 2019
```

4. Instale el repositorio Elastic y su clave GPG (*GNU Privacy Guard*).

```
# rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch


# cat > /etc/yum.repos.d/elastic.repo << EOF

[elasticsearch-7.x]

name=Elasticsearch repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

EOF
```

- **Instalación de Elasticsearch.**

Elasticsearch es un motor de búsqueda y análisis de texto completo, altamente escalable.

Para más información https://www.elastic.co/products/elasticsearch

5. Instale el componente Elasticsearch.

```
# yum install elasticsearch-7.3.0
```

6. Habilite e inicie el servicio Elasticsearch.

```
# systemctl daemon-reload


# systemctl enable elasticsearch.service


# systemctl start elasticsearch.service


# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled;
vendor preset: disabled)
  Drop-In: /etc/systemd/system/elasticsearch.service.d
           └─elasticsearch.conf
   Active: active (running) since Sat 2019-08-10 10:14:15 -05; 11h ago
     Docs: http://www.elastic.co
 Main PID: 1063 (java)
   CGroup: /system.slice/elasticsearch.service
           ├─1063 /usr/share/elasticsearch/jdk/bin/java -Xms2g -Xmx2g -
XX:+UseConcMarkSweepGC -XX:CMSInit...
           └─2529 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-
x86_64/bin/controller


Aug 10 10:14:15 elk.vm.local systemd[1]: Started Elasticsearch.
```

```
Aug 10 10:14:40 elk.vm.local elasticsearch[1063]: OpenJDK 64-Bit Server VM
warning: Option UseConcMark...se.
Hint: Some lines were ellipsized, use -l to show in full.
```

- **Instalación de Kibana.**

Kibana es una interfaz web flexible e intuitiva para la extracción y visualización de los eventos y archivos almacenados en Elasticsearch. Para más información https://www.elastic.co/products/kibana

7. Instale el componente Kibana:

```
# yum install kibana-7.3.0
```

8. Instale el plugin de la aplicación Wazuh para Kibana

```
# sudo -u kibana /usr/share/kibana/bin/kibana-plugin install
https://packages.wazuh.com/wazuhapp/wazuhapp-3.9.5_7.3.0.zip
```

9. Kibana sólo recibe tráfico en la interfaz loopback (localhost) por defecto, para que Kibana escuche en todas las interfaces, edite el archivo `/etc/kibana/kibana.yml` descomentando la configuración del parámetro `server.host` y cambie el valor a:

```
server.host: "0.0.0.0"
```

10. Habilitar e iniciar el servicio Kibana.

```
# systemctl daemon-reload
```

```
# systemctl enable kibana.service


# systemctl start kibana.service


# systemctl status kibana.service
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset:
disabled)
   Active: active (running) since Sat 2019-08-10 19:40:42 -05; 2h 4min ago
 Main PID: 23118 (node)
   CGroup: /system.slice/kibana.service
           └─23118 /usr/share/kibana/bin/../node/bin/node --no-warnings --max-
http-header-size=65536 /usr...


Aug          10          21:44:07          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:07Z","t...T 10
Aug          10          21:44:10          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:09Z","t...T 10
Aug          10          21:44:13          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:13Z","tags"...
Aug          10          21:44:20          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:20Z","t...T 10
Aug          10          21:44:23          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:23Z","tags"...
Aug          10          21:44:27          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:27Z","t...T 10
Aug          10          21:44:33          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:33Z","tags"...
```

```
Aug          10          21:44:43          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:43Z","tags"...
Aug          10          21:44:53          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:53Z","tags"...
Aug          10          21:44:54          elk.vm.local          kibana[23118]:
{"type":"response","@timestamp":"2019-08-11T02:44:54Z","t...T 10
Hint: Some lines were ellipsized, use -l to show in full.
```

11. Deshabilite el repositorio Elasticsearch, se recomienda desactivar el repositorio para evitar la actualización involuntaria a una nueva versión de Elastic Stack. Utilice el siguiente comando.

```
# sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/elastic.repo
```

Anexo D – Instalación de Wazuh Server.

El servidor Wazuh puede ser instalado en cualquier sistema operativo tipo Unix, aunque comúnmente se implementa en GNU / Linux. El proceso de instalación puede ejecutarse a través de los paquetes de software.

El proceso de instalación requiere de dos componentes que normalmente se instalan en un servidor Wazuh:

a. Wazuh Manager.
b. Wazuh API.

Además, se requiere el componente denominado Filebeat para enviar la información de registros de eventos hacia Elastic Stack.

- **Añadir el repositorio Wazuh**

1. El primer paso para configurar Wazuh se basa en añadir el repositorio Wazuh al servidor.

```
# rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH


# cat > /etc/yum.repos.d/wazuh.repo <<\EOF
[wazuh_repo]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=Wazuh repository
```

```
baseurl=https://packages.wazuh.com/3.x/yum/

protect=1

EOF
```

- **Instalación del Wazuh Manager**

2. El siguiente paso, es instalar el componente Wazuh Manager en el servidor implementado.

```
# yum install wazuh-manager
```

3. Una vez finalizado el proceso, puede verificar el status del servicio con el siguiente comando.

```
# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/etc/systemd/system/wazuh-manager.service; enabled; vendor
preset: disabled)
   Active: active (running) since Sat 2019-08-10 19:41:38 -05; 2h 5min ago
  Process: 23189 ExecStop=/usr/bin/env ${DIRECTORY}/bin/ossec-control stop
(code=exited, status=0/SUCCESS)
  Process: 23325 ExecStart=/usr/bin/env ${DIRECTORY}/bin/ossec-control start
(code=exited, status=0/SUCCESS)
   CGroup: /system.slice/wazuh-manager.service
           ├─23368 /var/ossec/bin/ossec-csyslogd
           ├─23381 /var/ossec/bin/ossec-integratord
           ├─23394 /var/ossec/bin/ossec-authd
           ├─23400 /var/ossec/bin/wazuh-db
           ├─23420 /var/ossec/bin/ossec-execd
           ├─23428 /var/ossec/bin/ossec-analysisd
```

```
            ├─23434 /var/ossec/bin/ossec-syscheckd
            ├─23443 /var/ossec/bin/ossec-remoted
            ├─23448 /var/ossec/bin/ossec-logcollector
            ├─23472 /var/ossec/bin/ossec-monitord
            └─23478 /var/ossec/bin/wazuh-modulesd


Aug 10 19:41:35 elk.vm.local env[23325]: Started wazuh-db...
Aug 10 19:41:36 elk.vm.local env[23325]: Started ossec-execd...
Aug 10 19:41:36 elk.vm.local env[23325]: Started ossec-analysisd...
Aug 10 19:41:36 elk.vm.local env[23325]: Started ossec-syscheckd...
Aug 10 19:41:36 elk.vm.local env[23325]: Started ossec-remoted...
Aug 10 19:41:36 elk.vm.local env[23325]: Started ossec-logcollector...
Aug 10 19:41:36 elk.vm.local env[23325]: Started ossec-monitord...
Aug 10 19:41:36 elk.vm.local env[23325]: Started wazuh-modulesd...
Aug 10 19:41:38 elk.vm.local env[23325]: Completed.
Aug 10 19:41:38 elk.vm.local systemd[1]: Started Wazuh manager.
```

- **Instalación de Wazuh API.**

4. Se requiere la instalación del servidos NodeJS 4.6.1 o superior, el cual es necesario para ejecutar Wazuh API. Se recomienda añadir el repositorio oficial de NodeJS.

```
# curl --silent --location https://rpm.nodesource.com/setup_8.x | bash -
```

5. A continuación, instale NodeJS.

```
# yum install nodejs
```

6. Instale el componente Wazuh API. Se actualizará NodeJS si fuera necesario:

```
# yum install wazuh-api
```

7. Una vez finalizado el proceso, puede verificar el status del servicio con el siguiente comando.

```
# systemctl status wazuh-api
● wazuh-api.service - Wazuh API daemon
   Loaded: loaded (/etc/systemd/system/wazuh-api.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2019-08-10 19:41:42 -05; 2h 6min ago
     Docs: https://documentation.wazuh.com/current/user-manual/api/index.html
  Process: 23969 ExecStop=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
 Main PID: 23978 (node)
   CGroup: /system.slice/wazuh-api.service
           └─23978 /bin/node /var/ossec/api/app.js

Aug 10 19:41:42 elk.vm.local systemd[1]: Started Wazuh API daemon.
```

8. Se recomienda desactivar el repositorio Wazuh para evitar actualizaciones accidentales. Para ello, utilice el siguiente comando.

```
# sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/wazuh.repo
```

- **Instalación de Filebeat**

9. Filebeat es el componente en el servidor Wazuh, que envía de forma segura las alertas y registros de eventos almacenados en Elasticsearch. Es necesario instalar el repositorio Elastic y su clave GPG (*GNU Privacy Guard*).

```
# rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch


# cat > /etc/yum.repos.d/elastic.repo << EOF
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

10. Instale Filebeat.

```
# yum install filebeat-7.3.0
```

11. Descargue el archivo de configuración de Filebeat, desde el repositorio Wazuh. Este archivo está preconfigurado para enviar las alertas y registros de eventos de Wazuh hacia Elasticsearch

```
# curl -so /etc/filebeat/filebeat.yml
https://raw.githubusercontent.com/wazuh/wazuh/v3.9.5/extensions/filebeat/7.x/
filebeat.yml


# chmod go+r /etc/filebeat/filebeat.yml
```

12. Descargue la plantilla de alertas para Elasticsearch

```
# curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v3.9.5/extensions/elasticsearch
/7.x/wazuh-template.json


# chmod go+r /etc/filebeat/wazuh-template.json
```

13. Edite el archivo de configuración `/etc/filebeat/filebeat.yml` y reemplace `YOUR_ELASTIC_SERVER_IP` por la dirección IP o el nombre FQDN (Fully Qualified Domain Name) del servidor Elasticsearch.

```
output.elasticsearch:
  hosts: ['http://elk.vm.local:9200']
  indices:
    - index: 'wazuh-alerts-3.x-%{+yyyy.MM.dd}'
```

14. Habilite e inicie el servicio Filebeat.

```
# systemctl daemon-reload


# systemctl enable filebeat.service


# systemctl start filebeat.service


# systemctl status filebeat.service
● filebeat.service - Filebeat sends log files to Logstash or directly to
Elasticsearch.
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; vendor
preset: disabled)
   Active: active (running) since Sat 2019-08-10 19:11:29 -05; 2h 40min ago
```

```
     Docs: https://www.elastic.co/products/beats/filebeat
 Main PID: 20659 (filebeat)
   CGroup: /system.slice/filebeat.service
           └─20659       /usr/share/filebeat/bin/filebeat        -e        -c
/etc/filebeat/filebeat.yml -path.home /usr/shar...


Aug  10  21:47:29  elk.vm.local  filebeat[20659]:  2019-08-10T21:47:29.226-0500
INFO        [monitoring...
Aug  10  21:47:59  elk.vm.local  filebeat[20659]:  2019-08-10T21:47:59.228-0500
INFO        [monitoring...
Aug  10  21:48:29  elk.vm.local  filebeat[20659]:  2019-08-10T21:48:29.225-0500
INFO        [monitoring...
Aug  10  21:48:59  elk.vm.local  filebeat[20659]:  2019-08-10T21:48:59.224-0500
INFO        [monitoring...
Aug  10  21:49:29  elk.vm.local  filebeat[20659]:  2019-08-10T21:49:29.224-0500
INFO        [monitoring...
Aug  10  21:49:59  elk.vm.local  filebeat[20659]:  2019-08-10T21:49:59.225-0500
INFO        [monitoring...
Aug  10  21:50:29  elk.vm.local  filebeat[20659]:  2019-08-10T21:50:29.225-0500
INFO        [monitoring...
Aug  10  21:50:59  elk.vm.local  filebeat[20659]:  2019-08-10T21:50:59.224-0500
INFO        [monitoring...
Aug  10  21:51:29  elk.vm.local  filebeat[20659]:  2019-08-10T21:51:29.225-0500
INFO        [monitoring...
Aug  10  21:51:59  elk.vm.local  filebeat[20659]:  2019-08-10T21:51:59.224-0500
INFO        [monitoring...
Hint: Some lines were ellipsized, use -l to show in full.
```

Anexo E – Agentes Wazuh.

El agente Wazuh se implementará en los activos de información que se precisa monitorizar. Es multi – plataforma y proporciona las siguientes capacidades:

a. Registro y recopilación de datos.
b. Monitoreo de la integridad de los archivos.
c. Detección de rootkits y malware.
d. Monitoreo de políticas de seguridad.
e. Evaluaciones de configuración.
f. Inventario de software.

Además, se comunica con el componente Wazuh Manager, enviando datos en tiempo real a través de un canal encriptado y autenticado. Existen varias opciones para instalar un agente Wazuh, dependiendo del sistema operativo, a saber:

a. GNU / Linux.
b. Microsoft Windows.
c. macOS.
d. Oracle Solaris.
e. HP-UX.
f. AIX.

Vita



Fabián Eduardo Balseca Chávez, Ingeniero de Sistemas e Informática graduado de la Universidad de las Fuerzas Armadas – Escuela Politécnica del Ejército (2004), con formación profesional en el campo de la Ingeniería del software, Desarrollo e infraestructura tecnológica, Comunicaciones y redes de datos, Seguridad de la información, Inteligencia de Negocios y Análisis de datos.

E-mail: fabianbch@yahoo.com