UNIVERSIDAD IBEROAMERICANA

Facultad de Ingeniería

Escuela de Ingeniería en Tecnologías de la Información y la Comunicación

Proyecto de grado para optar por el título de:

Ingeniero/a en Tecnologías de la Información y la Comunicación

PROYECTO DE GRADO

Creación e Implementación de un Sistemas de Gestión de Eventos e Información de Seguridad Para la Fintech GCS LTD: JH Collected Event Detector

Sustentantes:

José Manuel Pinales Figuereo 19-0737

Hanvan Sham Hernández 19-0783

Asesor/A:

Dr. Darwin Crisanto Muñoz Núñez

Santo Domingo, República Dominicana

01 de agosto del 2022

Dedicatoria

En primer lugar, a Dios, quien me ha guiado por el camino del bien y ha permitido que todo esto sea posible. A mi madre Justiliana A. Hernández Taveras por ser el motor principal que me impulsa a desarrollarme y a luchar en la vida.

A la memoria de mi padre Sham Shung Keung que, aunque no está a mi lado físicamente, fue mi guía para avanzar, superarme y siempre darme el apoyo incondicional que me ha permitido seguir adelante en diferentes procesos de la vida.

A mis hermanos y sobrinos para que me sigan los pasos; que me vean como su guía y sepan que todo con esfuerzo, empeño y aptitud se puede lograr, que nada en la vida es fácil, pero tampoco imposible y siempre vayan detrás de sus sueños y metas y sobre todo tengan aspiraciones de salir adelante, de ser personas de bien y prepararse para ser mejores ciudadanos y de esta manera podrán ofrecerle a nuestra familia la estabilidad que todo ser humano desea tener.

Hanvan Sham H.

Quiero dedicar mi proyecto de grado a Dios, pues porque todo lo que he logrado ha sido por su gracia y su misericordia. Luego a mi madre Gregoria Figuereo, que siempre estuvo apoyándome y ayudándome a superar cada paso en esta carrera.

También a mis hermanos, Junior y Mayerin Pinales, han sido un ejemplo para seguir. Además, quisiera dedicarlo a mi padre, el cual me enseñó que con empeño y dedicación puedo lograr mis metas.

José Manuel Pinales

Agradecimientos

A Dios por darme salud, sabiduría e iluminarme en cada paso que doy; por ser el centro y bastón de mi vida.

A mis compañeros de estudios en especial a José Manuel Pinales y Starling Javier Eusebio Bonifacio, quienes son más que una amistad.

A la Universidad Iberoamericana UNIBE por darme la oportunidad de ingresar y pertenecer a tan prestigiosa casa educativa para la formación de mi estudio profesional, en especial a la Escuela de Ingeniería en Tecnologías de la Información y la Comunicación y cada uno de los maestros que estuvieron capacitándome y preparándome para no ser una profesional mediocre.

A mi familia, en especial a mi madre Justiliana A. Hernández Taveras, por ser ejemplar, sabia y astuta; y siempre apoyarme y acompañarme en las buenas y en las malas, por brindarme todo su apoyo incondicional en cada etapa de mi vida, por su cooperación, comprensión y valentía.

A mi padre Sham Shung Keung que, aunque no está a mi lado físicamente, es mi fuente de inspiración para avanzar, superarme y realizarme como una gran profesional.

A mis hermanos Meilen Sham Hernández, Hansen Sham Hernández, Juliana Gómez Taveras, Isabel Arias Taveras y Gilberto Gómez Taveras por apoyarme siempre en mis proyectos; a pesar de nuestras diferencias me han apoyado en todo momento en mis desafíos y retos que me he propuesto para prepararme y profesionalizarme, a todos mis tíos, primos, sobrinos y mi padrino German Pimentel por ser parte de mi fuente de inspiración para superarme, romper pautas y no detenerme por más desafíos que me encuentre en la vida.

A Jafreisy Alcántara Vicente por siempre acompañarme, comprenderme y apoyarme en todas las etapas buenas y no tan buenas que la vida me ha presentado durante nuestro noviazgo, por siempre afrontar juntos las dificultades que se nos presentan por motivarme y

enseñarme que si caigo debo levantarme y continuar con más fuerzas, además de todo por ser una amiga fiable en la cual siempre poder contar y a Juana Vicente por siempre aconsejarme como si fuera su hijo, por sus consejos siempre persistente para que siempre salga adelante en busca de mejoría y mejor vida.

Hanvan Sham H.

Primero, gracias a Dios, por darme la oportunidad, la capacidad y las fuerzas necesarias para hoy en día lograr una de mis metas más anheladas.

Gracias a mis padres, José Pinales y Gregoria Figuereo, a mis hermanos, Junior y Mayerin Pinales, por darme el apoyo y la motivación necesaria para seguir adelante con mis estudios.

Gracias a mi compañero, Hanvan Sham, su consistencia siempre fue una cualidad digna de admirar. Starling Javier, quien me apoyó y me dio la mano en múltiples ocasiones. Edinson Montero, que en todo momento me ofreció su apoyo. Agradezco a mis maestros, por luchar y dar lo mejor de cada uno, para que hoy seamos mejores profesionales.

José Manuel Pinales

Abstract

Today the application of ICT is a necessity for the development and evolution of all companies. ICTs represent one of the most important sectors in the world we live in, they help to have efficient, fast and clear communication between various members of the same organization, benefiting indispensable sectors such as finance, education and health.

Today, companies produce a large amount of information. Mastering this data is impossible without the use of Security Information and Event Management Systems (SIEM) to centralize records management and increase the level of information security and data protection in the organization. A SIEM provides proactive threat detection and real-time analysis of system activity. Managing these problems will be very difficult without relying on established SIEM.

Through the construction and implementation of a security information and event management system we can have better control of activities within an organization allowing it to acquire new capabilities, determining factors for data protection in current business environments, and at the same time to detect fraudulent negative impact events.

Keywords: SIEM, Correlation, Data, Events, threats, cybersecurity.

Resumen

Hoy en día la aplicación de la TIC es una necesidad para el desarrollo y evolución de todas las empresas. Las TIC representan unos de los sectores más importantes en el mundo que vivimos, estas ayudan a tener una comunicación eficiente, rápida y clara entre diversos miembros de una misma organización, beneficiando sectores indispensables como las finanzas, la educación y la salud.

En la actualidad las empresas producen una gran cantidad de información. El dominio de estos datos es imposible sin el uso de Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) para centralizar la gestión de registros y aumentar el nivel de seguridad de la información y protección de datos en la organización. Un SIEM proporciona detección proactiva de amenazas y análisis en tiempo real de la actividad del sistema. Manejar estos problemas será muy difícil sin depender de SIEM consolidado.

Mediante la construcción e implementación de un sistema de gestión de eventos e información de seguridad podemos tener un mejor control de las actividades dentro de una organización permitiéndole adquirir nuevas capacidades, determinantes para la protección de los datos en los entornos actuales de negocio, y al mismo tiempo detectar eventos fraudulentos de impacto negativo.

Palabras Claves: SIEM, Correlación, Datos, Eventos, amenazas, Seguridad informática.

Tabla de contenido

Dedicatoria ii

Agradecimientos iv

Abstract vii

Keywords: SIEM, Correlation, Data, Events, threats, cybersecurity. vii

Resumen viii

Palabras Claves: SIEM, Correlación, Datos, Eventos, amenazas, Seguridad informática. viii

Lista de figuras xvi

Lista de tablas xviii

Capítulo I: Introducción e información general 1

1.0 Introducción 2

1.1 Planteamiento del Problema 3

1.2 Situación Actual 4

1.2.3 Tendencia de tráfico de Fuerza Bruta | enero-marzo 5

1.3 Justificación de la investigación 7

1.4 Importancia e interés del tema 8

1.5 Limitaciones 8

1.6 Hipótesis Preliminar 8

1.7 Objetivos 9

1.7.1 Objetivo General. 9

1.7.2 Objetivos Específicos. 9

1.8 Preguntas de investigación 9

CAPÍTULO 2: Marco Teórico y Estado del Arte 11

2.0 Introducción al capítulo 12

2.1 Antecedentes y referencias 13

2.1.1 Aplicaciones Similares. 19

2.1.1.1 OSSIM (Open-Source Security Information Management). 19

2.1.1.2 Sagan log analysis engine. 20

2.2 Base Teórica 20

2.2.1 Elasticsearch, Logstash y Kibana (ELK). 20

2.2.2 Beats. 20

2.2.3 SIEM. 20

2.2.4 Características de sistemas SIEM. 21

2.2.5 Acceso centralizado y administración de logs. 21

2.2.6 Logs. 22

2.2.7 Cumplimiento normativo de TI. 22

2.2.8 Correlación de eventos. 22

2.2.9 Respuesta activa (monitoreo y seguridad). 23

2.2.10 Amenazas 23

2.2.10.2 Amenazas externas. 24

2.2.11 Vulnerabilidades. 24

2.2.12 Configuración errónea. 25

2.2.13 Sistemas operativos.....25

2.2.14 Software libre.....26

2.2.15 Fintech. 28

2.2.16 Inteligencia artificial (IA). 29

2.2.17 API. 29

2.2.18 Datos. 30

2.2.19 Antivirus / antimalware (AV/AM). 30

2.2.20 Bot/Botnet. 30

2.2.21 Brecha de seguridad. 31

2.2.22 Ataque distribuido de denegación de servicio (DDoS). 31

2.2.23 Firewall. 31

2.2.24 Ingeniería social. 31

2.2.25 Red privada virtual (VPN). 31

2.2.26 Malware. 32

2.2.27 Virus.....32

2.2.28 Filtrado web. 32

2.2.29 Gusano. 32

2.2.30 IPS. 32

2.2.31 Dirección IP. 33

2.2.32 Objetivos de la seguridad. 33

2.2.33 Normas ISO 27001. 34

2.2.34 Monitoreo de redes. 34

2.3 Base Legal. 34

2.3.1 Ley de Ciberseguridad de la República Dominicana. 34

2.3.2 Ley 310-14, ley que regula el envío de correos electrónicos comerciales no solicitados (spam). 35

2.3.3 El Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria. 36

2.3.4 Protección de datos personales. 38

CAPÍTULO 3: Marco Metodológico 40

3.0 Introducción al capítulo 41

3.1 Tipo de investigación (metodología) 41

3.2 Método 42

3.3 Investigación Preliminar 42

3.4 Delimitación del problema 42

3.4.1 Área geográfica. 43

3.4.2 Tiempo. 43

3.4.3 Población y muestra. 43

3.4.4 Técnicas e Instrumentos 44

3.4.5 Técnica de procesamiento de análisis de datos. 45

3.4.6 Fuentes de datos. 45

CAPÍTULO 4: Plan de mercadeo y Análisis del entorno 46

4.0 Introducción al capítulo 47

4.1 Benchmarking....47

4.2 Mecanismo para poblar información al sistema....47

4.3 Modelo de negocio (Método Canvas)....48

4.4 Presupuesto....49

4.5 Retorno de la Inversión....50

CAPÍTULO 5: Análisis, presentación de resultados y Conclusiones....51

5.0 Introducción al Capítulo....52

5.1 Encuesta....52

5.1.1 APARTADO #1....53

5.1.2 APARTADO #2....55

5.2 Entrevistas....57

5.3 Resultados de la Hipótesis planteada....58

5.4 Verificación y evaluación de Objetivos....58

5.4.1 Verificación Objetivo General.....58

5.4.2 Verificación Objetivo Específicos.....59

5.4.3 Repuestas a las preguntas de investigación.....59

5.5 Conclusiones....61

5.6 Líneas Futuras de Investigación....61

CAPÍTULO 6: Análisis y Diseño del Prototipo....62

6.0 Introducción al capítulo....63

6.1 Narrativa General....63

6.1.1 Objetivos de la Institución, Empresa o Sector al que está dirigido el Proyecto. 63

6.1.2 Breve descripción del sistema propuesto. 63

6.1.3 Objetivos del sistema o proyecto. 64

6.1.4 Innovaciones del sistema propuesto 64

6.1.5 Ventajas y Beneficios. 64

6.2 Análisis FODA del sistema propuesto. 65

6.3 Análisis funcional del sistema 66

6.4 Diagramas de flujo de los procesos: 67

6.5 Diagrama de Flujo de Datos (DFD) del sistema propuesto: 68

6.6 Diseño de la Base de Datos 68

6.6.1 Esquema de la base de datos. 69

6.6.2 Diagrama Entidad Relación (E-R). 69

6.6.3 Diccionario de datos del sistema. 70

6.7 Recolección de datos 72

6.8 Formato de pantallas para las E/S de datos del sistema 72

6.9 Diagrama jerárquico de programas y/o menús principales 79

6.10 Seguridad y Control 79

6.10.1 Políticas de acceso seguridad. 79

6.10.2 Políticas de Backup sugeridas. 80

6.10.3 Descripción mecanismos de seguridad del sistema. 80

6.11 Especificaciones generales de programas 80

6.11.1 Elastic Stack (ELK). 80

6.12 Descripción de programas 81

6.12.1 Tecnología a utilizar. 82

6.13 Cronograma de actividades para el desarrollo del sistema (en MS Project) 84

Conclusiones 85

Referencias 86

APÉNDICE 89

ANEXOS 95

VITA 96

Lista de figuras

Figura No. 1 Boletín mensual marzo CNCS (2021) 5

Figura No. 2 Boletín mensual marzo CNCS (2021) 5

Figura No. 3 Boletín mensual marzo CNCS (2021) 6

Figura No. 4 Boletín mensual marzo CNCS (2021) 6

Figura No. 5 Plantilla Modelo de Negocio CANVAS 48

Figura No. 6 Análisis FODA. Fuente: elaborado por los sustentantes. 65

Figura No. 7 Diagrama de contexto del sistema. Fuente: Elaborado por los sustentantes. 66

Figura No. 8 Diagrama de flujo de procesos ELK. Fuente: elastic (2022) 67

Figura No. 9 Diagrama de Flujo de Datos (DFD) ELK. Fuente: Technolush (2022) 68

Figura No. 10 Esquema Elasticsearch. Fuente: Hackolade (2022) 69

Figura No. 11 Recolección, Diagrama Solución. Fuente: elaborado por los sustentantes.. 72

Figura No. 12 Pantalla login de nuestro SIEM 73

Figura No. 13 Pantalla de inicio luego de hacer acceder. 73

Figura No. 14 Plantilla de integración. 74

Figura No. 15 Eventos recibidos de intentos de login SSH 75

Figura No. 16 Alertas creadas de acuerdo a los eventos recibidos. 75

Figura No. 17 Integración de un equipo a monitorear. 76

Figura No. 18 Creación de reglas. 77

Figura No. 19 Opciones para definir políticas. 77

Figura No. 20 Monitoreo de servicios. 78

Figura No. 21 Flujo de nuestra red de datos. 78

Figura No. 22 Diagrama jerárquico. Fuente: Elaborado por los sustentantes. 79

Figura No. 23 ELK stack. Fuente: Victor Cordero. 83

Figura No. 24 A-1 Gráfico de: ¿Sabes usted lo que es una FINTECH? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.....89

Figura No. 25 A-2 Gráfico de: ¿Conoces el propósito de una FINTECH? Fuente: Elaborado en base a resultado de la aplicación de la encuesta. 89

Figura No. 26 A-3 Gráfico de: En qué área de GCS LTD labora. Fuente: Elaborado en base a resultado de la aplicación de la encuesta. 90

Figura No. 27 A-4 Gráfico de ¿Sabe usted cuales son los diferentes riesgos de seguridad de la información que enfrenta GCS LTD? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.....91

Figura No. 28 A-5 Gráfico de ¿Conoce usted lo que es un SIEM y cuál es su utilidad? Fuente: Elaborado en base a resultado de la aplicación de la encuesta. 92

Figura No. 29 A-6 Gráfico de ¿Cree usted que es necesario utilizar un SIEM en la Empresa GCS LTD? Fuente: Elaborado en base a resultado de la aplicación de la encuesta. 92

Figura No. 30 A-7 Instalación ES, llave repositorio para Elastic. 93

Figura No. 31 A-8 Instalación ES, repositorio 7.17.3.....93

Figura No. 32 A-9 Instalación ES, habilitar servicio. 93

Figura No. 33 A-10 Configuración ES, Usuario X-Pack.....94

Figura No. 34 A-11 Configuración ELK, Kibana Keystore. 94

Lista de tablas

Tabla No. 1 Principales delitos cibernético denunciados en enero-marzo 2021……...7

Tabla No. 2 Presupuesto de solución SIEM……49

Tabla No. 3 Retorno de Inversión……...50

Tabla No. 4 Campos esperado para los índex…….71

Tabla No. 5 Diagrama de Gantt, Planificación del proyecto……...84

Capítulo I: Introducción e información general

1.0 Introducción

Las Tecnologías de la Información (TIC) se mantienen en constante evolución donde cada individuo, empresa e institución necesita de dispositivo tecnológico para el desarrollo de sus actividades, estos equipos de alguna manera u otra están conectado a las redes, brindándonos grandes beneficios, de igual modo están en la órbita de grupos o personas no éticas cuyo objetivos es violar la privacidad de cada ente para el robo de información o impactar la continuidad de una organización de forma negativa.

Por ello se han creado una variedad de soluciones que ayuda a detectar, prevenir y alertar cualquier evento con patrón fraudulento, desde los antiguos antivirus hasta softwares sofisticados con inteligencia artificial para hacer frente a cualquier intento que pueda provocar daños a los sistemas y equipos de una persona u negocio.

Nos referimos a soluciones SIEM. Las organizaciones no cuentan con una herramienta para el monitoreo de sus redes de datos, debido a los costos del mismo en el mercado y la complejidad de la construcción e implementación de la solución. El nuevo reglamento de seguridad cibernética y de la información emitido por el banco central de la República Dominicana busca que toda entidad financiera tenga un Sistemas de Gestión de Eventos e Información de Seguridad para cumplimiento ante este marco.

Nuestro proyecto de grado busca solventar esta problemática dentro de la Fintech GCS con la construcción de un SIEM usando ELK (Elasticsearch, Logstash y Kibana), adaptado a la necesidad del negocio, donde se tenga un monitoreo en tiempo real de los equipos de comunicación, seguridad informática y servidores de la empresa.

1.1 Planteamiento del Problema

La República Dominicana posee el Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria, el cual obliga a toda entidad financiera autorizada por la Junta Monetaria a poseer herramientas de seguridad informática para tratar el riesgo tecnológico y evaluarse adecuadamente, en otras palabras, debe ser correctamente identificado, medido, gestionado y mitigado. Además de tener definido un gobierno corporativo y una estructura de respuesta a incidentes.

Muchas entidades financieras, especialmente las Fintech, no cuentan con una solución para identificar, medir, gestionar y mitigar cualquier evento fraudulento en tiempo real, debido a la complejidad de implementar y construir dicha solución, para así cumplir con el reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria. Por lo tanto, evaluando la panorámica actual de la Fintech GCS, hemos decidido llevar a cabo la construcción e implementación de un Sistemas de Gestión de Eventos e Información de Seguridad llamado JH Collected Event Detector, que permitirá a la empresa GCS monitorear en tiempo real las diferentes conexiones, equipos de seguridad, equipos de comunicación, servidores, etc.

JH Collected Event Detector permitirá a la Fintech contar con diferentes alertas para detectar cualquier ataque cibernético en tiempo real, identificarlo, tratarlo y colaborar a la gestión de respuesta a incidentes de la organización.

1.2 Situación Actual

Los sistemas informáticos han sido transformados radicalmente, han sido reemplazadas por múltiples entornos: red de área local (LAN), red de área amplia (WAN), múltiples nubes, centro de datos, trabajador remoto, Internet de las cosas (IoT), dispositivos móviles y más, cada uno con sus riesgos y vulnerabilidades únicos. Los dispositivos inteligentes que interactúan con los usuarios, como los asistentes virtuales basados en inteligencia artificial, recopilan y almacenan volúmenes de información sobre sus usuarios.

Poner en peligro dichos dispositivos puede generar información valiosa que puede hacer que los ataques basados en ingeniería social sean mucho más exitosos. Por causa de estas brechas, un alto número de ataques son dirigidos a las redes empresariales y servicios brindados por las compañías.

En un informe emitido por la empresa Fortinet (NASDAQ: FTNT), muestran los resultados para el cuarto trimestre de 2020 de los intentos de ciberataques obtenidos por su laboratorio de inteligencia de amenazas FortiGuard Labs, que colecta y analiza diariamente incidentes de ciberseguridad en todo el mundo. En República Dominicana se registraron más de 158 millones de intentos de ciberataques durante 2020, de un total de 41 billones en América Latina y el Caribe.

Luego de haber sido detectado el primer caso de COVID-19 en la República Dominicana en el 2020, se visualizó un aumento exponencial en los ataques de Botnet lo cuales incrementaron un 382% en relación al mes de abril de 2019.

Para el último boletín mostrado por el CSIRT-RD sobre el monitoreo del ciberespacio dominicano, durante el mes de marzo del año 2021 destacan 11,981 direcciones IP públicas que han sido comprometidas por ataques de infecciones de Botnet, refleja un aumento de 16% en comparación a febrero del presente año. Este aumento de los eventos de Botnet está correlacionado con el aumento de los casos de fuerza bruta, estando presente varias de estas

direcciones IP en la generación de ataques de fuerza bruta. Estos eventos han presentado un aumento en un 50% con respecto al mes de febrero.

1.2.3 Tendencia de tráfico de Fuerza Bruta | enero-marzo

Indicador que refleja los servicios de internet a través de los cuales se generan ataques para vulnerar otras localidades.

Figura No. 1 Boletín mensual marzo CNCS (2021)

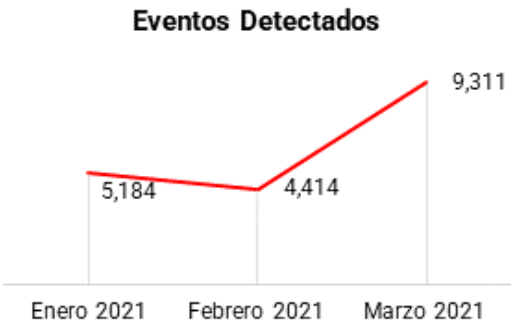


Figura No. 2 Boletín mensual marzo CNCS (2021)

Figura No. 3 Boletín mensual marzo CNCS (2021)

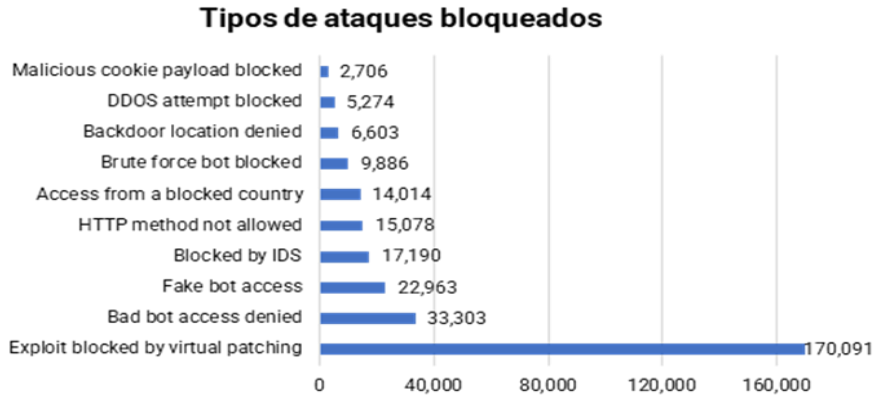


Figura No. 4 Boletín mensual marzo CNCS (2021)

Tabla No. 1

Principales delitos cibernéticos denunciados durante los meses enero-marzo 2021

Estafas	Extorsión	Robo de Identidad	Phishing	Skimming	Acceso Ilícito
65%	12%	6%	5%	4%	3%

Nota. Fuente: Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), Policía Nacional.

JH Collected Event Detector no solo permite la monitorización de las actividades que se llevan a cabo dentro de la red, sino que también puede brindar un sistema automatizado que puede buscar y descubrir ataques después del hecho y antes de que ocurran.

1.3 Justificación de la investigación

Los principales motivos que nos llevan a realizar la siguiente investigación son la falta de soporte en la parametrización de herramienta de seguridad informática en la fintech, la determinación de la causa de los riesgos, la detención de cambio en los sistemas informáticos, los altos niveles de ataques cibernético en la últimas décadas, el cumplimiento del reglamento de seguridad informática y la automatización de tareas para el análisis de los eventos fraudulento, esta solución permitirá a los agentes de seguridad tener un mejor control de todo lo que pueda pasar en su sistemas y equipos, además de tener una mejor respuesta a incidente de seguridad.

1.4 Importancia e interés del tema

Consideramos que este proyecto es de suma importancia debido a que gracias a esta solución es posible tener un control total sobre todos los eventos que suceden en la empresa para poder detectar cualquier tendencia o patrón fuera de lo común y así actuar de forma inmediata. Otra importancia es la automatización de tareas para el análisis de los datos y poder identificar de forma acelerada cualquier ataque cibernético.

1.5 Limitaciones

Dentro de las limitaciones existente en el proyecto se pueden destacar:

1. El prototipo se implementará en el ambiente de desarrollo por política de la empresa GCS.
2. La investigación estará limitada a la Fintech GCS LTD, ubicada en el Distrito Nacional.
3. Debida aprobación de departamento de riesgo y cumplimiento para la implementación del prototipo.

1.6 Hipótesis Preliminar

Mediante la recolección de eventos e información de seguridad de los equipos tecnológicos de una organización, se reducirá el riesgo de ataques cibernéticos, aportará capacidad de respuesta en tiempo real, contribuyendo a la disponibilidad de los servicios de la empresa.

1.7 Objetivos

1.7.1 Objetivo General.

Demostrar que una solución de Gestión de Eventos e información de Seguridad, eficientiza la detección de patrones de ataques e identifica las vulnerabilidades potenciales, protegiendo a las empresas y a sus clientes de devastadoras filtraciones de datos, además de validar la salubridad de los equipos críticos de TI.

1.7.2 Objetivos Específicos.

Analizar los riesgos de la red en GCS para determinar los tipos y valoración de los dispositivos.

1. Desarrollar e implementar de manera efectiva el sistema de gestión de eventos y seguridad de la información, para monitorear los servidores, equipos de comunicaciones y soluciones de seguridad informática críticos en GCS Systems.
2. Realizar una prueba piloto de nuestra herramienta en GCS Systems, empresa especializada en procesamiento a gran escala de transacciones financieras.
3. Combinar el stack ELK (Elasticsearch, Logstash y Kibana), como un SIEM.
4. Demostrar que es posible implementar ELK como SIEM para detectar, analizar y responder a las diferentes amenazas cambiantes.

1.8 Preguntas de investigación

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad, identificar eventos con patrones fraudulentos?

¿Puedes un Sistemas de Gestión de Eventos e Información de Seguridad mantenerse al tanto de toda la información sobre seguridad en tiempo real?

¿Permite un Sistemas de Gestión de Eventos e Información de Seguridad general reporte del número de eventos fraudulentos analizado y detectado en una organización?

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad detectar, analizar y responder amenazas cambiantes?

¿Permite un Sistemas de Gestión de Eventos e Información de Seguridad gestionar potenciales vulnerabilidades de forma proactiva?

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad evitar devastadoras violaciones de datos causadas tanto por agentes de riesgo internos como por amenazas externas?

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad elaborar una respuesta rápida a los impactos y amenazas de seguridad previamente desconocidas?

CAPÍTULO 2: Marco Teórico y Estado del Arte

2.0 Introducción al capítulo

Este capítulo tiene como objetivo tratar el marco teórico y estado del arte de nuestra investigación, donde procuramos mostrarle el estado y evolución de los sistemas de Gestión de Eventos e Información de Seguridad, limitando nuestra investigación a Europa, USA y Latinoamérica.

En este capítulo también se detallan los conceptos que sirven como base teórica para nuestro proyecto. Se definen varios términos de seguridad informática, debido a que el sistema JH Collected Event Detector busca descubrir y prevenir las brechas digitales de las empresas financieras orientadas a la tecnología.

Además, se detallarán las diferentes leyes que regulan el área de seguridad informática. Es necesario mencionar que, en la República Dominicana, se crea el Centro Nacional de Ciberseguridad la cual se dedicada al desarrollo de la ciberseguridad, al fortalecimiento de la confianza digital del usuario dominicano y la cual es la principal ley en la cual se basa este proyecto.

2.1 Antecedentes y referencias

Los registros del sistema de monitoreo se han vuelto más frecuentes a medida que los ataques cibernéticos complejos fuerzan el cumplimiento y los mecanismos regulatorios para exigir controles de seguridad de registro dentro de un marco de gestión de riesgos. Los niveles de registro, los cuales ofrecen indicaciones sobre la importancia y la urgencia del mensaje, comenzaron con la función principal de solucionar errores del sistema o depurar el código.

A medida que los sistemas operativos y las redes han aumentado en complejidad, también lo ha hecho la generación de eventos y registros en estos sistemas. En comparación, el registro de los eventos del sistema, la seguridad y las aplicaciones no es la única forma de realizar una respuesta a incidentes. Ofrecen la capacidad de rastrear las actividades de casi cualquier sistema o movimiento relacionado con el usuario durante un período determinado.

Desde finales de 1970 hubo una formación de grupos de trabajo para ayudar a establecer los criterios para la gestión de programas de auditoría y monitoreo y cómo se pueden usar los registros del sistema para amenazas internas, respuesta a incidentes y resolución de problemas. Esto también estableció una discusión base para muchos de los conceptos que todavía se utilizan en la ciberseguridad moderna. Ver Basis for Audit and Evaluation of Computer Security de la publicación especial 500-19 del National Institute of Standards and Technology (NIST) publicada en 1977.

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una solución de software que tiene como objetivo ofrecer a las empresas información valiosa sobre potenciales amenazas de seguridad de sus redes críticas de negocio, mediante la normalización de datos y priorización de amenazas. Esto es posible a través de un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas,

que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones. (Berjano, 2018).

Gartner acuñó el término “SIEM" en un reporte de 2005 titulado “Mejore la Seguridad de IT con la Gestión de Vulnerabilidades”. El término reúne los conceptos de Gestión de Eventos de Seguridad (SEM) con el de Gestión de Información de Seguridad (SIM), para obtener lo mejor de ambos mundos. SEM cubre la monitorización y correlación de eventos en tiempo real, al mismo tiempo que alerta la configuración y vistas de consola relacionadas con esas actividades. Por su parte, SIM lleva estos datos a una siguiente fase que incluye el almacenamiento, análisis y generación de reportes de los resultados.

Antes de 2005, había una disputa sobre la gestión de información de seguridad (SIM) y la gestión de eventos de seguridad (SEM). Esta discusión terminó tuvo fin gracias a Amrit Williams y Mark Nicollet de Gartner cuando definieron SIEM - Gestión de eventos de información de seguridad en 2005. Según la definición de Williams y Nicollet, una solución SIEM deberá:

- Ser capaz de analizar, recopilar y presentar información después de recopilarla de la red y los dispositivos de seguridad conectados.
- Disponer de aplicaciones de gestión de identidades y accesos,
- Disponer de herramientas para la gestión de vulnerabilidades y el cumplimiento de políticas.
- Consiste en el sistema operativo, los registros de la aplicación y la base de datos, y
- Datos de amenazas externas.

Al diferenciar la definición entre SIM y SEM, SIM se ocupa específicamente del almacenamiento, análisis y generación de informes de datos de registro. Recopila datos de varios dispositivos de seguridad y de la red. Por otro lado, SIEM procesa datos en tiempo real

para monitorear, correlacionar y notificar eventos de seguridad que se generan de manera regular.

Las soluciones SIEM se insertaron a partir del año 2000 en forma de una solución SIM o una solución SEM. Durante esta fase inicial de 2000 a 2005 proporcionaron agregación de registros básicos a través de diferentes tipos de sistemas junto con técnicas básicas de correlación de eventos. Estos sistemas se basaron solo en ataques de amenazas conocidas para detectar un ataque. Por lo tanto, fueron completamente incapaces de lidiar con los ataques de día cero en los sistemas de una organización. Otras limitaciones de los sistemas durante este período incluyeron:

1. Los sistemas iniciales se diseñaron sobre la base de direcciones IP, en lugar de usuarios. Con la asignación dinámica de direcciones IP y el rápido aumento en la cantidad de dispositivos móviles, correlacionar un dispositivo por su dirección IP es efectivamente inútil para una empresa, ya que una sola dirección IP se asigna a varios dispositivos en un día.
2. Los sistemas tradicionales usaban métodos basados en reglas para establecer una correlación entre varios eventos de seguridad. Por lo tanto, actualizar cientos de reglas en tiempo real no solo consume tiempo, sino que también da como resultado una utilización inadecuada de los recursos.
3. Dado que existe un sistema de correlación de eventos basado en reglas, tienden a generar una gran cantidad de eventos falsos positivos.
4. Abrumados por el número de falsos positivos así generados, los analistas podrían ignorar los eventos positivos verdaderos. Además, un enfoque basado en reglas es un enfoque retrospectivo e. ocurre una situación y luego se crean reglas para evitar que la misma situación vuelva a suceder.

Además, otros factores que jugaron un papel pertinente en la ineficiencia de estos sistemas incluyen la subestimación de costos, la falta de familiarización con los requisitos de infraestructura y las limitaciones de las bases de datos relacionales.

Los SIEM se desarrollaron inicialmente debido a la incapacidad del departamento de TI de una organización para lidiar con una gran cantidad de alertas generadas por IDS e IPS. Como vimos en la última sección, pasó a incluir capacidades de administración de registros agregando información de firewalls y otros dispositivos, además de asumir el rol de una plataforma de información en el transcurso de los próximos diez años.

Junto con la incorporación de las técnicas tradicionales de seguridad de la información, los SIEM han incluido técnicas avanzadas como el análisis del comportamiento del usuario y la inspección profunda de paquetes. User Behavior Analytics, o UBA, se centra en el análisis de datos y credenciales de usuario orientados al usuario. Los algoritmos utilizados en UBA se basan en el aprendizaje automático y, por lo tanto, trabajan en el modelo predictivo.

Los algoritmos de aprendizaje automático han aumentado la eficiencia de los SIEM al reemplazar los algoritmos basados en reglas. Muchos proveedores han desarrollado herramientas UBA para complementar los sistemas SIEM tradicionales, mientras que los proveedores que desarrollan nuevas herramientas SIEM incluyen SIEM como una herramienta incorporada.

Deep Packet Inspection es una aplicación de UBA que analiza datos a nivel de paquete para articular el comportamiento del usuario. Esta articulación no solo se limita a una sola computadora, sino que también incluye teléfonos móviles y tabletas.

La evolución constante de la tecnología en los países desarrollado como en los en vías de desarrollo ha llevado a las empresas de diferentes índoles a invertir y tener una base tecnológica para subsistir, competir en el mercado y la realización de las actividades de la organización de manera eficaz , no obstante conjunto a la evolución de las TIC trajo consigo

el riesgo de que los sistemas, hardware y los usuarios sean objeto de ataques cibernético, lo que ha obligado a muchas instituciones a invertir en equipos, herramientas y capacitación de seguridad informática para poder combatir y mitigar cualquier eventos no deseado. Pero además ha obligado a los países a crear convenios y leyes para combatir el cibercrimen.

Budapest es uno convenios internacionales que obliga a los países que formen parte él mismo a crear organizaciones para combatir el cibercrimen y leyes que obliguen a las empresas en especial financiera a implementar sistemas de seguridad para tener control de todo lo eventos que puedan ocurrir en su infraestructura y redes.

Budapest se firmó el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004, en la ciudad de Budapest, República de Hungría. Es el primer tratado internacional el cual fue creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. A la fecha, Budapest ha sido ratificado por 60 Estados, junto a los Estados miembros de la Unión Europea, el Convenio ha sido ratificado por países no europeos, entre ellos Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina, Colombia.

Luego de este convenio la República Dominicana creó varios proyecto en materia de tecnología para poder cumplir con lo reafirmado en el convenio de Budapest dentro de los proyecto elaborado por el estado dominicano están la ley orgánica sobre protección de datos de carácter personal, ley sobre crímenes y delitos de alta tecnología, ley que regula el envío de comunicaciones comerciales, publicitarias o promocionales no solicitadas, realizadas por vía correos electrónicos, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor (SPAM), El Departamento de Investigaciones de Crímenes y Delitos Alta Tecnología (DICAT), Centro Nacional de Ciberseguridad de

salvaguardar el ciberespacio dominicano, El Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria, etc.

Con el aumento de los complejos ataques de seguridad informática a nivel mundial, el 17 de mayo de 2021, el presidente de los Estados Unidos, Joseph Biden, firmó la Orden Ejecutiva 14028 Mejorando la Ciberseguridad de las Naciones. Esta Orden Ejecutiva exige la protección de endpoints, definiendo más los requisitos de registro, implementando el registro de auditoría de una manera unificada y mejorando las capacidades para proporcionar más información sobre las acciones del sistema y la cuenta.

Los registros de auditoría se identificaron en tres áreas técnicas separadas, todas relacionadas con la respuesta a incidentes y con el conocimiento de lo que está sucediendo en un sistema en un momento dado. Esta Orden Ejecutiva responde a un aumento en los ataques cibernéticos que utilizan ransomware para paralizar componentes de infraestructura críticos relacionados con la seguridad nacional y el público.

Mejorar los controles de seguridad de garantía de la información existentes como parte de un marco de gestión de riesgos es un mecanismo adecuado para forzar el cumplimiento y justificar la financiación en función de estos requisitos presidenciales.

Con los Marcos de Gestión de Riesgos (RMF) que se están implementando en todo el mundo en casi todos los sectores de la industria, la auditoría y el monitoreo son elementos centrales del aseguramiento y la seguridad de la información.

El personal de garantía de la información, los ingenieros de ciberseguridad y los analistas pueden utilizar la información de registro para realizar funciones críticas de seguridad en tiempo real.

Nos obstante al número de delitos cibernéticos la unión europea creó en año 2016 primer sistema nacional que obligue a los Estados miembros a identificar mejor, responder y reportar incidentes de ataques cibernéticos, dar a las autoridades el poder para auditar programas,

imponer sanciones y dar a los investigadores más alternativas para recopilar y compartir información sobre los patrones de ataque más amplios.

Con este sistema la unión europea fuerza a las diferentes entidades al tener visibilidad de todos los eventos dentro de una organización en ámbito de sus sistema, infraestructura y redes de datos.

2.1.1 Aplicaciones Similares.

En la actualidad existen un sin número de sistemas de Gestión de Eventos e Información de Seguridad, los cuales tienen el objetivo de combinar la gestión de la seguridad de la información con la gestión de eventos de seguridad, para responder a las amenazas de ciberseguridad. Lo que diferencia a cada sistema son las formas de procesar los datos, la correlación de los logs, el rendimiento, si es código abierto o privado, la construcción e implementación de la solución, entre otras características.

Algunos de los más importante dentro del rango de nuestra solución son:

2.1.1.1 OSSIM (Open-Source Security Information Management).

Es un SIEM desarrollado por Dominique Karg y Julio Casal en el año 2000, que implementa la detección y prevención de intrusiones, y la seguridad de redes en general. Este sistema funciona a partir de múltiples herramientas populares de monitoreo y seguridad de código abierto (Open Source), como Nagios, Snort, y otros, gracias a lo cual ofrece grandes capacidades y un alto rendimiento, creando así una inteligencia que traduce, analiza y organiza los datos de una forma única que la mayoría de los sistemas SIEM no pueden conseguir, resultando en un diseño que gestiona, organiza y observa riesgos que los administradores pueden apreciar.

2.1.1.2 Sagan log analysis engine.

Sagan es un motor de correlación y análisis de registros en tiempo real de código abierto (GNU / GPLv2) de alto rendimiento. Está escrito en C y utiliza una arquitectura de subprocesos múltiples para ofrecer un análisis de eventos y registros de alto rendimiento. La estructura de Sagan y las reglas de Sagan funcionan de manera similar al motor IDS " Snort " de Sourcefire. (Quadrant, 2019)

2.2 Base Teórica

2.2.1 Elasticsearch, Logstash y Kibana (ELK).

Es un conjunto de herramientas de gran potencial de código abierto que se combinan para crear una herramienta de administración de registros permitiendo la monitorización, consolidación y análisis de logs generados en múltiples servidores. ELK permite buscar, analizar y visualizar los datos con mayor facilidad. También puede manejar eficientemente gran cantidad de datos gracias a su escalabilidad. (Losada, 2018).

2.2.2 Beats.

Son agentes de datos ligeros, los cuales podremos utilizar para recopilar cierto tipo de información y que tras su transformación y enriquecimiento podremos por ejemplo insertarla en Logstash o Elasticsearch.

2.2.3 SIEM.

Un sistema de gestión de eventos e información de seguridad o SIEM (en inglés, Security Information and Event Management) es una tecnología que puede detectar y responder rápidamente las amenazas informáticas. (Berjano, 2020).

2.2.4 Características de sistemas SIEM.

De Pico Barrera, F. M. (2016). Con el avance de la tecnología los sistemas SIEM han evolucionado de manera exponencial básicamente en identificación de eventos reales y en aspectos de interfaz, logrando observar que la mayor cantidad de estos sistemas muestran interfaces gráficas o interfaces web en donde consolidan todos sus servicios, así como sus principales herramientas. Entre las características más comunes y básicas se citan:

- Control de direccionamiento IP.
- Acceso centralizado y administración de logs.
- Cumplimiento normativo de TI.
- Correlación de eventos.
- Respuesta activa del servidor (seguridad y monitoreo local).
- Seguridad de endpoint y escaneo de equipos.

2.2.5 Acceso centralizado y administración de logs.

De Pico Barrera, F. M. (2016). Una solución de SIEM tiene la cualidad de centralizar todos los procesos que se encuentran disponibles para lograr obtener su cometido, adicional la administración de logs empieza con la configuración de equipos que se integrarán al mismo dentro de un sistema de tecnologías de la información, particularmente los nodos más importantes o críticos, para enviar la información relevante y eventos de aplicaciones (logs) a una base de datos centralizada y administrada por la aplicación SIEM. La base de datos de la aplicación SIEM primero analiza y normaliza los datos enviados por los numerosos y muy rápidos nodos existentes dentro de un sistema de tecnologías de la información.

2.2.6 Logs.

Los logs nos ayudan a detectar y analizar los errores y problemas relativos a eventos de red y de sistemas, por ejemplo, incidentes de seguridad, actividades irregulares o problemas operacionales. También nos permiten conocer mejor a los usuarios: ver los hábitos de navegación, qué franja horaria es la más demandada a la hora de conectarse, desde dónde acceden a webs y cuánto tiempo permanecen navegando, entre otras cosas.

2.2.7 Cumplimiento normativo de TI.

De Pico Barrera, F. M. (2016). Una vez que todos los eventos sean registrados en el sistema, es factible aplicar filtros o reglas para actividades de auditoría, evaluación de cumplimiento o identificación de violaciones de los requerimientos básicos. Las normas exigidas a los logs de los sistemas por lo general requieren la frecuencia de los cambios de contraseñas, identificación de sistemas operativos, errores de aplicaciones que no se puedan instalar y auditorías de antivirus y antispyware.

2.2.8 Correlación de eventos.

De Pico Barrera, F. M. (2016). La correlación de eventos permite aportar al sistema SIEM con un nivel de inteligencia mayor debido a que no muestra únicamente los eventos sino también la posibilidad de reaccionar o no a dicha acción, fundamentándose en varias condiciones una vez ejecutadas las alarmas. El motor de correlación de los sistemas SIEM está diseñado para investigar y considerar eventos existentes dentro de una base de datos dispuesta para este fin

2.2.9 Respuesta activa (monitoreo y seguridad).

De Pico Barrera, F. M. (2016). Esta característica permite tomar medidas como respuesta a incidentes suscitados dentro del servidor, eventos que pueden afectar al sistema y por consiguiente traer resultados inesperados. La configuración del sistema de seguridad para que responda de manera adecuada es recomendado que posee herramientas eficientes pero ligeras, pues ayudará a que las actividades del servidor no colapsen, ya que puede suceder que el sistema se encuentre respondiendo a falsos positivos o es posible que ejecutara una DoS hacia su propia red, lo cual implica un desperdicio en el uso de recursos, tanto hardware como software, dando la posibilidad de que la respuesta activa se convierta en el evento maligno dentro de la organización.

2.2.10 Amenazas

De Pico Barrera, F. M. (2016). Dentro de los sistemas SIEM es necesario saber que los eventos inusuales que se presenten son denominados amenazas, debido a que dan origen a distintos incidentes de seguridad.

2.2.10.1 Amenazas internas.

De Pico Barrera, F. M. (2016). La mayoría de las redes organizacionales invierten grandes cantidades de recursos para mejorar la seguridad externa de dichas entidades con el fin de evitar inconvenientes con ataques originados por terceros.

Este hecho da origen a que los diseñadores y administradores de redes descuiden la seguridad interna, pensando tener el control y sin tomar en cuenta que las amenazas internas pueden ser mayores a las externas, incluso alcanzando entre el 50% y 90% del total de amenazas existentes.

Se debe discurrir que los ataques internos son una amenaza real y deben ser considerados en los programas de seguridad de organizaciones, permitiendo establecer políticas institucionales de seguridad al momento de implementar redes informáticas.

2.2.10.2 Amenazas externas.

De Pico Barrera, F. M. (2016). En la actualidad las amenazas externas se han convertido en amenazas más fáciles de detectar y controlar, debido a que la gran mayoría de organizaciones implementan sistemas de seguridad apuntando hacia afuera de la organización, implicando un peligro latente las amenazas originadas en el interior de las organizaciones.

Las amenazas externas pueden ir desde un simple script que permita saber si el sistema es vulnerable o toda una estructura que permita violentar las seguridades organizacionales con el fin de tener acceso a información o bases de datos que faciliten la obtención de réditos económicos o reconocimiento social.

Las amenazas externas pueden ser manuales o automáticas, las manuales se presentan cuando algún individuo o atacante intenta acceder de manera sistemática y sutil en algún sistema, claro está que el proceso será lento y centrado. En cambio, las amenazas automáticas se presentan en forma de virus, gusanos o ataques de secuencia de comandos, dando origen a una tasa mayor de intentos fallidos.

2.2.11 Vulnerabilidades.

De Pico Barrera, F. M. (2016). Como vulnerabilidades son consideradas todas las debilidades de los sistemas o redes informáticas a través de las cuales los atacantes tienen acceso a la información. El sistema SIEM es el encargado de verificar y reportar dichas

vulnerabilidades ofreciendo al usuario la posibilidad de obtener eventos de seguridad o asignarle la responsabilidad de reconfigurar los equipos de red. (Fortinet, 2020).

2.2.12 Configuración errónea.

De Pico Barrera, F. M. (2016). Una configuración eficiente dentro de un sistema SIEM garantiza una eficiente seguridad en el desarrollo de la empresa, ya que de lo contrario es muy posible que las vulnerabilidades y falsos positivos dentro del sistema tengan una presencia mayoritaria lo cual puede incidir una posible sustracción de información.

Las configuraciones erróneas no siempre son intencionales, existen ocasiones en las que su origen provienen de accidentes o descuidos del administrador e incluso de pequeñas acciones laborales como por ejemplo desactivar o apagar un firewall, no iniciar algún servidor o personal no calificado en la manipulación de servidores o estaciones de trabajo. En muchos sistemas SIEM existe la posibilidad de gestionar las configuraciones y sistemas de verificación, los mismos que sirven para identificar e informar los cambios realizados sobre configuraciones específicas o cambios en archivos dentro de sistemas críticos.

2.2.13 Sistemas operativos.

De Pico Barrera, F. M. (2016). Son aplicaciones que permiten gestionar los componentes hardware del computador, mediante la interacción del usuario con el software del mismo computador. Es necesario resaltar que sin un sistema operativo un computador sería un equipo tecnológico inservible.

La elección del sistema operativo a instalar en un computador se fundamenta en el uso que se dé a dicho equipo, básicamente un equipo puede ser utilizado como servidor o simplemente como cliente.

En el mercado informático existen principalmente dos grandes alternativas de sistemas operativos: los sistemas operativos Windows y los sistemas operativos Linux, el primero tiene un uso específico, es decir puede ser utilizado solo como cliente o solo como servidor, claro está dependiendo de la versión de cada uno de los sistemas operativos Windows, ejemplo: Windows 10, Windows 7, Windows Server 2008, etc. En cambio, los sistemas operativo Linux tienen la posibilidad de interactuar como cliente o como servidor, esto debido a la robustez que poseen estos sistemas, entre las distribuciones más conocidas están, CentOS, RedHat, Ubuntu, Mint, etc.

Otro de los aspectos a tener en cuenta al momento de decidirse por un sistema operativo es el factor económico, pues los sistemas Windows son sistemas comerciales, los cuales tienen un costo económico que permite su instalación y uso, en cambio las distribuciones Linux pertenecen al grupo de software de código abierto o también conocido como software libre, sin querer interpretar que esto sea sinónimo de gratuidad, por ejemplo la distribución RedHat es una distro Linux que obligatoriamente requiere la adquisición de una licencia para su respectivo uso.

2.2.14 Software libre.

Según Stallman, R. (2004), “La tarea de enseñar a los nuevos usuarios el valor de la libertad se complicó especialmente en 1998, cuando parte de la comunidad decidió abandonar el término «software libre» y empezó a hablar de «software de código abierto»”

El objetivo de este cambio fue el de evitar la confusión entre los términos libre y gratuito, con la finalidad de convencer a los usuarios que era factible desarrollar software de código abierto de gran calidad y capacidad, pero sin embargo los dos términos citados hacen referencia a la misma categoría de software, pero implican aspectos muy distintos referentes al software y sus valores.

Según (Zazo, 2010), “El software libre y el software de código abierto, así como los movimientos que hay detrás de ambos, han pasado de ser fenómenos marginales para convertirse en los últimos años en herramientas muy conocidas y utilizadas por gran parte de la sociedad.”

Este tipo de software es muy importante en el desarrollo del software a nivel mundial, pues es muy común encontrar anuncios de software propietario sobre plataformas de software libre o software de código abierto.

Las aportaciones del software libre han sido el germen de un gran debate intelectual y social sobre nuevos modelos de regulación de los derechos de autor y la circulación del conocimiento; debate que, lejos de quedarse en presupuestos teóricos, ha dado sus frutos en numerosas propuestas ya implementadas y exitosas para la libre construcción y circulación del conocimiento, sobre todo a través de las tecnologías computacionales conectadas en red.

Es común encontrar comunidades detrás de cada producto de software libre, permitiendo una constante evolución tanto en desarrollo como en soporte, logrando alcanzar mejoras continuas en cada una de las aplicaciones desarrolladas.

2.2.14.1 Ventajas del software libre o software de código abierto.

- Acceso a software de alta calidad.
- Ahorro en el pago de licencias.
- Disponibilidad del código fuente para todo el mundo.
- Posibilidad de que entidades educativas puedan mejorar el código fuente.
- La desaparición de “dueños” de los sistemas o programas.
- La factibilidad de copiar parte del código de algún software.

2.2.14.2 Desventajas del software libre o software de código abierto.

- Al ser “gratuito” no contará con soporte técnico.
- La falta de publicidad para dar a conocer el software
- Pocos recursos económicos para invertir en publicidad ya que no tiene sentido publicitar productos “gratuitos”.
- Al ser de código abierto aumenta la posibilidad de ataques por alguna vulnerabilidad existente.

2.2.15 Fintech.

En un artículo leído en la biblioteca CRAI y publicado por la enciclopedia Salem indican que la tecnología financiera, o fintech, es un término utilizado para describir los avances tecnológicos y los cambios en la industria bancaria y financiera. Implica nuevas tecnologías, como aplicaciones para teléfonos inteligentes, e innovaciones, como la banca solo en la web y el crowdsourcing, que permiten a las personas realizar un seguimiento de su dinero de maneras que difieren de la banca tradicional.

2.2.15.1 Importancia de las Fintech.

Hoy en día las Fintech son unos de los sectores más importante en el sector financiero, estas empresas emergentes son el foco principal para lidiar con la demanda de clientes que tienen los bancos y la transformación digital en la banca.

El Fintech es una nueva área de la industria financiera que aprovecha la creación y el uso de las nuevas tecnologías para mejorar las actividades financieras: procesos, productos, gestión de la información, modelos de negocio…

2.2.15.2 Característica de las Fintech.

Según el portal: https://leasein.pe/caracteristicas-de-las-fintech/, indicas la siguientes:

1. Modelo de negocio centrado en la experiencia del usuario
2. Metodologías de trabajo ágiles
3. Constante innovación tecnológica
4. Priorizan la seguridad de sus usuarios
5. Construyen ecosistemas de alianzas

2.2.16 Inteligencia artificial (IA).

En un artículo investigado en el CRAI UNIBE y publicado por la enciclopedia Salem resume el término de la siguiente manera, la inteligencia artificial es el diseño, la implementación y el uso de programas, máquinas y sistemas que exhiben inteligencia humana, siendo sus actividades más importantes la representación del conocimiento, el razonamiento y el aprendizaje. La inteligencia artificial abarca una serie de subáreas importantes, que incluyen el reconocimiento de voz, la identificación de imágenes, el procesamiento del lenguaje natural, los sistemas expertos, las redes neuronales, la planificación, la robótica y los agentes inteligentes. Varios investigadores de inteligencia artificial han mejorado varias técnicas de programación importantes, incluida la búsqueda clásica, la búsqueda probabilística y la programación lógica.

2.2.17 API.

Una API es un conjunto de definiciones y protocolos que se utilizan para desarrollar e integrar el software de las aplicaciones. API significa interfaz de programación de aplicaciones.

Las API permiten que sus productos y servicios se comuniquen con otros, sin necesidad de saber cómo están implementados. Esto simplifica el desarrollo de las aplicaciones y permite ahorrar tiempo y dinero. Las API le otorgan flexibilidad; simplifican el diseño, la administración y el uso de las aplicaciones, y proporcionan oportunidades de innovación, lo cual es ideal al momento de diseñar herramientas y productos nuevos (o de gestionar los actuales) (Red Hat, 2019).

2.2.18 Datos.

Son información, valores que recibe el computador a través de distintos medios. Cifra, letra o palabra que se suministra a la computadora como entrada y la máquina almacena en un determinado formato. (Fortinet, 2020).

2.2.19 Antivirus / antimalware (AV/AM).

Proporciona protección contra Virus, spyware y otros tipos de ataques de malware en la web, el correo electrónico y el tráfico de transferencia de archivos. Responsable de detectar, eliminar e informar sobre códigos maliciosos. Al interceptar e inspeccionar el tráfico y el contenido basados en aplicaciones, la protección antivirus garantiza que las amenazas maliciosas ocultas dentro del contenido legítimo de la aplicación sean identificados y eliminados de los flujos de datos antes de que puedan causar daños. (Fortinet, 2020).

2.2.20 Bot/Botnet.

Es una red de computadoras privadas infectadas con software malicioso y controladas como grupo sin el conocimiento del propietario, y se utiliza para realizar un ataque DDoS, robar datos o enviar correo no deseado. El actor de amenazas que controla una botnet a veces se denomina "pastor de bots". (Fortinet, 2020).

2.2.21 Brecha de seguridad.

Es el momento en que un hacker explota con éxito una vulnerabilidad en una computadora o dispositivo, y obtiene acceso a sus archivos y red. (Fortinet, 2020).

2.2.22 Ataque distribuido de denegación de servicio (DDoS).

La orquestación sistemática de un gran número de sistemas comprometidos que se extienden por Internet, cada uno de los cuales genera una red rápidamente solicitudes a un sistema de destino. Esta gran cantidad de solicitudes congestiona al servidor de destino, lo que resulta en incapacidad del servidor para responder a solicitudes legítimas. (Fortinet, 2020).

2.2.23 Firewall.

Es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico según un conjunto definido de reglas de seguridad. (Fortinet, 2020).

2.2.24 Ingeniería social.

Es el arte de manipular a las personas para obtener información confidencial o hacer que ellos hagan algo de lo cual no tenían la intención. (Fortinet, 2020).

2.2.25 Red privada virtual (VPN).

Es una herramienta que extiende una red privada a través de una red pública y permite a los usuarios enviar y recibir datos a través de redes públicas o compartidas como si los dispositivos estuvieran conectados directamente a la red privada. (Fortinet, 2020).

2.2.26 Malware.

Es un software malicioso que daña un sistema informático. Los tipos de malware incluyen gusanos, virus, troyanos, spyware, adware y ransomware. (Fortinet, 2020).

2.2.27 Virus.

Es un tipo de malware destinado a corromper, borrar o modificar información en una computadora antes de difundir a otros. (Fortinet, 2020).

2.2.28 Filtrado web.

Ofrece la opción de permitir explícitamente sitios web o pasar tráfico web sin inspeccionar tanto hacia como desde sitios web conocidos para acelerar los flujos de tráfico. Permite una amplia variedad de acciones para inspeccionar, calificar y controlar tráfico web perimetral a nivel granular. (Fortinet, 2020).

2.2.29 Gusano.

Es una forma de malware auto replicante, auto propagable y autónoma que utiliza redes mecanismos para extenderse a otros sistemas. Generalmente, el daño causado por un gusano es indirecto y debido a las actividades de replicación y distribución del gusano que consumen todos los recursos del sistema. El gusano se puede utilizar para depositar otras formas de malware en cada sistema que encuentre. (Fortinet, 2020).

2.2.30 IPS.

En resumen, un sistema de prevención de intrusiones (IPS), también conocido como sistema de prevención de detección de intrusiones (IDPS), es una tecnología que monitorea

una red para detectar cualquier actividad maliciosa que intente explotar una vulnerabilidad conocida.

2.2.31 Dirección IP.

De Pico Barrera, F. M. (2016). Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

2.2.32 Objetivos de la seguridad.

El autor Álvaro Gómez, en su obra Enciclopedia de la Seguridad Informática, define el concepto de seguridad informática como: “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.”

La seguridad de la información busca salvaguardar los datos o información de una organización, evitando que la misma sea sustraída para fines ilícitos o desaparecida. Además, busca que en una empresa haya integridad, disponibilidad y confiabilidad.

2.2.32.1 Confidencialidad.

Según el blog ceupe.com, es la capacidad de garantizar que la información solamente va a estar disponible para aquellas personas autorizadas, es decir, que personas ajenas no podrán acceder a la información e interpretación.

2.2.32.2 Integridad.

Según el blog ceupe.com, es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. Esta función es muy importante cuando, por ejemplo, estamos realizando trámites bancarios por Internet.

2.2.32.3 Disponibilidad.

Según el blog ceupe.com, es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles para el usuario en todo momento.

2.2.33 Normas ISO 27001.

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

2.2.34 Monitoreo de redes.

Según el autor Antoni Martí, el monitoreo de la red o la monitorización se define como el conjunto de actividades que, por medio de la identificación y detección de posibles problemas, hace posible la evaluación del desempeño y la disponibilidad de la red.

2.3 Base Legal.

2.3.1 Ley de Ciberseguridad de la República Dominicana.

El 23 de abril de 2007 se promulgó en República Dominicana la ley 53-07 sobre crímenes y delitos de alta tecnología. El objetivo de dicha ley es la protección integral de los sistemas

que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en dicha ley.

La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de estos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de estos, son todos bienes jurídicos protegidos. (Dominicana.Gob.do, 2021).

El Departamento de Investigaciones de Crímenes y Delitos Alta Tecnología (DICAT), forma parte de la Policía Científica y su objetivo es combatir el crimen de alta tecnología dentro de la República Dominicana. (Dominicana.Gob.do, 2021).

2.3.2 Ley 310-14, ley que regula el envío de correos electrónicos comerciales no solicitados (spam).

En noviembre del 2014 se promulgó la Ley 310-14 que regula el envío de comunicaciones comerciales, publicitarias o promocionales no solicitadas, realizadas vía correos electrónicos, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor (SPAM).

La seguridad informática o seguridad TIC es el área de las TIC que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta. La privacidad puede ser definida

como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse confidencial. (Dominicana.Gob.do, 2021).

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiendo, por ejemplo, en información privilegiada. (Dominicana.Gob.do, 2021).

2.3.3 El Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria.

Aunado a lo anterior, consideramos importante destacar que las autoridades de una de las infraestructuras críticas del Estado dominicano, concretamente del sistema monetario y financiero de la nación, ha dictado un cuadro normativo específico para atender los asuntos de ciberseguridad.

La Junta Monetaria aprobó en fecha 1 de noviembre de 2018, mediante la Resolución JM 181101-02, el Reglamento de Seguridad Cibernética y de la Información (el Reglamento).

Este Reglamento fue dictado “en consonancia con los esfuerzos realizados por el Estado dominicano para fortalecer las capacidades nacionales en esa materia, conforme las disposiciones establecidas en el Decreto No. 258-16 que crea el Programa de República Digital, de fecha 16 de septiembre del 2016 y, el Decreto No. 230-18 que define y regula la Estrategia Nacional de Ciberseguridad 2018-2021, de fecha 19 de junio de 2019” y como una “respuesta a los incidentes de seguridad cibernética acaecidos en los sistemas monetarios y financieros de otras economías del mundo, cuyos efectos y consecuencias han elevado la prioridad dad a este tema a nivel internacional.

Igualmente, debido a la digitalización e interconexión acelerada de todos los servicios y sistemas financieros, se requiere establecer mecanismos de protección de la información, que es su activo principal, para evitar acceso y uso ilegal de la misma, así como de la infraestructura tecnológica que soporta la operatividad de dichos servicios y sistemas". (acento.com.do, 2021).

Del Reglamento se pueden extraer varios tópicos muy importantes acorde con nuestro proyecto y empresa a implementar el piloto, por ejemplo:

1. El Reglamento contiene disposiciones de carácter vinculante (de obligatorio cumplimiento) no solo para las entidades de intermediación financiera (EIF´s) en general, sino también para las Administradoras de Sistemas de Pago y Liquidación de Valores; Participantes del Sistema de Pagos de la República Dominicana (SIPARD) autorizados por la Junta Monetaria; así como cualquier otro tipo de entidad del SIPARD, que la Junta Monetaria autoriza en el futuro y a las entidades de apoyo y servicios conexos vinculadas a la intermediación financiera, que funcionen "mediante el mantenimiento de una conexión electrónica o el intercambio de información esencial, a través de cualquier medio digital, en la medida en que dicha vinculación pueda comprometer los objetivos del SIPARD". Esto significa que las empresas tecnológico-financieras (o sea, empresas que aplican la tecnología en la prestación de facilidades, servicios y productos financieros), mejor conocidas como Fintech, que se desempeñen en el ámbito de los sistemas de pagos, tienen en este Reglamento disposiciones de obligatorio cumplimiento de gobernanza corporativa y de gestión de riesgos tecnológicos. Por lo que este Reglamento puede considerarse como uno de los primeros instrumentos de regulación especial de las Fintech en República Dominicana.

2. El riesgo tecnológico debe tratarse y evaluarse adecuadamente, o sea, que debe ser correctamente identificado, medido, gestionado y mitigado. El riesgo tecnológico es uno de los tantos elementos a tomar en consideración en la gestión integral de riesgos, por ende, se consideraría como una buena práctica de gobierno corporativo que en ocasión de grupos o conglomerados financieros, la implementación del Reglamento y, concretamente, el diseño y ejecución del Programa de Seguridad Cibernética y de la Información, así como de las políticas internas complementarias, se hagan de manera consolidada, que tengan alcance hacia todas las filiales y subsidiarias del grupo financiero de que se trate, bajo la supervisión de la casa matriz o holding. En adición, el artículo 14 del Reglamento indica que las entidades obligadas "deben procurar, de manera periódica, la gestión de riesgos tecnológicos a las entidades interconectadas con las que actualmente mantengan relación contractual" debiendo proceder a la "desconexión" cuando la evaluación de riesgo tecnológico realizada de un resultado no satisfactorio.

2.3.4 Protección de datos personales.

La Ley No. 172-13 tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. No. 10737 del 15 de diciembre de 2013.

La protección de datos personales es un derecho fundamental consagrado en el Art. 44.2 de la Constitución de la República Dominicana, texto que establece que: "Toda persona tiene derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley.

El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos." (Dominicana.Gob.do, 2020).

CAPÍTULO 3: Marco Metodológico

3.0 Introducción al capítulo

En este apartado vamos a presenciar el marco metodológico donde se exponen los aspectos de la metodología, técnicas, estrategias y procedimientos que implementaremos. en nuestra investigación de proyecto de grado.

Según Balestrini, el marco metodológico corresponde a una serie de secuencias lógicas que tiene como objetivo poner de manifiesto y sistematizar los procedimientos implícitos en el proceso de investigación (2006). De igual forma, a través de la investigación, permite descubrir y analizar patrones en los datos y reconstruirlos de una forma en la que se pueda mostrar de forma convencional.

Tamayo & Tamayo también definen el marco metodológico como un proceso que se basa en el método científico para poder descubrir informaciones relevantes que permitan verificar y aplicar diferentes conocimientos (2012). Se puede decir que estos conocimientos son adquiridos para poder relacionarlos con las hipótesis planteadas.

3.1 Tipo de investigación (metodología)

Para la elaboración de este proyecto el tipo de investigación apropiado es de tipo correlacional y explicativo, dado que el tema principal es la recolección de eventos de seguridad y su posterior escalamiento para brindar soluciones efectivas para mantener la integridad, la disponibilidad y la confidencialidad de la información en la Fintech GCS LTD.

La utilidad y el propósito principal de los estudios correlacionales-explicativos es saber cómo se puede comportar un concepto o variable, conociendo el comportamiento de otra u otras variables relacionadas, además de proporcionar un sentido de entendimiento del fenóme-no a que hacen referencia e indicar regularidades. Metodológicamente este tipo de estudio se recomienda para el análisis de un caso o de una situación con cierta intensidad en un período de tiempo corto. (Dra. Yudith Laura Ferreiro, 2014).

3.2 Método

Nuestra investigación estará enmarcada en función de una metodología mixta donde se hará uso del método cualitativa, basándose en los parámetros a ser considerados dentro de las actividades organizacionales a través de redes informáticas, no obstante, la metodología cuantitativa también formará parte de la investigación, aunque en menor porcentaje debido a que la fundamentación estadística es primordial para lograr obtener los resultados esperados.

En las últimas décadas, numerosos investigadores han apuntado a un método "mixto", que integra ambos enfoques, argumentando que al probar una teoría a través de dos métodos pueden obtenerse resultados más confiables. Este enfoque aún es polémico, pero su desarrollo ha sido importante en los últimos años (Hernández, Méndez y Mendoza, 2014).

3.3 Investigación Preliminar

Nuestra investigación, la cual tiene un enfoque mixto (cualitativo-cuantitativo) trabajaremos en la construcción e implementación de una solución de seguridad informática la cual tiene como objetivo proporcionar una visión global de la seguridad de las tecnologías de la información en un Fintech.

Esta herramienta ayudará a la organización en el cumplimiento del estándar PCI-DSS (Payment Card Industry – Data Security Standard) y en el reglamento de seguridad de la información de la junta monetaria, así como también a fortalecer la seguridad informática.

3.4 Delimitación del problema

Nuestro proyecto busca solventar la problemática que tienen las Fintech en la gestión de los eventos de seguridad, identificación de amenazas, análisis datos y respuesta a incidentes, para garantizar la disponibilidad y la confiabilidad de la empresa ante los clientes.

3.4.1 Área geográfica.

Este proyecto será realizado en la empresa Fintech GCS LTD, compañía especializada en tecnología de vanguardia para el procesamiento a gran escala de transacciones financieras. GCS LTD está ubicada en la torre Roble Corporate Center, Calle Rafael Augusto Sánchez #2, esquina Freddy Prestol, Piso 8, Piantini, Santo Domingo. RD.

3.4.2 Tiempo.

El tiempo propuesto para la realización de esta investigación, así como la ejecución del proyecto tardará cuatro (4) meses. Durante la mitad del primer mes se llevará a cabo el proceso de recolección de datos, la segunda mitad del primer mes y el segundo mes será utilizado para la creación del ambiente de la solución, construcción e implementación de nuestra herramienta, integración de los dispositivos críticos y parametrización y correlación de los eventos, el tercer mes será para la evaluación del funcionamiento de la misma, además la implementación de mejoras y correcciones de errores, si así es necesario, y en el transcurso del último mes será para la evaluación general y presentar las conclusiones de nuestro proyecto.

3.4.3 Población y muestra.

Nuestra principal población estará compuesta de empresas tecnológica-financieras (o sea, empresas que hacen uso la tecnología en la prestación de facilidades, servicios y productos financieros), estas conocidas como Fintech, que se desempeñen en el ámbito de los sistemas de pagos, pero además abordaremos esas pequeñas y medianas que poseen una infraestructura tecnológica con equipos críticos y que hagan uso de una red de datos para el desarrollo de sus actividades.

3.4.4 Técnicas e Instrumentos.

Rojas Soriano, (1996-197) señala al referirse a las técnicas e instrumentos para recopilar información como la de campo, lo siguiente:

Que el volumen y el tipo de información-cualitativa y cuantitativa- que se recaben en el trabajo de campo deben estar plenamente justificados por los objetivos e hipótesis de la investigación, o de lo contrario se corre el riesgo de recopilar datos de poca o ninguna utilidad para efectuar un análisis adecuado del problema.

En opinión de Rodríguez Peñuelas, (2008:10) las técnicas son los medios empleados para recolectar información, entre las que destacan la observación, cuestionario, entrevistas, encuestas.

En nuestra investigación estaremos utilizando los siguientes instrumentos de recolección de datos:

- Cuestionario a través de encuestas. Este instrumento nos permitirá obtener un modelo en el ámbito de seguridad institucional centrándonos en estructuras propias del cuestionario.

- Utilizaremos el método de observación directa, con este instrumento el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar.

La observación: permitirá ser un testigo directo en el accionar de las actividades y procedimientos informáticos dentro de las Fintech.

Por último, es imprescindible usar la entrevista como fuente de obtención de información. La entrevista se define como “una conversación que se propone con un fin determinado distinto al simple hecho de conversar”. Es un instrumento técnico de gran utilidad en la investigación cualitativa, para recabar datos. (Laura Díaz-Bravo, 2013).

Entrevista: permitirá conseguir el criterio y pensamiento de las personas relacionadas en el proceso de administración y control de las seguridades en cada una de las entidades.

3.4.5 Técnica de procesamiento de análisis de datos.

Según Hernández, Fernández, Baptista, Pilar (2006) El procesamiento de los datos se refiere a todo el proceso que sigue un investigador desde la recolección de datos, hasta la presentación de estos en forma resumida. Tiene básicamente tres etapas: recolección y entrada, procesamiento y presentación.

En este espacio se mostrará el medio que se utilizará para registrar la información obtenida. Debido al tiempo propuesto para realizar el proyecto y la población para la recolección de información, se emplea el método mixto (cualitativo y cuantitativo) el cual se basa en la observación de la estructura de la empresa y el alcance de los procesos relacionados con seguridad de la información.

Para procesar la información cuantitativa se utilizará encuestas a un grupo determinado de habitantes a través de formularios en línea. Luego estos datos serán procesados para obtener la información correspondiente necesaria.

3.4.6 Fuentes de datos.

Como fuente de datos principal para esta investigación se tomarán en cuenta la respuesta y retroalimentación suministrada por el personal de seguridad informática de la empresa donde se implementará en piloto de nuestro proyecto, como además los diferentes analistas del centro de operaciones de seguridad (SOC).

CAPÍTULO 4: Plan de mercadeo y Análisis del entorno

4.0 Introducción al capítulo

En el presente capítulo vamos a presentar los aspectos de mercadeo y análisis del entorno de nuestro proyecto con la finalidad de que el mismo se convierta en una solución para solventar una problemática a esas organizaciones que no cumple con los recursos para obtener una herramienta de cumplimiento y monitoreo.

4.1 Benchmarking

Benchmarking es un análisis estratégico profundo de las mejores prácticas llevadas a cabo por empresas del mismo segmento que el tuyo. Benchmarking viene de la palabra de origen inglés "benchmarking", que significa referencia, y es una herramienta de gestión esencial para el perfeccionamiento de procesos, productos y servicios. Consiste en evaluar y analizar los procesos, productos, servicios y aspectos de otras compañías o áreas para compararlos y tomarlos como punto de referencia para tus futuras estrategias. (Oliveira. 2017).

La intención es aprender de otros proyectos para mejorar la idea propia que se está llevando a cabo.

4.2 Mecanismo para poblar información al sistema

Hoy en día se encuentran diversos sistemas de Gestión de Eventos de Seguridad, los cuales tienen como meta informar sobre las anomalías encontradas en los equipos tecnológicos para su análisis, y así dar respuesta ante filtraciones en la red corporativa. Lo que distingue al JH Collected Event Detector es la forma de procesar los datos, la correlación de los logs, y la construcción e implementación de la solución.

4.3 Modelo de negocio (Método Canvas)

El modelo canvas es la herramienta para analizar y crear modelos de negocio de forma simplificada. Se visualiza de manera global en un lienzo dividido en los principales aspectos que involucran al negocio y gira en torno a la propuesta de valor que se ofrece. El modelo canvas se utiliza para pasar de idea a proyecto y plasmar nuestra idea en un modelo empresarial. (Carazo. 2017).

Figura No. 5 Plantilla Modelo de Negocio CANVAS

4.4 Presupuesto

Tabla No. 2

Presupuesto de desarrollo e implementación de un sistema de gestión de eventos e información de seguridad para la empresa GCS LTD.

Actividades	Horas trabajadas	Costos de trabajo USD	Otro USD	Total USD	Comentario
Consultoría GCS LTD.	40	$6,000.00	$500.00	$6,500.00	Los SIEM requieren consultoría para la implementación. Y, para algunos de los SIEM y "alternativas" de SIEM más complejos la consultoría es necesaria para la personalización básica.
Diagramación de Red de la entidad	24	$5,600.00	$0.00	$5,600.00	Para la contrucción del sistemas es necesario conocer la estructura de red de la entidad.
Identificación y descripción de los dispositivos a monitorizar, GCS LDT.	20	$5,600.00	$0.00	$5,600.00	Es importante conocer la catidad de dispositivo que reportaran al SIEM y que tipo de dipositivos.
Subtotal	---	---	---	**$17,700.00**	---
Combinación componente ELK para contruir el SIEM.	160	$15,000.00	$0.00	$15,000.00	Nuestra solución estará sobre la base de ELK.
Mano de obra para administrar, modificar los datos, Configuración y Parseo de Datos.	200	$20,000.00	$0.00	$20,000.00	Muchos SIEM no cuentan con bases de datos autoadministradas, lo que significa que son necesarios administradores de bases de datos con gran talento para configurar el funcionamiento básico del sistema. Además, el manejo ineficiente de los datos puede requerir un ajuste constante de los datos que salen y entran. (Solarwinds, 2021)
Creación de tablero de datos UI	80	$5,600.00	$0.00	$5,600.00	En un sistema SIEM los tableros muestran los diferentes resultado obtenido de forma grafica y amigable.
Subtotal	---	---	---	**$40,600.00**	---
Almacenamineto de Datos.	120	$10,000.00	$0.00	$10,000.00	Una función básica de un SIEM es almacenar datos de registro y eventos para fines de archivo y análisis histórico. Según la velocidad de compresión y el método utilizado, los costos de almacenamiento pueden administrarse, o bien, dispararse sin control.
Servicio de Respaldo Y Backup de Datos.	100	$5,000.00	$0.00	$5,000.00	Tener un Backup es parte primordial cuando se trata de sistema y tecnología.
Subtotal	---	---	---	**$15,000.00**	---
Soporte Técnico.	8	$5,800.00	$0.00	$5,800.00	El soporte es parte de la del cumplimiento en una organización
Mantenimiento y Update	2	$360.00	$0.00	$360.00	Las actualizaciones y mantenimiento son eneciales en la seguridad informática.
Capacitación Analista GCS	40	$6,000.00	$600.00	$6,600.00	Es necesario dotar de conocimiento a las personas y equipos que estaran acargo de la herramienta para sacar el mejor de los prevecho de la saolución.
Subtotal	---	---	---	**$12,760.00**	---
Total	---	---	---	**$86,060.00**	

Nota. Esta tabla muestra un pronóstico sobre el presupuesto y las actividades a realiza en la implementación de nuestra herramienta.

4.5 Retorno de la Inversión

Nuestro proyecto es sin fines de lucro, se hará uso de nuestra herramienta para solventar una problemática en el departamento de seguridad, esto busca brindar conocimientos situacionales continuos, informes de cumplimiento automatizados, respaldo con el proceso de respuesta ante incidentes mediante el análisis de la causa raíz y servir como plataforma de investigación.

$$ROI = \frac{Ingresos - Egresos}{Egresos} * 100$$

Donde el ROI es igual a la diferencia entre los ingresos y egresos divididos entre los egresos.

Para realizar este cálculo vamos a simular montos ficticios debido a que se investigó sobre la ganancia que obtiene la empresa en sus operaciones como Fintech y esté datos es confidencial por política de la organización. Es necesario recordar que como Fintech y empresa certificada por la junta monetaria y estándar PCI-DSS es obligatorio la implementación de un sistema de manejo de eventos de seguridad para poder operar y la empresa no sea multada o deje operar.

Tabla No. 3

Representación Retorno de Inversión de la herramienta.

Ingreso Netos de Inversión	Gato Neto (Egresos)	**ROI**
$892,857.143	$125,000.00	**714186%**

Nota. Fuente: Elaborado por los sustentantes

CAPÍTULO 5: Análisis, presentación de resultados y Conclusiones

5.0 Introducción al Capítulo

Este capítulo tiene como propósito el análisis de la recolección datos dentro de la empresa, como también la entrevista realizada al personal de la organización donde implementaremos nuestro piloto. Por otra parte, se recapitulan los objetivos generales, objetivos especifico, conclusiones e hipótesis planteada en nuestro proyecto.

5.1 Encuesta

La encuesta es un instrumento de investigación que nos permite alcanzar información valiosa, la misma está orientada a obtener datos de las personas con el fin de que las respuestas sean utilizadas para el proyecto o investigación. Con la finalidad de “obtener información que se pueda analizar, extraer modelos y hacer comparaciones” (López & Fachelli, 2015).

La encuesta se estructuró en dos apartados. En el primero se realizaron preguntas a los analistas de seguridad de la información, administradores de sistema, operadores SOC y NOC, gerentes de seguridad y TI, como además al área de riesgo y cumplimiento, la misma haciendo referencia al conocimiento que presentan los empleados sobre la empresa GCS LTD y su puesto de trabajo. El segundo apartado se ocupó de los aspectos de la solución a crear e implementar en GCS LTD.

Los resultados de esta pueden ser visualizados en el Apéndice A.

5.1.1 APARTADO #1

5.1.1.1 ¿Sabes usted lo que es una FINTECH?

- SI
- NO
- TALVEZ

Con esta interrogante buscamos validar si los empleados tienen conocimiento del tipo de empresa en la que laboran.

5.1.1.2 ¿Conoces el propósito de una FINTECH?

- SI
- NO
- TALVEZ

Con esta interrogante buscamos saber si los empleados saben el propósito del tipo de empresa en la que trabajan y los posibles riesgos informáticos.

5.1.1.3 En qué área de GCS LTD labora.

- SOC
- NOC
- TI
- SEGURIDAD

Está interrogante busca identificar a que área pertenece cada colaborador.

5.1.1.4 Que puesto representa dentro de la empresa GCS LTD.

- OFICIAL DE MONITOREO NOC
- OFICIAL DE MONITOREO SOC
- ANALISTA DE CIBERSEGURIDAD DE LA INFORMACIÓN
- GERENTE SEGURIDAD
- GERENTE TI
- ADMINISTRADORES DE SISTEMAS
- RIESGO Y CUMPLIMIENTO

Con esta interrogante buscamos saber que puesto representa cada trabajador encuestado dentro de la empresa GCS LTD.

5.1.1.5 ¿Sabe usted cuales son los diferentes riesgos de seguridad de la información que enfrenta GCS LTD?

- SI
- NO
- TALVEZ

Con esta interrogante buscamos saber si cada colaborador encuestado tiene conocimiento de los riesgos de seguridad informática que presenta la empresa.

5.1.2 APARTADO #2

5.1.2.1 ¿Conoce usted lo que es un SIEM y cuál es su utilidad?

- SI
- NO
- POCO

Con esta interrogante buscamos validar si cada encuestado tiene conocimiento de lo que es una solución de manejo de eventos de seguridad SIEM.

5.1.2.2 ¿Con que frecuencia se detectan eventos de seguridad dentro de la infraestructura de TI de GCS LTD?

- POCO
- SIEMPRE
- NUNCA
- N/A

Con esta interrogante buscamos validar la frecuencia con la se detectan eventos anómalos de seguridad informático dentro de empresa.

5.1.2.3 ¿En su opinión cuales servicios generan la mayor cantidad de eventos de seguridad de la información?

- SERVICIO WEB
- BASE DE DATOS
- CORREOS ELECTRONICOS
- EQUIPOS DE COMUNICACIÓN DE DATOS
- SERVIDORES DE DOMINIOS

- OTROS
- N/A

Con esta interrogante buscamos identificar según la opinión del colaborador cuales servicios y equipos de tecnología son lo que mayores eventos de seguridad generan.

5.1.2.4 ¿Cree usted que se realiza un monitoreo adecuado de los equipos de comunicación, equipos finales, servidores críticos de TI y consolas de seguridad de la información?

- SI
- NO
- TALVEZ

Con esta interrogante buscamos saber si el monitoreo actual en la empresa es eficaz.

5.1.2.5 ¿Piensa usted que el análisis de los eventos de seguridad y la data para un reporte de incidentes es conciso y rápido?

- SI
- NO
- TALVEZ

Con esta interrogante buscamos validar que tan ágil es analizar las alertas generadas por los equipos y servicio de la empresa y la creación de los reportes.

5.1.2.6 ¿Cree usted que es necesario utilizar un SIEM en la Empresa GCS LTD?

- SI
- NO
- TALVEZ

Con esta interrogante buscamos validar si es de interés la estructuración e implementación de un sistema de gestión de eventos de seguridad en la empresa GCS LTD.

5.2 Entrevistas

Según Martínez (2010), la entrevista adopta la forma de un diálogo coloquial o entrevista semiestructurada, complementada con otras técnicas y de acuerdo con la naturaleza específica de la investigación que se va a realizar, de las cuales, podrán derivarse categorías de análisis no preestablecidas, las mismas pueden emerger en la medida en que se analizan los resultados.

Asimismo, indica que la entrevista es un instrumento técnico que tiene gran sintonía epistemológica con el enfoque cualitativo y también su teoría metodológica (p.99). La entrevista está basada en recopilar información de una manera detallada oral y personalizada, la cual está enfocada en obtener datos precisos y relevantes.

Una entrevista conlleva una planificación competente para una implementación exitosa. Esta requiere un estudio preliminar basado en el programa de trabajo y se necesitan algunas informaciones y documentos para formular su transformación. Durante la realización de esta investigación, se entrevistó al Ing. Victor Cordero, Gerente en Riesgo Cibernético y Comunicaciones en GCS LTD, el cual facilitó información crucial sobre la estructura tecnológica y de seguridad informática de la empresa, como además el funcionamiento de las operaciones, el mismo se dispuso a aceptar la estructuración e implementación de la solución

de seguridad SIEM, basada en ELK y así aprovechar lo beneficio que traerá la misma a la empresa.

Unas la de parte más importante es que mediante el reglamento de ciberseguridad del banco central de la república dominicana obliga a toda entidad con fine financiero y que forman parte su ecosistema a implementar soluciones seguridad para el monitoreo y reporte a incidente de sus infraestructuras de TI.

El mismo nos informa que es de suma importancia contar con una solución de manejo de evento de seguridad, tanto para la parte de cumplimiento, como para tener una mejor visión de todo lo que pasa en nuestra red de datos y equipos de comunicación como servicios.

5.3 Resultados de la Hipótesis planteada

Mediante la recolección de eventos e información de seguridad de los equipos tecnológicos de una organización, se reducirá el riesgo de taques cibernético, aportará capacidad de respuesta en tiempo real, contribuyendo a la disponibilidad de los servicios de la empresa.

Según nuestra hipótesis planteada y de acuerdo los resultados de la entrevista, recolección de datos y nuestro prototipo implementado quedo evidenciado que la hipótesis planteada se cumple, esto se puede confirmar en el capítulo 6 y en el apéndice A.

5.4 Verificación y evaluación de Objetivos

5.4.1 Verificación Objetivo General.

Demostrar que una solución de Gestión de Eventos e información de Seguridad, eficientiza la detección de patrones de ataques e identifica las vulnerabilidades potenciales, protegiendo a las empresas y a sus clientes de devastadoras filtraciones de datos, además de validar la salubridad de los equipos críticos de TI.

Para el cumplimiento de este objetivo realizamos la implementación de ELK como SIEM en la infraestructura de GCS LTD, para hacer el monitoreo de los principales equipos críticos que soportan la organización a nivel de TI, el mismo con el fin de tener una visualización de nuestra red de datos y detectar cualquier evento no deseado dentro de la organización. Para validar este objetivo general pueden consultar el capítulo 6 de este documento y el apéndice A.

5.4.2 Verificación Objetivo Específicos.

Replanteando los objetivos iniciales:

1. **Desarrollar e implementar de manera efectiva el sistema de gestión de eventos y seguridad de la información, para monitorear los servidores, equipos de comunicaciones y soluciones de seguridad informática críticos en GCS Systems.** Este objetivo puede ser verificado en el capítulo 6.
2. **Realizar una prueba piloto de nuestra herramienta en GCS Systems, empresa especializada en procesamiento a gran escala de transacciones financieras.** Este objetivo puede ser verificado en el capítulo 6.
3. **Combinar el stack ELK (Elasticsearch, Logstash y Kibana), como un SIEM.** Este objetivo puede ser verificado en el capítulo 6.
4. **Demostrar que es posible implementar ELK como SIEM para detectar, analizar y responder a las diferentes amenazas cambiantes.** Este objetivo puede ser verificado en el capítulo 6.

5.4.3 Repuestas a las preguntas de investigación.

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad, identificar eventos con patrones fraudulentos?

Si, se pueden identificar, en el prototipo implementado se validaron intento de autenticación fraudulento, ver capítulo 6.

¿Puedes un Sistemas de Gestión de Eventos e Información de Seguridad mantenerse al tanto de toda la información sobre seguridad en tiempo real?

Si, se pudo validar que este sistema analiza y muestra los reporte en tiempo real, en el mismo se validó las negociaciones de VPN site to site, ver capítulo 6.

¿Permite un Sistemas de Gestión de Eventos e Información de Seguridad general reporte del número de eventos fraudulentos analizado y detectado en una organización?

Si, el mismo se pudo validar en el capítulo 6.

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad detectar, analizar y responder amenazas cambiantes?

Esta pregunta no se pudo comprobar debido a que no visualizamos amenazas cambiantes, pero según las fuentes nuestra solución cuenta con IA que ayuda al aprendizaje.

¿Permite un Sistemas de Gestión de Eventos e Información de Seguridad gestionar potenciales vulnerabilidades de forma proactiva?

No se pudo comprobar debido que no se obtuvimos una vulnerabilidad en el nuestro desarrollo.

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad evitar devastadoras violaciones de datos causadas tanto por agentes de riesgo internos como por amenazas externas?

Esta pregunta no se pudo validar debido a que no analizaron eventos de violaciones de datos, pero si se validaron intentos de login de usuario no permitidos.

¿Puede un Sistemas de Gestión de Eventos e Información de Seguridad elaborar una respuesta rápida a los impactos y amenazas de seguridad previamente desconocidas?

Esta pregunta no se validó contra una amenaza desconocida, pero si pudimos ver que con amenazas ya conocida se pudo elaborar una respuesta rápida.

5.5 Conclusiones

A lo largo de esta investigación hemos podido corroborar que implementar una solución de manejo de ventos y seguridad informática es un activo valioso para las empresas con bases tecnológica y operaciones financieras.

Al realizar las encuestas y las entrevistas quedó en evidencia la importancia de tener una solución SIEM en una Fintech o empresa dedicada al área financiera, el mismo permite tener un control de todo lo que sucede dentro de una infraestructura de TI, además de darle continuidad al negocio y cumplir con las regulaciones impuesta para poder operar.

5.6 Líneas Futuras de Investigación

Durante la recolección de datos para este proyecto fue posible validar otro aspecto que no tocamos y que se pueden profundizar y dar seguimiento como es la integración de un Sandboxing o aislamiento de proceso dentro de la misma solución.

Otro punto importante es la integración de SDN o redes definidas por software dentro de la misma solución para automatizar y administra los equipos y servicio que están integrado en nuestro SIEM.

CAPÍTULO 6: Análisis y Diseño del Prototipo

6.0 Introducción al capítulo

El presente capitulo tiene como propósito mostrar los aspectos técnicos de nuestro proyecto de grado, donde se muestra un análisis del prototipo a crear como piloto en la Fintech GCS LTD.

6.1 Narrativa General

6.1.1 Objetivos de la Institución, Empresa o Sector al que está dirigido el Proyecto.

El objetivo de GCS LTD es proveer el más alto nivel de cuidado del medio ambiente a través de la conservación, la responsabilidad social, el uso sostenible, la educación, la honestidad y la sobriedad. Busca continuamente el diseño y desarrollo de productos y servicios tecnológicos optimizando procesos para cumplir requerimientos y necesidades de nuestros clientes de manera segura, ágil, y confiable, logrando la eficacia del Sistema de Calidad. GCS se enfoca está orientado al cumplimiento de los objetivos estratégicos manteniendo a un personal comprometido con la máxima satisfacción del cliente y gestionando el liderazgo del mercado local e internacional. (GCS.2019).

6.1.2 Breve descripción del sistema propuesto.

JH Collected Event Detector es un sistema que tiene como función recopilar, analizar y correlacionar datos, con la capacidad de brindar detección de amenazas y capacidades de respuesta a incidentes. A medida que las amenazas cibernéticas se vuelven más sofisticadas, se necesitan análisis de seguridad y monitoreo en tiempo real para una rápida detección y corrección de ataques. Es por eso por lo que, JH Collected Event Detector proporciona las capacidades necesarias de monitoreo y respuesta, mientras que nuestro componente de servidor proporciona la inteligencia de seguridad y realiza análisis de datos.

6.1.3 Objetivos del sistema o proyecto.

- Prevención de amenazas, vulnerabilidades del software, tales como malware, o la denegación del servicio.
- Controlar las amenazas cibernética.
- Centralizar la vista de potenciales amenazas.
- Determinar qué amenazas requieren resolución y cuáles son solamente ruido.
- Escalar temas a los analistas de Seguridad apropiados, para que puedan tomar una acción rápida.
- Documentar, en un registro de auditoría, los eventos detectados y cómo fueron resueltos.
- Cumplir con las regulaciones de la industria en un formato de reporte sencillos externos e internos.

6.1.4 Innovaciones del sistema propuesto

El componente innovador que ofrecemos en esta propuesta es implementar de acuerdo al tipo negocio que representa la empresa GCS LTD, un sistema gestión de eventos y seguridad de la información basado en el stack ELK para brindad una visualización en tiempo real de todos los posibles eventos que puedan pasar dentro de la infraestructura tecnológica de la empresa y así poder mitigar y analizar cualquier evento fraudulento.

6.1.5 Ventajas y Beneficios.

Dentro de las ventajas y beneficios que posee esta solución de seguridad informática se pueden destacar las siguientes:

- La detección de amenazas previamente desconocidas.
- Una mayor velocidad a la hora de llevar a cabo la investigación de las alertas.

- La posibilidad de buscar amenazas en registros archivados.
- La monitorización de las actividades que se llevan a cabo dentro de la red.
- El sistema SIEM garantiza que las alertas lleguen a las personas adecuadas.
- Reduce los costes de la compañía.
- Restaurar configuraciones de ciberseguridad en caso de que se hayan cambiado por error.
- Control y protección de los ciberataques.

6.2 Análisis FODA del sistema propuesto.

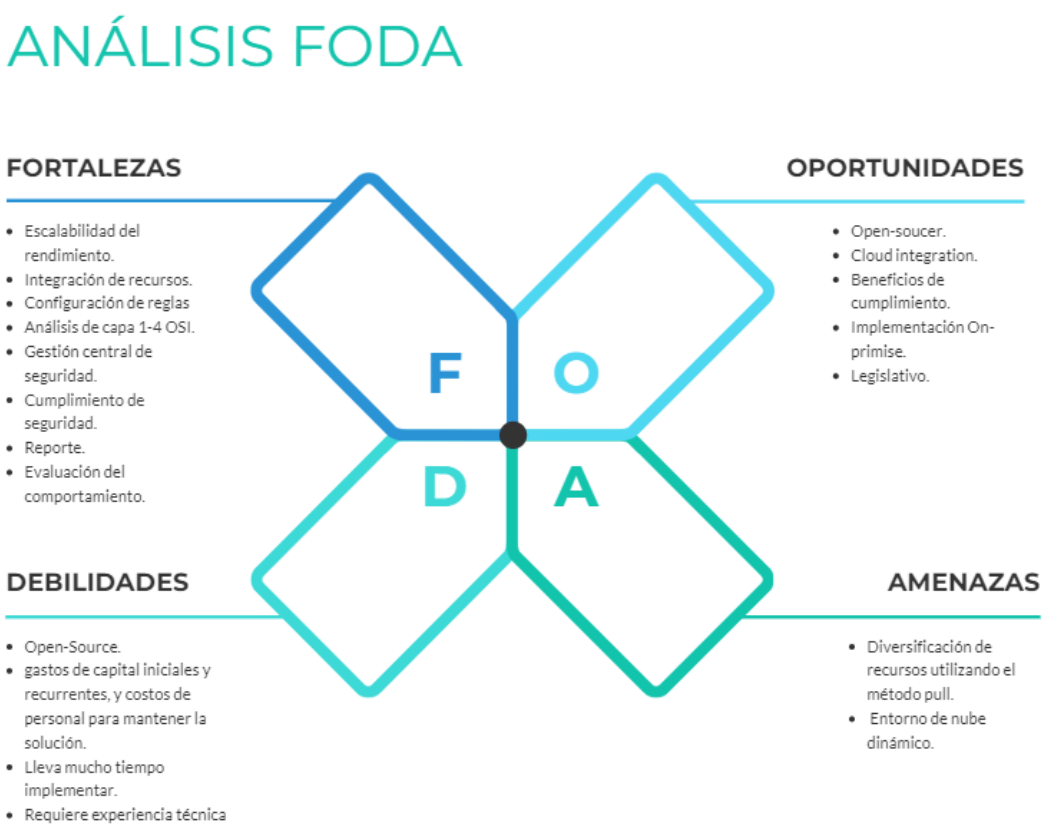


Figura No. 6 Análisis FODA. Fuente: elaborado por los sustentantes.

Diagrama de contexto del sistema:

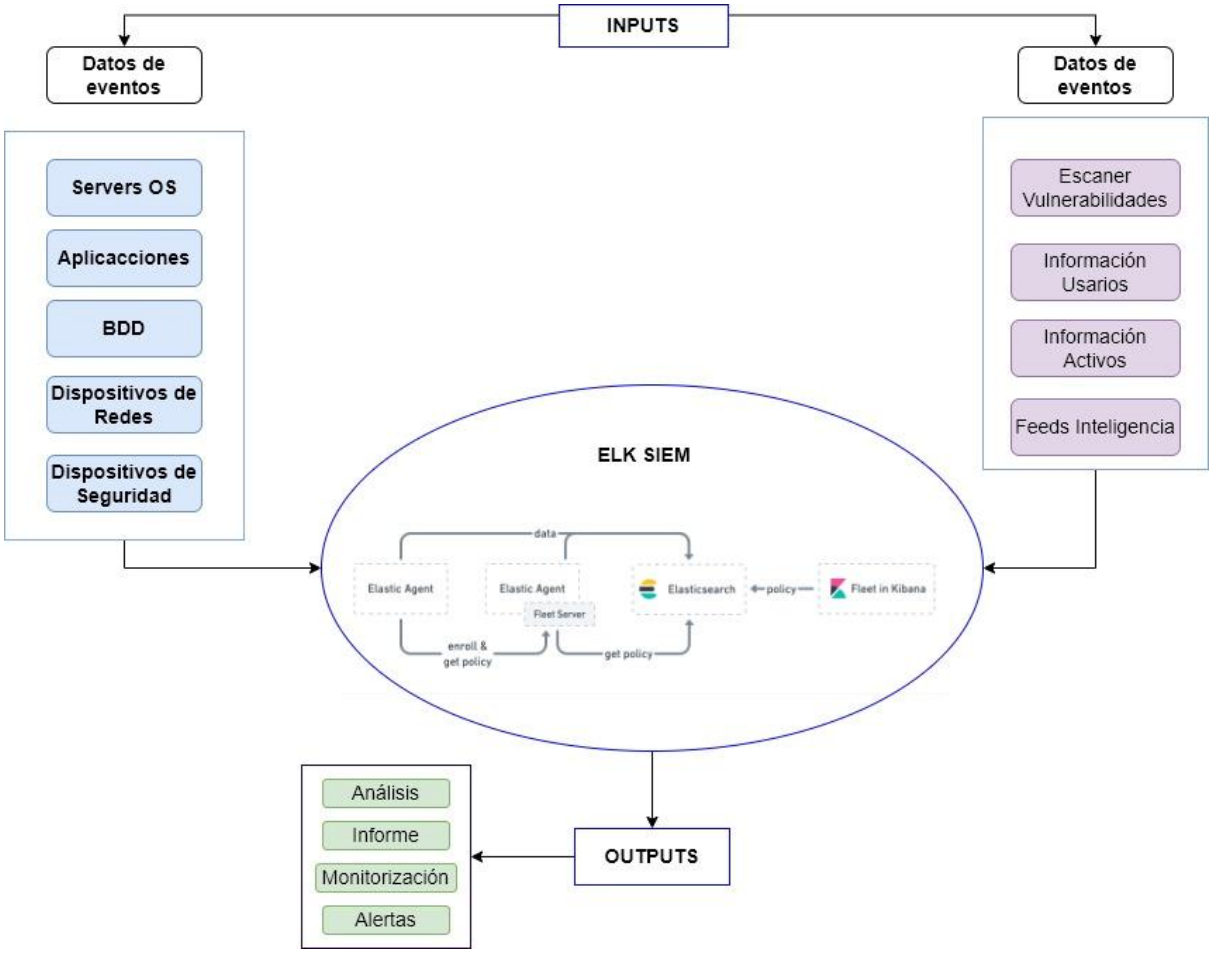


Figura No. 7 Diagrama de contexto del sistema. Fuente: Elaborado por los sustentantes.

6.3 Análisis funcional del sistema

La implementación de un sistema gestión de eventos y seguridad de la información cuenta varias funciones dentro de las cuales se destacan las siguientes funciones:

- Colección de Log
- Procesamiento de Log
- Almacenamiento
- Consulta de Log

- Visibilidad con el Uso de Dashboards
- Notificación de eventos
- Forense Informática

6.4 Diagramas de flujo de los procesos:

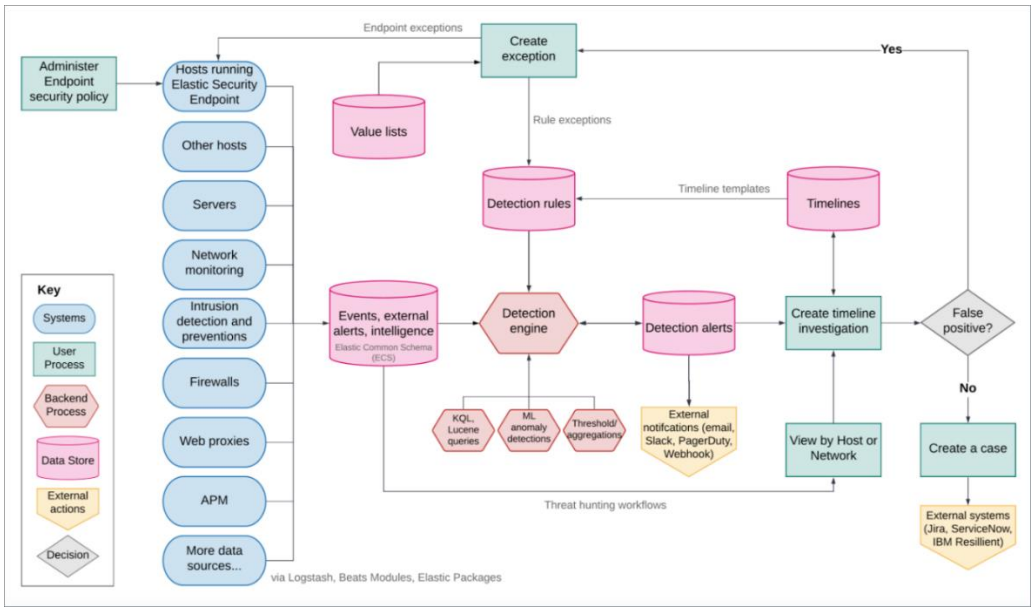


Figura No. 8 Diagrama de flujo de procesos ELK. Fuente: elastic (2022)

6.5 Diagrama de Flujo de Datos (DFD) del sistema propuesto:

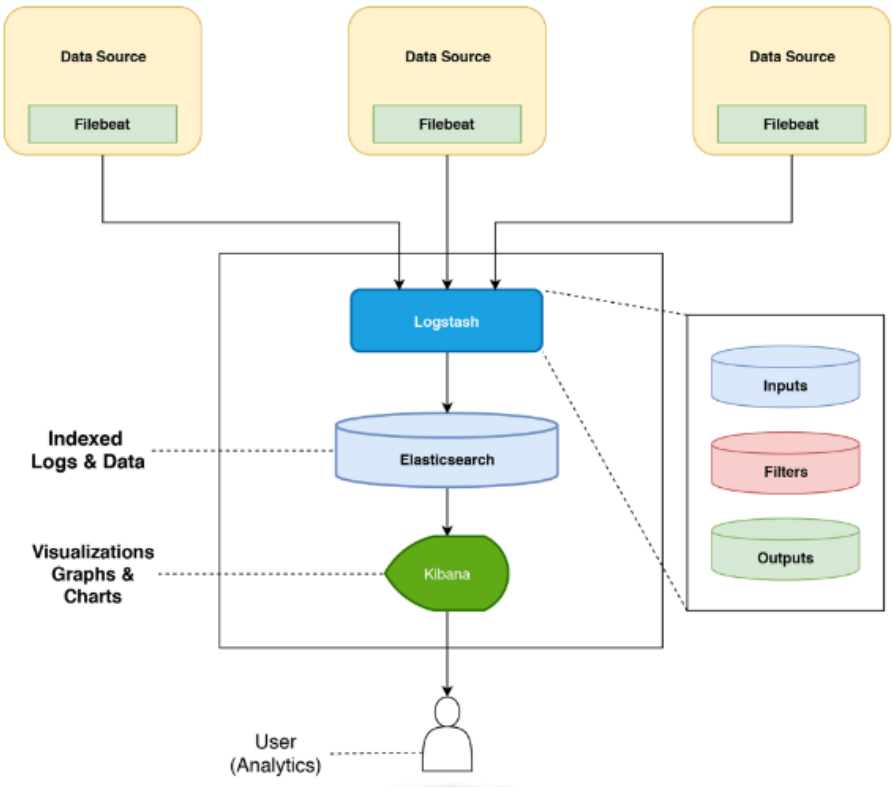


Figura No. 9 Diagrama de Flujo de Datos (DFD) ELK. Fuente: Technolush (2022)

6.6 Diseño de la Base de Datos

La base de datos de nuestra solución de SIEM está basada en Elasticsearch, esta es una base de datos distribuida que escala de manera dinámica de forma horizontal, por lo que a mayor demanda podemos ir creciendo en nodos. Llegando a poder almacenar petabytes de información.

Es una base de datos NoSQL orientada a documentos JSON, al estilo de MongoDB. Por lo cual no necesita que se definan esquemas a la hora de insertar los datos.

Elasticsearch se basa en los documentos JSON para poder realizar esta indexación. El documento JSON son un conjunto de pares clave/valor. Las claves son cadenas de texto y los valores pueden ser cadenas, números, fechas o listas.

Elasticsearch, al basarse en modelos NoSQL, almacena la información de forma desnormalizada. Es por ello que no se permiten hacer joins o subqueries

Elasticsearch se organiza mediante nodos, los cuales son alojados dentro de un cluster. Permite añadir nuevos nodos al cluster para poder acometer nuevas cargas.

6.6.1 Esquema de la base de datos.

Elasticsearch admite varios tipos de datos diferentes para los campos de un documento, incluidos tipos de datos básicos, complejos, geográficos y especializados.

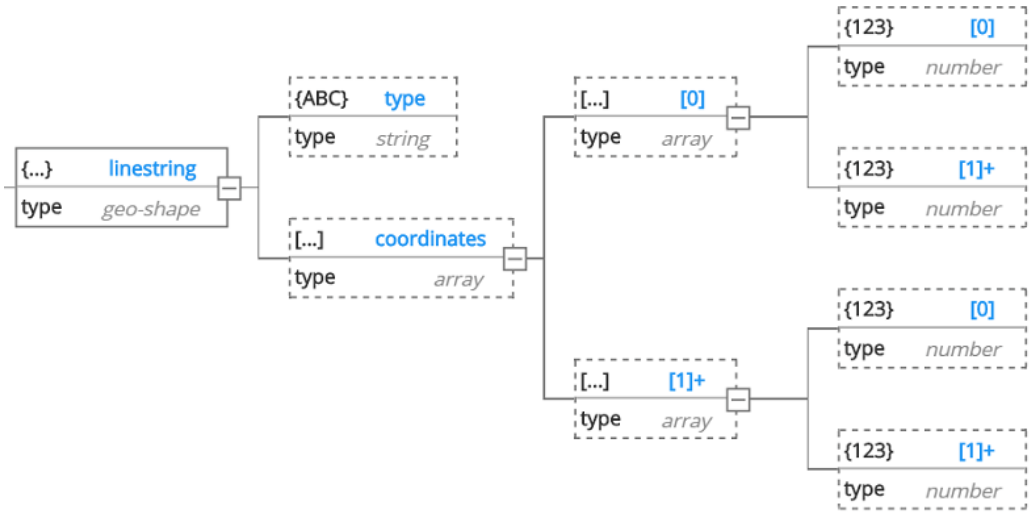


Figura No. 10 Esquema Elasticsearch. Fuente: Hackolade (2022)

6.6.2 Diagrama Entidad Relación (E-R).

En nuestra solución utilizaremos Elasticsearch como almacenamiento de datos y el mismo no utiliza un esquema E-R para el manejo las tablas y columnas, más bien utiliza index el cual definiremos a continuación.

Según el portal de elastic un índice es como una 'base de datos' en una base de datos relacional. Tiene un mapeo que define múltiples tipos.

Un índice es un espacio de nombres lógico que se asigna a uno o más fragmentos primarios y puede tener cero o más fragmentos de réplica.

Hay dos conceptos en esa definición. En primer lugar, un índice es algún tipo de mecanismo de organización de datos que permite al usuario particionar los datos de cierta forma. El segundo concepto se relaciona con réplicas y fragmentos, el mecanismo que usa Elasticsearch para distribuir datos alrededor del clúster.

- MySQL => Databases => Tables => Columns/Rows
- Elasticsearch => Indices => Types => Documents with Properties

Un clúster de Elasticsearch puede contener varios índices (bases de datos), que a su vez contienen varios tipos (tablas). Estos tipos contienen varios documentos (filas) y cada documento tiene propiedades (columnas).

6.6.3 Diccionario de datos del sistema.

Es necesario recordar que nuestra solución no utiliza una base datos E-R, la misma hace usos de índices por días, tamaños y equipos que están reportando hacia el agente elástico, estos índices son una estructura JSON la cual vamos mostrar la creada para nuestros quipos cisco asa hacer monitoreados y los capos más comunes.

Tabla No. 4

Campo esperado para los índex

Campo	Descripción	Tipo
@timestamp	Event timestamp.	date
cisco.asa.assigned_ip	The IP address assigned to a VPN client successfully connecting	ip
connection_type	The VPN connection type	keyword
cisco.asa.command_line_arguments	The command line arguments logged by the local audit log	keyword
cisco.asa.destination_interface	Destination interface for the flow or event.	Keyword
cisco.asa.mapped_destination_ip	The translated destination IP address.	ip
cisco.asa.mapped_source_ip	The translated source IP address.	ip
cisco.asa.mapped_source_port	The translated source ports.	long
cisco.asa.rule_name	Name of the Access Control List rule that matched this event.	keyword
cisco.asa.source_username	Name of the user that is the source for this event.	keyword
cisco.asa.tunnel_type	SA type (remote access or L2L)	keyword
client.ip	IP address of the client (IPv4 or IPv6).	ip
client.port	Port of the client.	long
client.user.name	Short name or login of the user.	keyword
destination.address	Some event destination addresses are defined ambiguously.	
destination.as.organization.name	Organization name.	keyword
destination.ip	IP address of the destination (IPv4 or IPv6).	ip
destination.nat.ip	Translated ip of destination-based NAT sessions	ip
destination.nat.port	Port the source session is translated to by NAT Device.	long
destination.port	Port of the destination.	long
error.message	error.message.	match_only_text
event.type	This is one of four ECS Categorization Fields, and indicates the third level in the ECS category hierarchy.	
host.ip	Host ip addresses.	ip
network.protocol	In the OSI Model this would be the Application Layer protocol.	keyword
network.protocol	In the OSI Model this would be the Application Layer protocol. For example, HTTP, DNS, or SSH. The field value must be normalized to lowercase for querying.	keyword
related user	All the user names or other user identifiers seen on the event.	keyword

Nota. Fuente: Elaborado por los sustentantes.

6.7 Recolección de datos

Para fines de este proyecto, solo estaremos colectando los logs de los diferentes firewalls que administran las entradas y las salidas de todos los datos dentro de la Fintech.

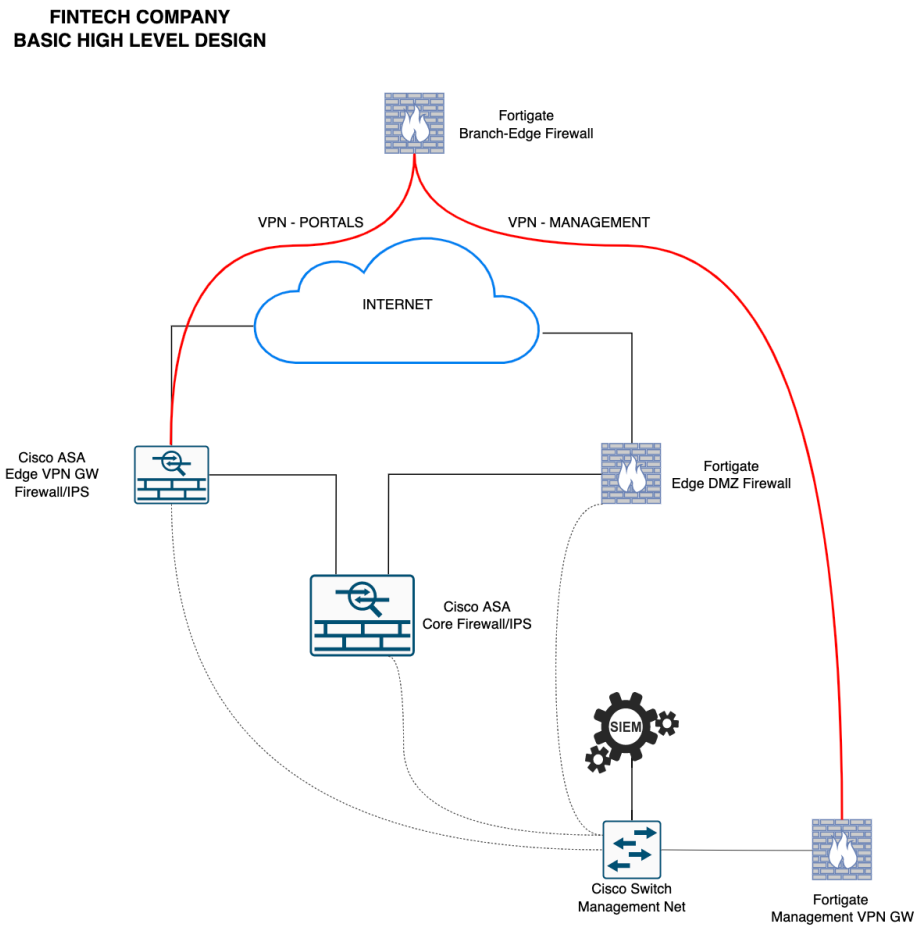


Figura No. 11 Recolección, Diagrama Solución. Fuente: elaborado por los sustentantes.

6.8 Formato de pantallas para las E/S de datos del sistema

A continuación, se muestran las pantallas de la solución SIEM, que será utilizada para el monitoreo de la infraestructura de TI en GCS LTD.

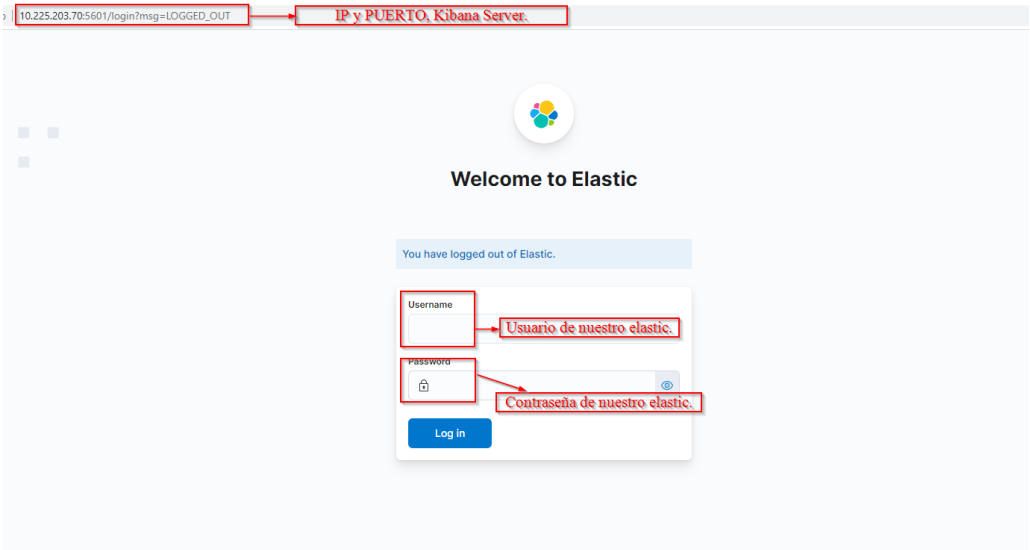


Figura No. 12 Pantalla login de nuestro SIEM

Aquí el analista de seguridad puede acceder de manera web a Kibana.

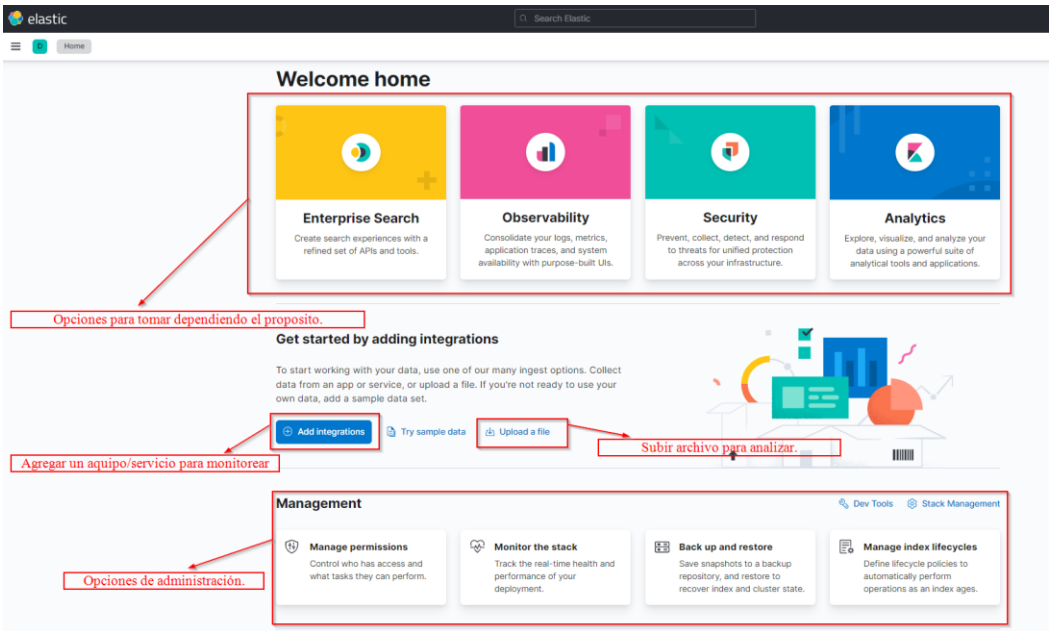


Figura No. 13 Pantalla de inicio luego de hacer acceder.

Aquí se puede navegar hacia nuestro propósito, si deseamos integrar algún equipo o servicio para monitorear, si queremos hacer algún análisis de un archivo de logs para validar algún patrón de fraudulento, entre otras opciones.

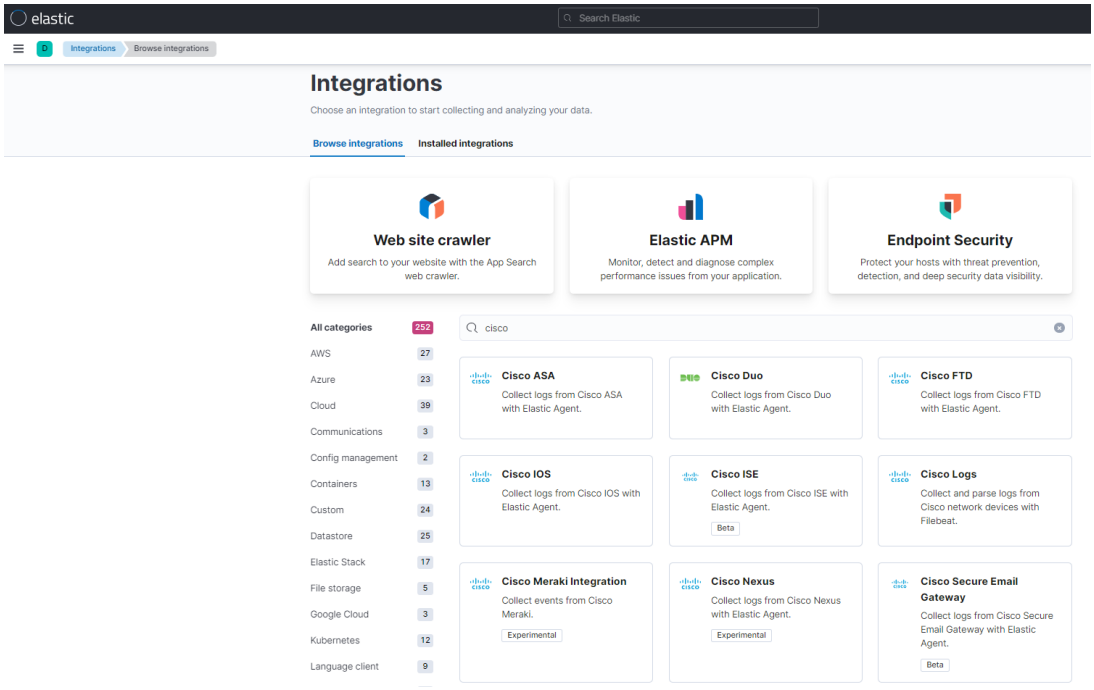


Figura No. 14 Plantilla de integración.

Aquí podemos buscar el vendor o servicio a integrar para monitorear.

Figura No. 15 Eventos recibidos de intentos de login SSH

Aquí estamos dentro de la opción de análisis donde descubrimos lo eventos y logs recibidos de los equipos que están reportando hacia nuestra solución, estos eventos están de acuerdo con la estructura JSON configurada y en su forma bruta lo cual se puede optimizar y correlacional para un mejor entendimiento.

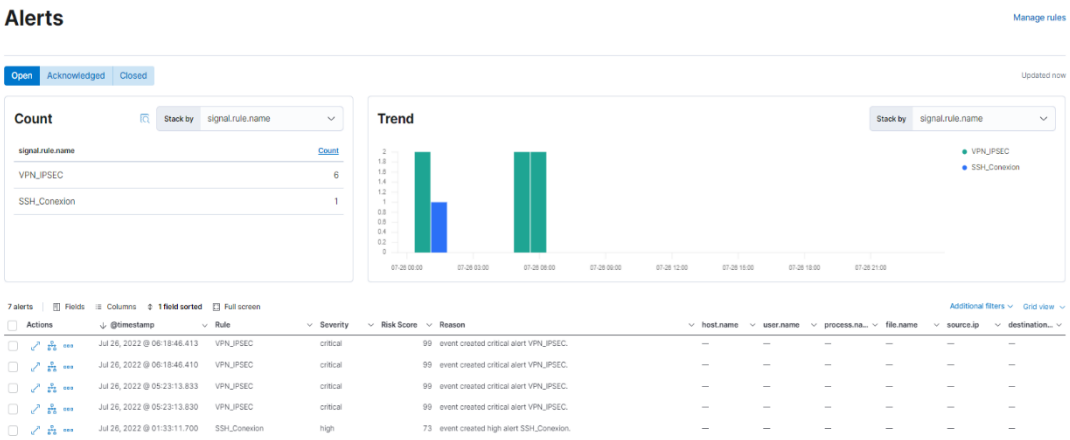


Figura No. 16 Alertas creadas de acuerdo a los eventos recibidos.

Aquí podemos ver algunas alertas creadas y correlacionadas de acuerdo con los logs recibidos de los equipos que están integrado a nuestra solución, estas alertas son búsquedas basada en criterios, las mostradas son intento de conexión SSH y servicio de VPN site to site sobre IPSec fallido.

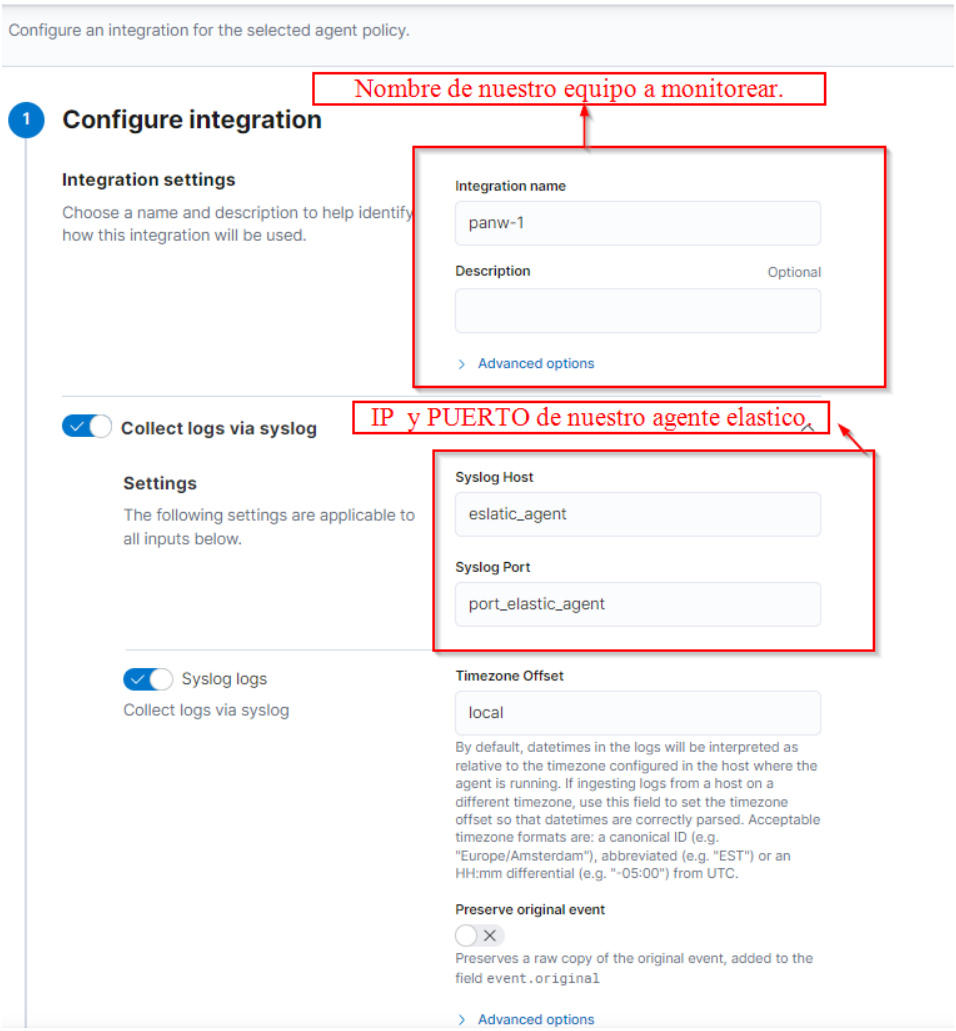


Figura No. 17 Integración de un equipo a monitorear.

Aquí podemos configurar un dispositivo para recibir los eventos y poder crear las políticas y alertas, en el mismo se coloca la dirección IP y puerto de nuestro agente que estará recibiendo los logs.

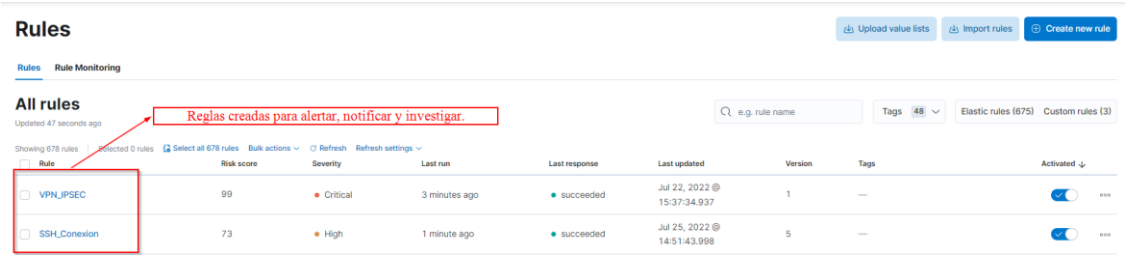


Figura No. 18 Creación de reglas.

Aquí podemos visualizar la creación de reglas para eventos críticos y que requieren investigación.

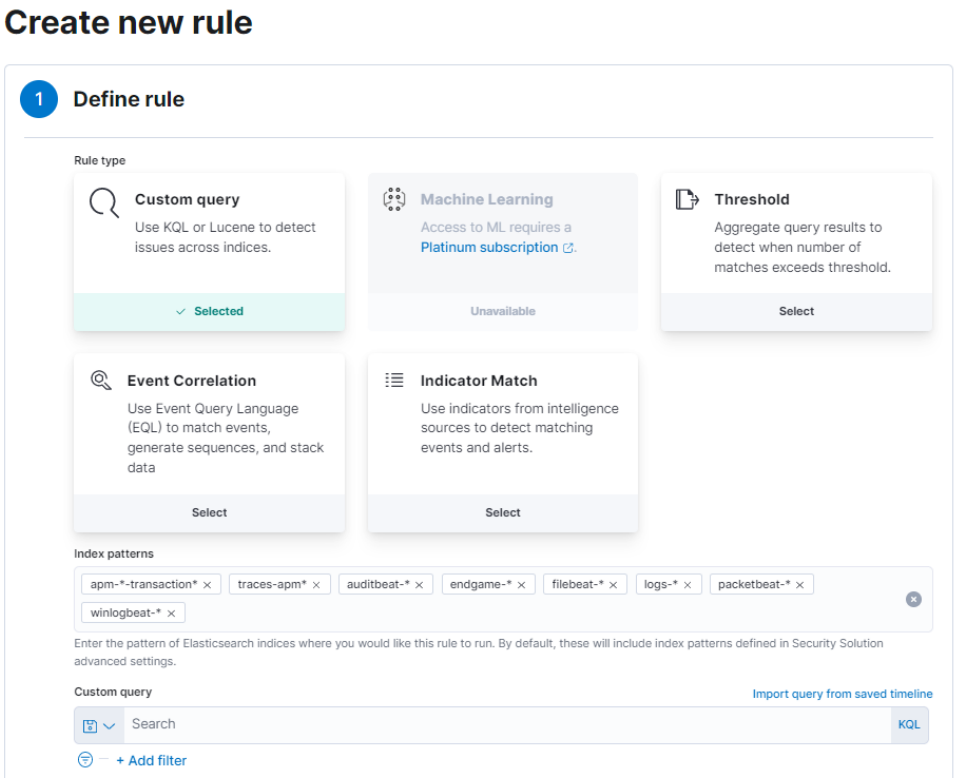


Figura No. 19 Opciones para definir políticas.

Aquí podemos ver las opciones para crear nuestras reglas.

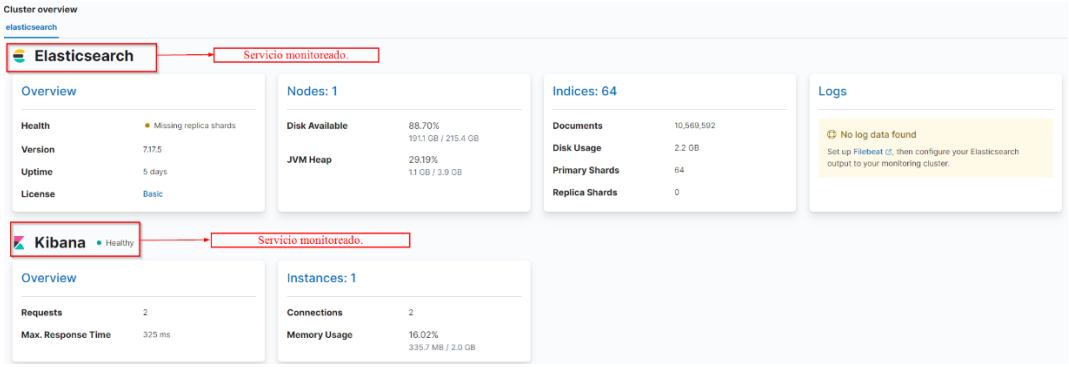


Figura No. 20 Monitoreo de servicios.

Aquí podemos ver como se visualiza un servicio o server, para ver cómo están sus recursos.

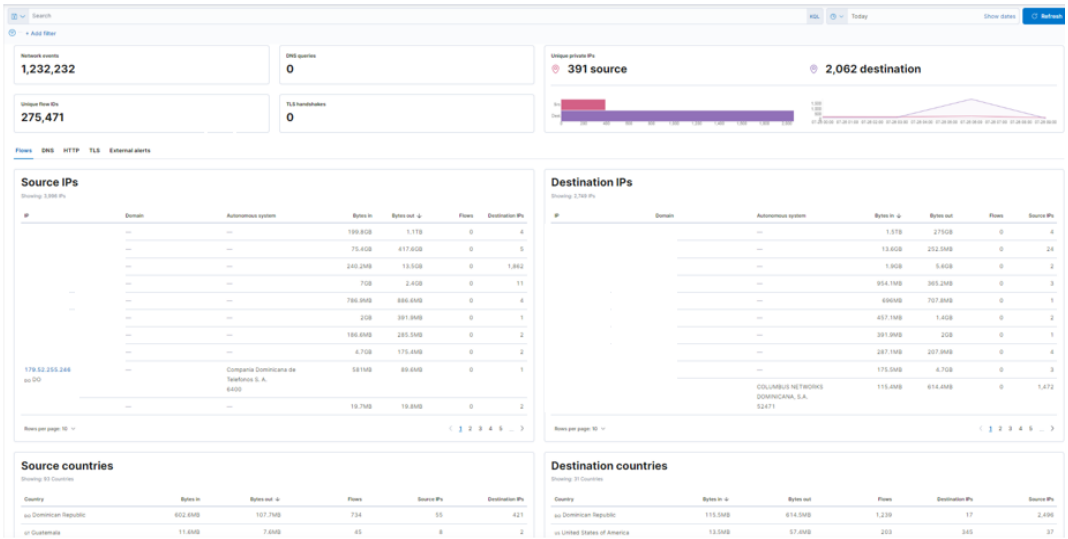


Figura No. 21 Flujo de nuestra red de datos.

Aquí podemos ver una pizarra del flujo de nuestra red de datos, como interactúan las direcciones IP.

6.9 Diagrama jerárquico de programas y/o menús principales

En esta sección estaremos presentando el diagrama jerárquico de la solución EKL que está compuesto por los siguientes elementos vistos a continuación.

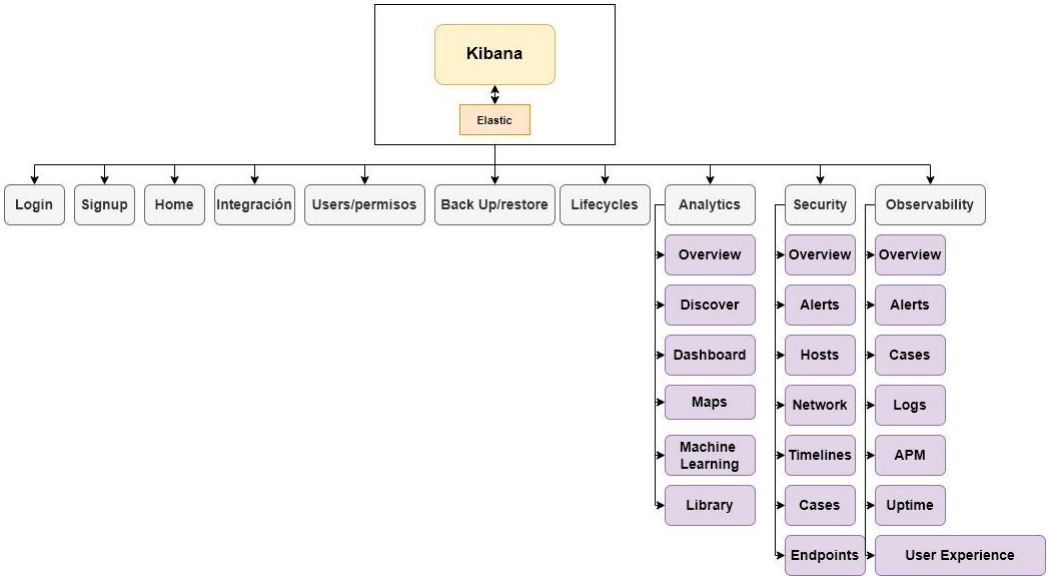


Figura No. 22 Diagrama jerárquico. Fuente: Elaborado por los sustentantes.

6.10 Seguridad y Control

6.10.1 Políticas de acceso seguridad.

Nuestra solución SIEM Elastic Stack cuenta con característica de seguridad para dar acceso adecuado a las personas correcta, esto permite gestionar usuarios bien intencionados y mantener alejados los actores maliciosos.

Las funciones de seguridad de Elastic Stack le permiten proteger fácilmente un clúster. Con la seguridad, puede proteger sus datos con contraseña e implementar medidas de seguridad más avanzadas, como el cifrado de comunicaciones, el control de acceso basado en roles, el filtrado de IP y la auditoría.

6.10.2 Políticas de Backup sugeridas.

Nuestra solución proporciona una función de instantánea que puede usar para hacer una copia de seguridad de sus datos.

ElastichSearch permite hacer copias de seguridad sobre distintos soportes: Discos, Amazon S3, etc.

En nuestro caso estamos realizando back up diarios hacia un repositorio local y también validando la posibilidad de hacerlo en una nube privada.

6.10.3 Descripción mecanismos de seguridad del sistema.

El Elastic Stack se compone de muchas partes móviles. Están los nodos de Elasticsearch que forman el clúster, además de las instancias de Logstash, las instancias de Kibana, los agentes de Beats y los clientes que se comunican con el clúster.

Desde el inicio de la configuración de nuestra solución se habilito la seguridad, la cual permite la protección con contraseña, proteger la comunicación interna con Transport Layer Security (TLS) y cifrar las conexiones entre Elasticsearch y Kibana.

Por otra parte, los servidores implementando están en un segmento aislado de la red local y en la cuales implantamos medidas de seguridad adicionales, como control de acceso basado en roles, filtrado de IP y auditoría.

6.11 Especificaciones generales de programas

6.11.1 Elastic Stack (ELK).

La solución SIEM propuesta permite a los analistas de seguridad de la información monitorear los principales equipos y servicios del área de infraestructura y seguridad,

teniendo así un mejor control de lo que pasa dentro de la organización a nivel tecnológico y reportando cualquier evento que pueda impactar de forma negativa la empresa.

6.12 Descripción de programas

Los principales componentes de nuestra solución de seguridad son:

- Index Lifecycle Management: permite al usuario definir y automatizar políticas para controlar cuánto tiempo debe vivir un índice en cada una de las cuatro fases, así como el conjunto de acciones que se deben realizar en el índice durante cada fase. Esto permite un mejor control del costo de operación, ya que los datos se pueden colocar en diferentes niveles de recursos.
- Snapshot and restore: Esta opción nos permite hacer un respaldo de un clúster de Elasticsearch en ejecución.
- Alertas: Las funciones de alerta del Elastic Stack le brindan todo el poder del lenguaje de consulta de Elasticsearch para identificar cambios en sus datos que le resulten interesantes. En otras palabras, si puede consultar algo en Elasticsearch, puede alertarlo.
- Notificaciones: La función de notificación nos permite enviar cualquier comunicado de una alerta por varias vías como son: Correo electrónico, IBM Resilient, Jira, Microsoft Teams, PagerDuty, ServiceNow, xMatters y Slack.
- Search threshold alerts for Discover: Analiza documentos en un intervalo de tiempo determinado para verificar si se alcanza un umbral para documentos con los criterios designados y luego activa una alerta.
- Audit logging: Realiza un seguimiento de los eventos relacionados con la seguridad, como fallas de autenticación y conexiones rechazadas.

- IP filtering: Aplicar filtrado de IP a clientes de aplicaciones, clientes de nodos o clientes de transporte, además de otros nodos que intentan unirse al clúster.
- Security realms: Las funciones de seguridad del Elastic Stack autentican a los usuarios mediante el uso de dominios y uno o más servicios de autenticación basados en tokens. Un reino se utiliza para resolver y autenticar a los usuarios en función de los tokens de autenticación.

6.12.1 Tecnología a utilizar.

Este proyecto ha sido creado e implementado de manera responsive para hacer posible la integración de diferentes vendor.

Para la implementación del prototipo se utilizó la tecnología siguiente:

- Elasticsearch: Es un motor de búsqueda basado en la librería Lucene. Este proporciona un motor de búsqueda de texto completo distribuido y con capacidad para múltiples usuarios con una interfaz web HTTP y documentos JSON sin esquema.
- Logstash: Es una herramienta para recopilar, procesar y reenviar eventos y registrar mensajes.
- Kibana: Es una interfaz de análisis y búsqueda basada en navegador para Elasticsearch que se desarrolló principalmente para ver datos de eventos de Logstash.
- Beats: Es una plataforma abierta y gratuita para remitentes de datos de un solo propósito. Envían datos de cientos o miles de máquinas y sistemas a Logstash o Elasticsearch.

Para nuestro ambiente local utilizamos lo siguiente:

- Un servidor con el rol de colector, que es el responsable de recibir los eventos de los equipos críticos a monitorear para luego enviarlo a Elasticsearch y procesarlo.
- Un servidor con el rol de procesamiento de datos el cual será el motor de nuestra solución y donde se manejará la data suministrada por los diferentes equipos para su análisis requerido.

Las especificaciones de hardware para esta instalación son las siguientes:

- Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz [Dual]
- 7995MiB System memory
- Virtio SCSI [240GB]

Las especificaciones de software son las siguientes:

- Ubuntu Linux 20.04.3 LTS
- Windows Server 2012 R2
- ELK Full Stack 7.17.3

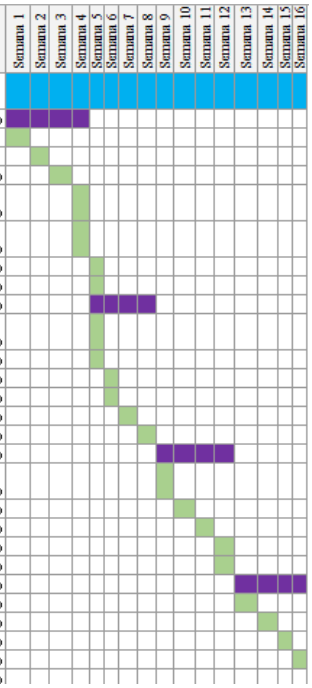
Figura No. 23 ELK stack. Fuente: Victor Cordero.

6.13 Cronograma de actividades para el desarrollo del sistema (en MS Project)

Tabla No. 5

Diagrama de Gantt, Planificación del Proyecto.

Nombre de la tarea	Duración	Asignado	Estado
Desarrollo e implementación de un sistema de gestión de eventos e información de seguridad	**114 días**	Hanvan Sham, Jose Pinales	Abierto
Fase I	**30 días**	Hanvan Sham, Jose Pinales	En progreso
Identificación de los requerimientos de la empresa	4 días	Hanvan Sham	Terminado
Descripción del entorno	4 días	Hanvan Sham	Terminado
Generación de plan de trabajo con definición de las	4 días	Hanvan Sham, Jose Pinales	En progreso
Definición de activos de información que participaran inicialmente de ELK	4 días	Hanvan Sham, Jose Pinales	En progreso
Investigación de los requerimientos para integrar los activos iniciales que reportaran al SIEM	4 días	Hanvan Sham, Jose Pinales	En progreso
Investigación acerca de contruir ELK como un SIEM.	5 días	Hanvan Sham, Jose Pinales	En progreso
Definición de los requerimientos para el montaje de la	5 días	Hanvan Sham, Jose Pinales	En progreso
Fase II	**29 días**	Hanvan Sham, Jose Pinales	En progreso
Solicitud de server para el motaje de ELK de acuerdo a los requisitos ya indagados	4 días	Hanvan Sham, Jose Pinales	En progreso
Diseño Arquitectura ELK como SIEM	4 días	Hanvan Sham, Jose Pinales	En progreso
Definición de los logs a procesar	4 días	Hanvan Sham, Jose Pinales	En progreso
Configuración Previa ELK	4 días	Hanvan Sham, Jose Pinales	En progreso
Instalación ELK	7 días	Hanvan Sham, Jose Pinales	En progreso
Construcción SIEM con ELK	6 días	Hanvan Sham, Jose Pinales	En progreso
Fase III	**30 días**	Hanvan Sham, Jose Pinales	En progreso
Configuración ELK como SIEM y de los sistemas de la empresa enviar los logs al SIEM	7	Hanvan Sham, Jose Pinales	En progreso
Configuración de los Beats	7	Hanvan Sham, Jose Pinales	En progreso
Parametrización de los logs y eventos a mostrar	7	Hanvan Sham, Jose Pinales	En progreso
Tunning del SIEM.	4	Hanvan Sham, Jose Pinales	En progreso
Creación y configuración de tableros.	5	Hanvan Sham, Jose Pinales	En progreso
Fase IV	**24**	Hanvan Sham, Jose Pinales	En progreso
Evaluación inicial de la solución	6	Hanvan Sham, Jose Pinales	En progreso
Ajuste y correción de errores	5	Hanvan Sham, Jose Pinales	En progreso
Monitoreo del sistema	4	Hanvan Sham, Jose Pinales	En progreso
Documentación del proyecto	5	Hanvan Sham, Jose Pinales	En progreso
Entrega del proyecto	4	Hanvan Sham, Jose Pinales	En progreso



Nota. Fuente: Elaborado por los sustentantes.

Conclusiones

Si bien es cierto, el objetivo de esta investigación se basó en demostrar las ventajas que ofrece una solución de manejo de eventos y seguridad informática y como la misma puede ayudar a mantener las operaciones de una Fintech.

Es necesario recalcar que luego de conocer un poco sobre las empresas de Fintech, queda claro la estrecha relación con la triada de la seguridad de la información C.I.D (Confidencialidad, Integridad y Disponibilidad (C.I.A, por sus siglas en inglés), y es que al igual que toda empresa bancaria, el manejo de los recursos financieros está sujeto a regulaciones que entre otras cosas obligan al cumplimiento de la mencionada triada.

Ciertamente de los tantos elementos de seguridad que pueden incorporarse en una infraestructura, el SIEM no es utilizado para aplicar Confiabilidad, sin embargo, puede mostrar cuando la misma ha sido vulnerada o se intenta vulnerar, mediante los registros de servidores de autenticación (LDAP, Radius, SAML, etc). No es utilizado para garantizar la Integridad, pero si muestra cuando en una red de datos están en uso protocolos que no la garantizan, mediante los registros de Firewalls, Endpoint protection, IPS, entre otros.

Tampoco podemos garantizar disponibilidad mediante un SIEM, pero podemos ver cuando la misma puede perderse mediante la información consolidada de los activos que están destinados a garantizarla.

Si bien es cierto que en este proyecto nos hemos enfocado en la solución de SIEM basada en Elasticsearch y su Stack, no queda duda de que existe un sin número de soluciones entre comerciales, de código abierto, de implementación local (on-premise) o para ejecutar desde la nube. Y sin importar la solución que se elija, ninguna puede operar “out of the box”, se requiere conocer la infraestructura y cuáles son los activos críticos. Con esta información a solo necesitamos que nuestro SIEM posea las herramientas que nos permitan que la solución se adapte a nuestra infraestructura.

Referencias

¿Qué es el convenio de budapest? (s. f.). Recuperado de https://nic.ar/es/enterate/novedades/que-es-convenio-budapest

¿Qué es el ELK stack? (s. f.). Recuperado de https://www.elastic.co/es/what-is/elk-stack

¿Qué es SIEM? ¿Y por qué es importante tener? (2018, 28 de mayo). Recuperado de https://www.helpsystems.com/es/blog/que-es-un-siem

Alcalde, J. C. (2017, 14 de junio). Modelo canvas – economipedia. Recuperado de https://economipedia.com/definiciones/modelo-canvas.html

Anónimo. (2021, 17 de agosto). Qué es una fintech: El sector que vuelve loco al sector financiero tradicional. Recuperado de https://www.infobae.com/economia/2021/08/17/que-es-una-fintech-el-sector-que-vuelve-loco-al-sector-financiero-tradicional/

Boletín mensual marzo 2021 (Informe CSIRT-RD 30/03/2021). (2021). Santo Domingo. Recuperado de https://cncs.gob.do/boletines/

Bonne, L. (2022). Finanncial technology (fintech). Recuperado de https://ezproxy.unibe.edu.do:2055/login.aspx?direct=true&db=ers&AN=119214065&lang=es&site=eds-live

Cordero, V. (2022). *Diseño e implementación de un SIEM* (Master no publicada). IMF Businesss School, Madrid.

García, S. (2020, 16 de julio). ¿Qué son los beats de elastic? + ejemplo de uso de filebeat - davinci group. Recuperado de https://www.davincigroup.es/beats-elastic-ejemplo-filebeat/

González, J. (s. f.). Instituto tecnológico de santo domingo - INTEC. Recuperado de https://www.intec.edu.do/oferta-academica/postgrado/articulos-de-postgrado/intec-postgrado-por-que-es-necesario-y-como-elegir-el-mas-indicado-2#:~:text=Tipos%20de%20tesis%20según%20el%20método%20de%20investigación&text=Básica,%20pu

Kagan, J. (2015, 17 de marzo). What is fintech? Recuperado de https://www.investopedia.com/terms/f/fintech.asp

Losada, S. (2018, 30 de julio). ¿Qué es ELK? Elasticsearch, logstash y kibana. Recuperado de https://openwebinars.net/blog/que-es-elk-elasticsearch-logstash-y-kibana/

Método cualitativo. (s. f.). Recuperado de https://concepto.de/metodo-cualitativo/

Monroe, B. (2016, 27 de julio). Nueva directiva de Europa sobre ciberseguridad presiona a bancos y compañías para que se preparen mejor para los ciberataques - CFCS | Asociación de Especialistas Certificados en Delitos Financieros. Recuperado de https://www.delitosfinancieros.org/nueva-directiva-de-europa-sobre-ciberseguridad-presiona-a-bancos-y-companias-para-que-se-preparen-mejor-para-los-ciberataques/

Open source. (2021, 28 de abril). Recuperado de https://quadrantsec.com/sagan_log_analysis_engine/

Pinedo, A. (s. f.). 5 características de las fintech que las diferencian de los bancos. Recuperado de https://leasein.pe/blog/caracteristicas-de-las-fintech/

Políticas de seguridad para la pyme. (s. f.). Recuperado de https://www.incibe.es/protege-tu-empresa/herramientas/politicas

Pedroza Arango, J. D. (2016). *Implementación de un gestor de seguridad de la información y gestión de eventos (SIEM)* (Trabajo de grado no publicado). UNIVERSIDAD DE SAN BUENAVENTURA MEDELLÍN, MEDELLÍN.

Qué es benchmarking y consejos de uso para el marketing. (2017, 25 de agosto). Recuperado de https://rockcontent.com/es/blog/que-es-benchmarking/#:~:text=Es%20decir,%20que%20el%20benchmarking,para%20mejorar%20tu%20propio%20desempeño.

SIEM - ciberseguridad al alcance de su presupuesto - gudix security. (s. f.). Recuperado de https://blog.gudixsecurity.com/ciberseguridad-a-su-alcance-siem/

Tipos de Investigación en la elaboración de tesis de Grado. (2020, 12 de julio). Recuperado de https://asesoriamss.com/servicios/empresa-2/item/153-tipos-de-investigacion-en-la-elaboracion-de-tesis-de-grado

Whitson, G. (2020). Artificial intelligence. Recuperado de https://ezproxy.unibe.edu.do:2055/login.aspx?direct=true&db=ers&AN=89250362&lang=es&site=eds-live.

APÉNDICE

Figura No. 24 A-1 Gráfico de: ¿Sabes usted lo que es una FINTECH? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.

Interpretación

De un total de 13 empleados encuestado, todos tiene conocimiento de lo que es una Fintech.

Figura No. 25 A-2 Gráfico de: ¿Conoces el propósito de una FINTECH? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.

Interpretación

De un total de 13 empleados encuestado, 11 empleados equivalente al 84,6% de los encuestado saben cual es el proposito de una Fintech, mientras que 2 empleados equivalente al 15,4% de los encuestado indicaron que NO y Talvez.

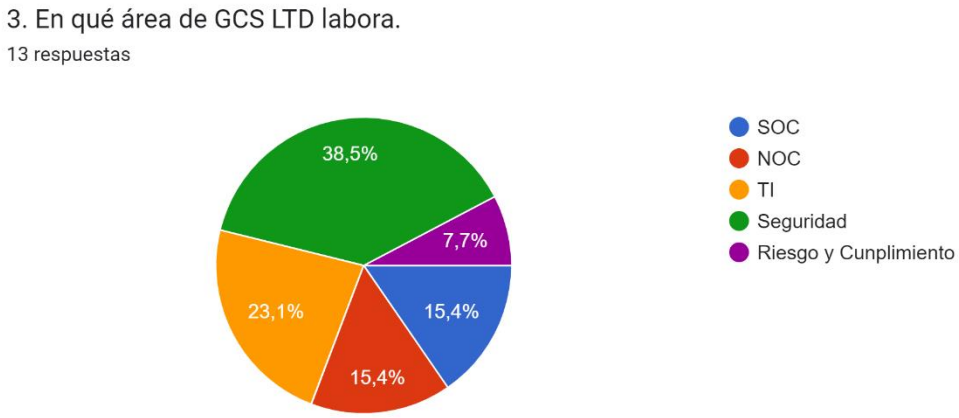


Figura No. 26 A-3 Gráfico de: En qué área de GCS LTD labora. Fuente: Elaborado en base a resultado de la aplicación de la encuesta.

Interpretación

De un total de 13 empleados encuestado, 5 empleado son de seguridad informatica obteniendo un 38,5% de los encuestados, 3 son empleado de TI obteniendo un 23,1% de los encuestados, 2 empleados son operadores del centro de monitoreo obteniendo el 15.4, 2 empleados son operadores del SOC obteniendo tambien un 15,4% de los encuestados y 1 empleado es de reisgo y cumplimiento obteniedo el 7,7% de los empleados.

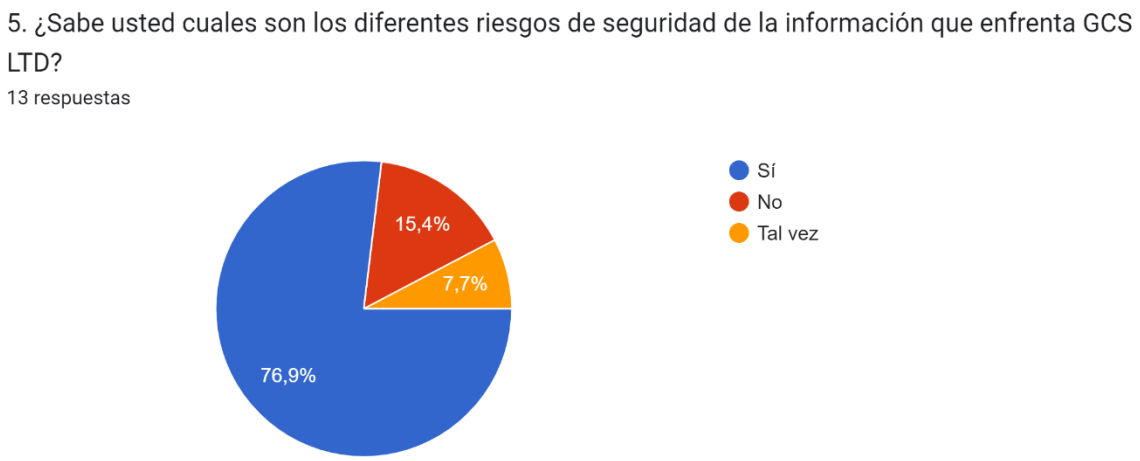


Figura No. 27 A-4 Gráfico de ¿Sabe usted cuales son los diferentes riesgos de seguridad de la información que enfrenta GCS LTD? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.

Interpretación

De un total de 13 empleados encuestado, 10 empleados equivalente al 76,9% saben cuales son los riesgo, 2 empleados equivalente al 15,4% no conocen los riesgo y 1 empleados equivalente al 7,7% indico que tal vez sabe.

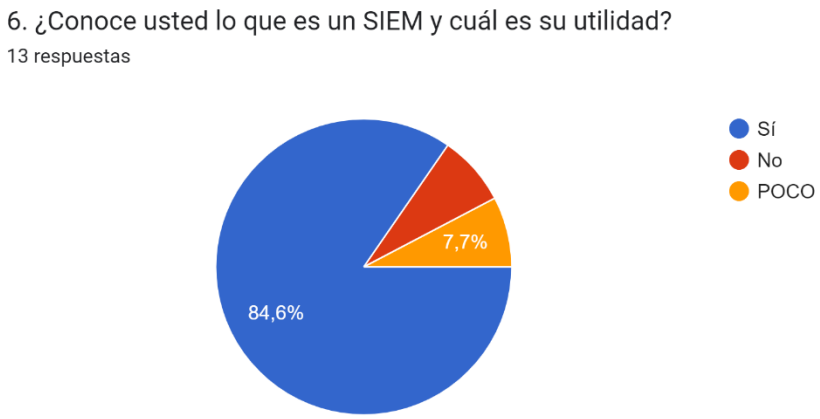


Figura No. 28 A-5 Gráfico de ¿Conoce usted lo que es un SIEM y cuál es su utilidad? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.

Interpretación

De un total de 13 empleados encuestado, 11 empleados equivalnete al 84,6% conoce lo que es un SIEM, el 15,4% de los empleados no tienen conocimiento de un SIEM.

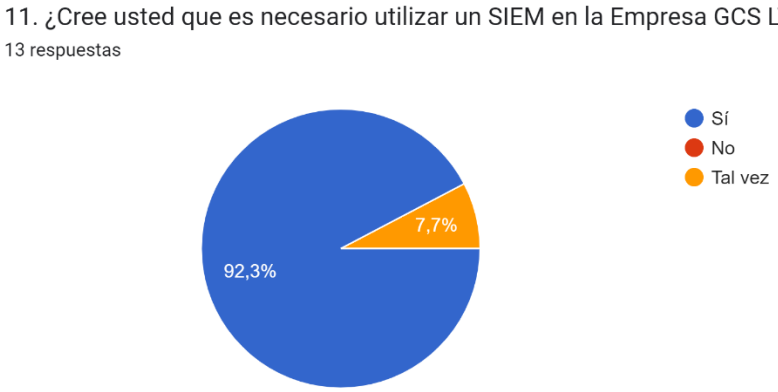


Figura No. 29 A-6 Gráfico de ¿Cree usted que es necesario utilizar un SIEM en la Empresa GCS LTD? Fuente: Elaborado en base a resultado de la aplicación de la encuesta.

Interpretación

De un total de 13 empleados encuestado, 12 empleados equivalnete al 92,3% estuvo de acuerdo con la implementación de un SIEM dentro de la organización, solo 1 empleado indico que tal vez.

Figura No. 30 A-7 Instalación ES, llave repositorio para Elastic.

En esta imagen estamos descargando la llave pública PGP con lo que están firmados los paquetes oficiales de Elastic.

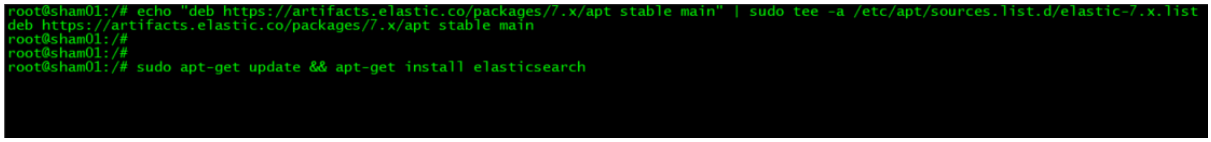


Figura No. 31 A-8 Instalación ES, repositorio 7.17.3

Aquí agregamos el repositorio en nuestras “fuentes” de apt, actualizamos y procedemos con la descarga de los paquetes.

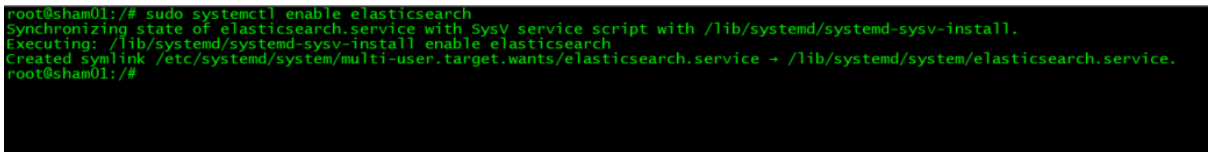


Figura No. 32 A-9 Instalación ES, habilitar servicio.

Aquí procedemos a configurar el Elasticsearch para que opere en forma de daemon (servicio) y auto arranque ante un reinicio del servidor.

Figura No. 33 A-10 Configuración ES, Usuario X-Pack.

Esto generará todas las credenciales (usuarios y passwords), de los diferentes servicios que componen el stack.

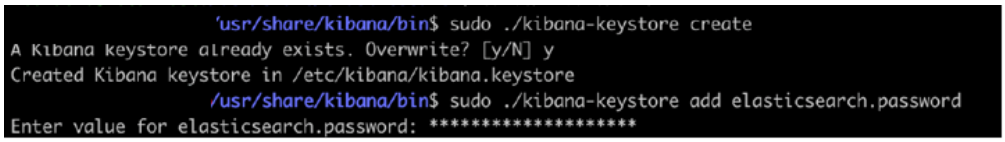
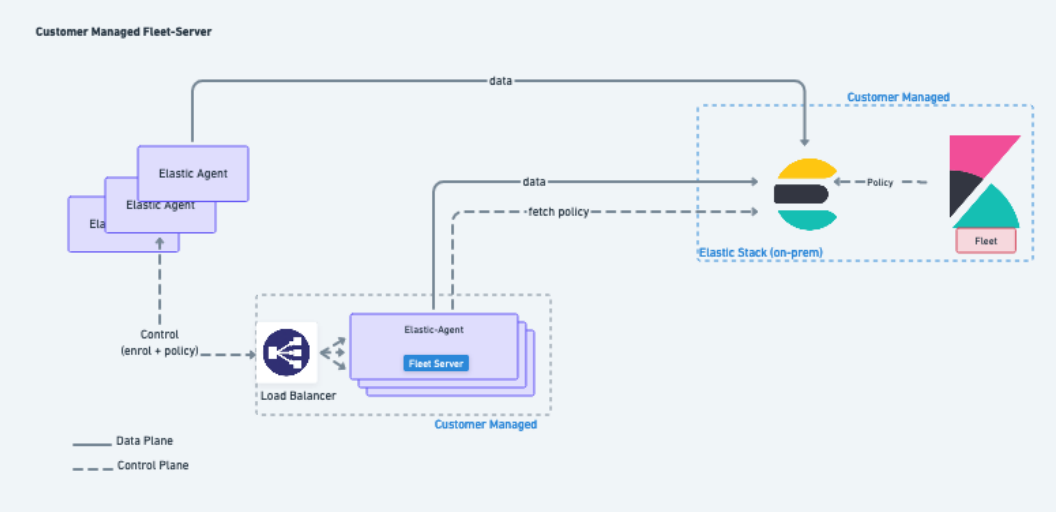
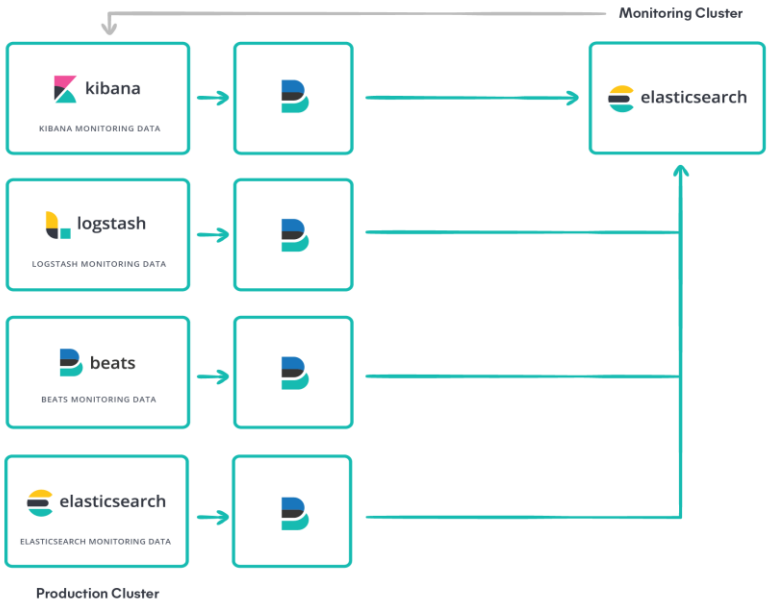


Figura No. 34 A-11 Configuración ELK, Kibana Keystore.

Aquí configuramos el keystore de kibana.

ANEXOS


Customer Managed Fleet-Server
data
Customer Managed
Elastic Agent
Elastic Agent
data
Policy
fetch policy
Elastic Stack (on-prem)
Fleet
Control
(enrol + policy)
Elastic-Agent
Fleet Server
Load Balancer
Customer Managed
Data Plane
Control Plane


Monitoring Cluster
kibana
KIBANA MONITORING DATA
elasticsearch
logstash
LOGSTASH MONITORING DATA
beats
BEATS MONITORING DATA
elasticsearch
ELASTICSEARCH MONITORING DATA
Production Cluster

VITA

Nacido en la ciudad de Santo Domingo, R.D., el 06 de febrero del año 1993. Cursó sus estudios primarios en la escuela básica Dr. Joaquín Balaguer y sus estudios secundarios en el liceo nocturno Jamaica. Egresado del tecnólogo de Redes de la información del Instituto Tecnológico de las Américas (ITLA). Estudiante de término de la carrera de Ingeniería en Tecnologías de la información y comunicación (TIC's). En Materia laboral ha trabajado para las siguientes instituciones: Claro Opitel, Wolf Security Systems y actualmente brinda servicio para DC SOLUTIONS y GCS LTD, cuenta con acreditada experiencia de más de 3 años en Gestión de TI, Administrador de redes de datos y Seguridad informática. Laborando y asesorando empresas del sector industrial, financiero y de servicios.

Hanvan Sham H.

Nacido el 20 de diciembre de 1995, hijo de José Pinales y Gregoria Figuereo. José Manuel Pinales es el tercero de tres hijos de esta unión, quien ha vivido en el gran Santo Domingo toda su vida. Desde muy pequeño le gustaba los deportes por lo que a temprana edad inicio a practicar béisbol.

Estudió el nivel básico en la Escuela Básica Cruz Grande y secundarios en el politécnico Cristo Obrero mención informática. Egresado del tecnólogo de Redes de la información del Instituto Tecnológico de las Américas (ITLA). En el ámbito laboral ha trabajado para las diferentes instituciones tales como American Mobile International Teleservice, Trilogy Dominicana (Viva) y actualmente labora en Altice Dominicana. Cuenta con más de 3 años de experiencia en redes de información, en análisis, diseño, implementaciones, solución de problemas y operación.

José Manuel Pinales