UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Análisis de funcionalidad y utilidad de herramientas de seguridad instaladas en un Security Operation Center (SOC)
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autor:
Eugenio Patricio Garzón Ullaguari
Tutor:
Msc. Pablo Marcel Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Recalde con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado Análisis de funcionalidad y utilidad de herramientas de seguridad instaladas en el Security Operation Center (SOC) en la empresa XY

Elaborado por: Patricio Garzón, de C.I: 1002359808, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 25 marzo del 2023

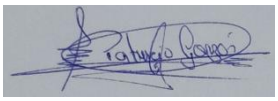
Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Eugenio Patricio Garzón Ullaguari C.I: 1002359808, autor del proyecto de titulación denominado: Análisis de funcionalidad y utilidad de herramientas de seguridad instaladas en un Security Operation Center (SOC) en la empresa XY. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., 25 marzo del 2023



Firma

Orcid: 0000-0003974-9134

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

El avance progresivo de la sociedad en el campo tecnológico ha sido evidente en los últimos 20 años, de forma que la humanidad se va haciendo cada vez más tecnológicamente dependientes y en esa medida también somos más vulnerables (Arroyo, 2020)

Es importante indicar y por razones de confidencialidad en la institución donde se desarrolla este trabajo actualmente, durante el desarrollo de este análisis, la institución se llamará “EMPRESA XY”; en los casos que fuere necesario.

Contextualización del tema

En un mundo tan cambiante, incierto, complejo y que avanza vertiginosamente sin detenerse, en el cual el avance imparable de la tecnología, junto a la imperiosa necesidad de todas las personas por obtener información para cumplir con sus diferentes propósitos cotidianos, y cuyas amenazas, estrategias y herramientas de los ciber-atacantes son cada vez más sofisticadas, ha provocado que se creen soluciones y herramientas de seguridad informática acorde a las nuevas circunstancias, y con la finalidad de poder ejecutar las normas de control y prevención de los posibles ataques cibernéticos.

Generalmente, las herramientas creadas por los ciber-atacantes suelen ir por delante de las defensas. Esto se evidencia en los reportes de alertas y advertencias del Centro de Respuesta a Incidentes Informáticos de la ARCOTEL EcuCERT, donde se registran denuncias de cientos de ataques diarios que se producen a nivel nacional; y así mismos miles de ataques a nivel internacional que registra una Organización de Ciberseguridad de España (INCIBE), según muestra los boletines informativos semanales de ciberseguridad publicado por el Instituto en mención (INCIBE, 2023).

Algunos ciber-ataques consiguen su propósito y otros no; y por ello, cada vez las organizaciones o instituciones cada día tienen la necesidad de implementar un Centro que realice el monitoreo de las Operaciones de Seguridad (SOC por sus siglas en inglés), que permita de manera proactiva, disminuir y evitar que los ciber-ataques tengan éxito y así se disminuya el impacto del ataque, en caso de que se materialice.

Es indispensable señalar, que un SOC es generalmente un sistema que se encuentra compuesto por varios elementos, entre ellos: «un grupo que comprende expertos en seguridad, que lleva a cabo diversas operaciones de seguridad, incluida la detección, el análisis, respuesta, notificación y prevención de incidentes de ciberseguridad» (Chaeyeon Oh, 2002) así mismo, permite gestionar las actividades o alertas informáticas para tomar medidas preventivas, correctivas o de análisis de los aspectos que engloban la ciberseguridad

y de esta manera proteger o disminuir el impacto que puede tener la perdida de información dentro de su infraestructura crítica.

El mercado nos permite el análisis de un sin número de herramientas para el control de las amenazas cibernéticas, que se basan en el uso de herramientas que están bajo software gratuito, libre o de código abierto, y otras que son appliance o bajo licencias; que son necesarias e indispensables para el correcto funcionamiento de un SOC; como por ejemplo: Sistemas de Detección de Intrusos (IDS), Administrador de Eventos de Seguridad de la Información (SIEM), Next Generation Firewall (NGF), Unified Threat Management (UTM), entre otras.

Es por ello que, conociendo la funcionalidad y la utilidad de algunas herramientas específicas que se emplean en un SOC, el presente trabajo realizará un análisis de algunas de ellas, a fin de poder detectar riesgos de ciberseguridad mediante alertas o amenazas que se dan en el software o hardware de la infraestructura critica de la empresa XY.

Problema de investigación

Las variables para proteger una infraestructura de TIC de cualquier institución, es necesario identificar las amenazas y establecer alternativas de protección y contramedidas. Este proceso de protección se cristaliza mediante las políticas de seguridad en la que se indican expresamente la infraestructura crítica de información a proteger como son instalaciones, equipos, desarrollo de aplicativos, privacidad, etc., para esto es preciso que constantemente se evalúe la importancia de cada uno de ellos, la posibilidad de se vea afectado por múltiples amenazas y el impacto de estas (Arroyo, 2020)

En virtud de los múltiples ataques informáticos que se han producido en el último año a las instituciones públicas y privadas; la empresa XY consiente de las amenazas que se presentan en sus sistemas y aplicativos institucionales publicados en el internet e intranet y que son utilizados por los usuarios de la institución desde cualquier parte del mundo y; con la finalidad de tener el menor impacto posible en caso de un ciber-ataque a su infraestructura critica de información; el SOC tiene muchas dudas sobre qué tipo de herramientas de seguridad debe implementar y si debe ser bajo software libre o bajo licencias, y que permitirán garantizar y alcanzar de sobre manera la SEGURIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD de la información institucional y de sus usuarios.

A esto se contrapone el Decreto Ejecutivo No. 1014 emitido el 10 de abril de 2008 donde se «dispone el uso de Software Libre en los sistemas y equipamientos informáticos de la Administración pública de Ecuador. Es interés del Gobierno ecuatoriano alcanzar soberanía y autonomía tecnológica, así como un ahorro de recursos públicos» (Correa, 2009)

Actualmente en el mercado existen muchas herramientas tecnológicas de seguridad ya sean estas bajo software libre o bajo licencias; en el SOC de la empresa XY se han implementado algunas herramientas de seguridad como son: IDS-wazhu, SIEM-splunk, NGF-Palo Alto, Firewall-shorewall; y, que en cierto modo proporcionan alertas sobre posibles vulnerabilidades o incidencias de ataques. De las herramientas mencionadas algunas son bajo software libre y otras con licencia; es necesario realizar el respectivo análisis de funcionalidad y utilidad de las mismas para poder medir sus capacidades de respuesta ante algún tipo de incidente de ciberseguridad y poder determinar si son las correctas o las más idóneas para la institución.

Es importante que el personal que trabaja en el SOC, posean toda la capacidad de interpretar los logs de los sistemas o los registros del sistema, con la finalidad de identificar incidentes de seguridad, o identificar actividades irregulares en los sistemas de información, de comunicación, base de datos, sistemas operativos, aplicativos, servicios web; entre otros.

¿Cómo, el conocer la funcionalidad y utilidad de herramientas de seguridad ya sean en software libre como dispone el decreto 1014 o con software licenciado; y que se instalarán en un SOC permitirá responder de una manera eficiente ante cualquier tipo de amenazas o vulnerabilidades?

Objetivo general

Analizar la funcionalidad de herramientas de seguridad basadas en software libre y con licencia, instaladas en el Security Operation Center (SOC) de la empresa XY.

Objetivos específicos

1. Analizar la utilidad de las herramientas de seguridad bajo software libre y con licencia instaladas en SOC de la empresa XY, como son: IDS-WAZHU, SIEM- SPLUNK, NGF-PALO ALTO, FW-SHOREWALL.
2. Comparar las ventajas y desventajas al usar herramientas de seguridad de software libre o de código abierto y los equipos appliance o bajo licencias, para tomar la mejor elección a momento de elegirlas.
3. Determinar un proceso para levantar un reporte con el detalle del evento de seguridad registrado en base a los registros que arroja estas herramientas de seguridad Intrusion Detection System (IDS) y el Security Information Event Management (SIEM)

Vinculación con la sociedad y beneficiarios directos:

En el Ecuador al interior de empresas públicas y privadas han creado departamentos especializados de Respuesta a Incidentes de Seguridad de la Informátición (CSIRT) y podemos encontrarlas en las siguientes áreas: universidades, fuerzas armadas, sector privado y financiero. Resulta importante ir articulando una estructura o sistema para realizar la coordinación de sus respuestas, y de esta manera poder trabajar de con resultados integrados, en base a protocolos, normativas, políticas y lineamientos nacionales.

El Centro de Respuestas a incidentes informáticos de Ecuador (EcuCERT) debe fomentar la creación de centros coordinadores sectoriales, con la única finalidad de poder gestionar los incidentes o ciber-ataques a nivel nacional e intersectorial (MINTEL, 2021)

La empresa XY como institución del sector defensa y como parte del Consejo de Seguridad Nacional que se encuentra al servicio de todos los ciudadanos y contribuye al desarrollo del País; cuya misión es la de garantizar la protección de la libertad y la lealtad, vigilando el espacio aéreo; empleando todos sus sistemas de información y comunicaciones y de esta manera poder desarrollar su poder militar aéreo para el cumplimiento de sus objetivos institucionales para garantizar la defensa y contribuir con la seguridad y desarrollo de la sociedad.

Al desarrollar este proyecto se pretende mejorar la capacidad de anticipar un posible ataque a la infraestructura crítica digital institucional; de igual manera mejorar la administración de las herramientas que se pueden implementar en un SOC y también poseer un mecanismo de defensa ante un sin número de ciber-ataques que intenten impedir el cumplimiento de la misión operativa institucional.

Se pretende mejorar el esquema en la toma de acciones de respuesta a los sistemas de seguridad de procesamientos de datos o de Información, a fin de garantizar de una manera adecuada la «confidencialidad, integridad y disponibilidad que es parte fundamente de la seguridad; para mantener procedimientos de seguridad de datos lógica y física de la infraestructura de información de la empresa XY.

Los sistemas de información y comunicaciones ahora más que nunca son determinantes para la toma de decisiones y, por tanto, también son más vulnerables a ataques internos y externos.

Objetivos de Desarrollo Sostenible (ODS), será en base al número nueve «Industria, Innovación e Infraestructura». La innovación conjuntamente con el progreso y avance tecnológico actualmente son las claves para crear, desarrollar y aplicar soluciones que

perduren en el tiempo para afrontar con soluciones prácticas los desafíos económicos y medioambientales (ETICENTRE, 2019).

Brinda el asesoramiento sobre las herramientas de seguridad que pueden ayudar a combatir la detección de amenazas o vulnerabilidades mediante la administración de estos sistemas: SIEM, IDS y NGF, garantizando la seguridad de la información.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Luego de la pandemia el aumento masivo del uso y aprovechamiento de todas las bondades y herramientas que poseen las tecnologías de información y comunicaciones (TIC) en cualquier aspecto de la sociedad en general y a nivel mundial; se han producido amenazas de ciberseguridad que resultan cada vez más complejo, sofisticado, malicioso, bien organizado y bien financiado.

El uso generalizado de herramientas impulsadas por tecnologías de inteligencia artificial (IA) las mismas que conducirán a tecnologías más personalizadas y de alto impacto en el tema de ciberataques. Poder incluir la complejidad y la modernidad de tales ataques requiere llevar a cabo la instalación, configuración e implementación de un centro de operaciones de seguridad (ISACA, 2021)

1.1. Contextualización general del estado del arte

Un SOC es un lugar con una ubicación física donde se compacta el recurso humano y material , la misma que posee una gran responsabilidad para el personal que opera estos centros y es que es la monitorización, detección, análisis, prevención y seguimiento de los eventos de seguridad en las redes e infraestructuras de la organización (Estrada, 2017)

Según Fueyo (2020), en la investigación que realizó sobre la configuración de las actividades para operar un SOC en el sistema financiera desde cero con soluciones IDS y SIEM, Introdujo la imperiosa necesidad de implementar un SOC. cuyo objetivo es el de realizar el monitoreo y protección de un sin número de amenazas cibernéticas que en la actualidad se está haciendo muy común ataques dirigidos a instituciones públicas o privadas; tal implementación requiere del consumo de logs o registros del sistema que se almacenan en cada proceso lógico de acuerdo a su transaccionalidad: esto servirá como input para replicar casos semejante ante un comportamiento anómalo o extraño en los sistemas y evitar que los datos puedan ser alertados.

Múltiples amenazas de ciberseguridad están esperando el momento de penetrar en las redes hoy en día para todo el mundo pero, es especialmente para las empresas, y más

aún para las instituciones financieras, donde este riesgo o amenaza aumenta, debido a que los grandes actores especializados en ciber-ataques, centran sus actividades en ellas.

Considerando lo anteriormente indicado y de acuerdo a la experiencia personal laborando en el Departamento Tecnologías de Información de la empresa XY, podría indicar que la importancia de la implantación de un SOC con las herramientas indicadas ayuda a las empresas sean públicas o privadas a anticipar a un incidente de vulnerabilidad, prevenir la posibilidad de ser atacados y cómo reaccionar de manera rápida y efectiva ante un ataque, además es muy importante saber cómo las organizaciones o en este caso la empresa XY debe hacer ante un posible ataque o amenaza.

Entendiendo a fondo la infraestructura con la que los atacantes operan; pero más importante aún, es como las organización depende de esa infraestructura para responder con sus defensas ante diferentes ataques; esto sin duda se convierte en un reto porque se debe entender a profundidad su entorno u organización, deben entender el entorno en el que vivimos en términos de amenazas de ciberseguridad y es ahí donde se debe desarrollar las estrategias ante una respuesta a un incidente.

Software libre y software licenciado

Según Mahecha (2022) Free Open Software Source de sus siglas FOSS y Total Cost of Ownership de sus siglas COTS, El software libre o de código fuente abierto en el uso e implementación de nuevas herramientas de seguridad se han ido incrementando constantemente y de igual manera en importancia, esto se debe a que muchas herramientas o sistemas operativos basados en estos sistemas, tanto en organizaciones públicas como en privadas las están implementando en el mundo.

La migración a sistemas de código abierto open source es hoy en día una de las alternativas que están adoptando y que ponen en práctica las instituciones u organizaciones que conforman los países de Sur América, esto es el resultado de un menor Costo Total de Propiedad (TCO) y el aumento en las capacidades para hacer frente a las vulnerabilidades y ataques a la infraestructura de datos de las instituciones.

Durante los últimos años, el desarrollo de distribución del software y sus múltiples aplicaciones está regido por dos modelos que han impactado a las organizaciones, como son los productos con costo de licencia que ofrecen a sus usuarios una gran variedad de características y funcionalidades basado en un modelo de compra y venta de licencias y el producto que se distribuyen libremente. El software propietario de alguna persona o una empresa donde existen restricciones de su uso basado en un acuerdo de licencia y su código de origen o fuente se mantiene en absoluto confidencialidad o secreto.

Existen limitaciones propias del software con costo de propiedad que se han implementado con el tiempo como actualizaciones costosas o debilidades de seguridad, lo que ha servido de gran utilidad para que se vaya consolidando el modelo basado software de libre acceso.

Herramientas para un SOC

Según Tocino (2022) dentro del funcionamiento para un SOC, convergen diversas herramientas que en su mayoría son utilizadas para la gestión y análisis de alertas de vulnerabilidades; entre las cuales, se pueden diferenciar algunas categorías de programas o software. Para este caso, el SIEM, IDS, NGF y Firewall; son programas de seguridad que tienen como objetivo primordial brindar a las organizaciones que procesan gran cantidad de información con herramientas que son bastantes útiles para evaluar potenciales amenazas de seguridad de la información en la infraestructura crítica de negocio, a través de la ingesta e interpretación de datos y priorización de amenazas.

Se hace posible debido a que el SOC mantiene un análisis centralizado de datos de seguridad, que a su vez son correlacionados a partir de múltiples sistemas de seguridad, que incluyen software antivirus, firewalls o cortafuego y soluciones de prevención de intrusiones.

1.2. Proceso investigativo metodológico

De acuerdo a Abreu (2020), señala que el marco metodológico se describe con los pasos detallados la forma en que se ha lleva a cabo el proceso de investigación; bajo una metodología científica. Esto permite dar una explicación sobre la propiedad y características de la metodología de investigación que se utilizan la aprobación de resultados, que poseen el tipo de información que es adecuada para para comprender, aceptar y demostrar la capacidad de réplica de los análisis de resultados de la investigación, o dicho de otra manera es una estructura que permite estudiar los medios y caminos para investigar y llegar a demostrar una verdad.

Investigación Cualitativa

Este tipo de investigación cualitativa se puede definir como el estudio, método o proceso cuyo propósito es apoyar al entendimiento y compresión de los sentidos y las perspectivas de las personas que se encuentran a nuestro alrededor; esto es, ver el mundo desde la perspectiva del propio de investigador; y cómo este punto de vista se encuentran definidos por sus contextos físicos, sociales y culturales (Maxwell, 2019)

En otras palabras, es un proceso o método de recolección y análisis de información y a su vez se utiliza estos datos para responder las dudas que se dan en el proceso de investigación

o indicar nuevas interrogantes, en esta investigación no se utilizan información que realiza medición numérica, utiliza descripciones profundas e interpretaciones de fenómenos.

En esta redacción, la metodología de investigación que se utilizará es el análisis cualitativo, en el cual se recolectarán datos de información a partir de análisis de contenido en publicaciones similares o trabajos investigativos sobre las herramientas que se utilizan en un SOC, sea en software libre o bajo licencia; y con esta información se podrá validar la funcionalidad y utilidad de herramientas de seguridad instaladas en un SOC como: IDS-wazhu, SIEM-splunk, Next Generation Firewall Palo Alto, firewall-shorewall,

Proceso Inductivo

Según Urzola (2020), El proceso inductivo puede definirse como el pensamiento abstracto es el pensamiento teórico o la validación de conceptos, mientras que la obtención o la experiencia cotidiana que son las experiencias, ideas, espectativas, percepción y opinión del investigador que ha plantado desde las vivencias cotidianas diarias y laborales, profesional u otro campo; esto es una idea o afirmación que va de lo específico a lo general a partir de un conjunto de evidencias, donde se utiliza el razonamiento para la obtención de las conclusiones y que además pueden partir de hechos que son particulares y aceptados como válidos.

Se aplicó el proceso de investigación inductivo para realizar el estudio o comparación sobre la factibilidad o no al usar herramientas de software libre o código abierto y los equipos appliance o bajo licencias; de igual manera con este proceso se va a determinar un proceso para levantar un reporte con el detalle del evento de seguridad registrado en base a los registros de las herramientas

1.3. Análisis de resultados

Acorde a Estrada (2017) la variedad de herramientas que puede realizar un buen trabajo y operar un SOC son: firewall, IDS´s, sistemas de ataque de denegación de servicio por sus siglas AntiDDoS, SIEM´s, herramienta de encriptación Rivest-Shamir-Adelman (RSA), antivirus, Data Lost Prevention (DLP); y todas deben proporcionar por lo menos los siguientes servicios:

Monitoreo y gestión de la infraestructura de seguridad

Son aplicativos que permiten de alguna manera monitorear y administrar las diferentes herramientas que protegen y dan seguridad de vulnerabilidades internas o externas; así como a su infraestructura de red.

Gestión de incidentes de seguridad

Es la identificación, análisis y respuesta referente a eventos de seguridad que son registrados por las diferentes herramientas que se encuentran en un SOC.

Gestión de vulnerabilidades

La gestión de vulnerabilidades son las fallas de los sistemas de seguridad que se encuentran en los servicios web o servidores de aplicaciones, ofrecen detección temprana de amenazas y pueden identificar, evaluar y corregir las diferentes vulnerabilidades que se encuentran en la red.

Auditorias de seguridad

Son acciones que permiten verificar que un sistema informático ha sido violentado o ha existido fuga o robo de información, revisa las listas de verificación en los diferentes procesos definidos del hardware o software.

Seguridad en Internet

La red de procesamiento de información extensa y que a nivel mundial conocida como Internet y que al mismo tiempo es la red interconectada más grande del mundo en donde se puede encontrar cualquier tipo de información sea apropiada o inapropiada; de hecho a través de la implementación, instalación y configuración de medidas de seguridad en internet y que ayudan a mantener la integridad, privacidad y la seguridad en la misma.

Controles de acceso (ACL´s)

Son listas de controles de acceso, y que permiten o niegan el acceso a los protocolos de comunicaciones, son herramientas que permiten controlar el tráfico desde y hacia la red; también realiza las tareas de acceso o deny a ciertas páginas con contenido no autorizado o censurado a través de blacklist o whitelist.

Detección y análisis de malware

Son sistemas que permiten detectar, identificar y desactivar algún tipo de programa malicioso en dispositivos informáticos, estas herramientas son esenciales para mantener y dar la seguridad respectiva a los datos de los usuarios.

Detección de prevención/protección de intrusos

Los sistemas IDS/IPS son complemento entre sí, a través de una verificación proactiva del tráfico de datos entrante de un sistema que permite eliminar paquetes maliciosos, estas herramientas utilizan filtrado de tráfico para dar protección y seguridad.

Funcionalidades de software libre y licencias

De acuerdo a Lascano (2022) las funcionalidades que deben tener una herramienta de seguridad informática y sus componentes radican en la elección. Está decisión está basada en contextos de muchos casos de uso que la herramienta debe resolver; por lo general esta evaluación, aunque no obligada a realizarla muchas veces es necesaria para poder analizar aspectos que se desea conseguir de los necesarios para permitir elevar a niveles de categoría y dar la importancia deseada a la característica de los resultados y conocer la pertinencia de una herramienta y de este modo comparar con otras soluciones.

CAPÍTULO II: PROPUESTA

Los datos de información actualmente es considerado como el activo más frágil y valioso de mayor cuidado en la mayoría de las organizaciones y a su vez para la empresa XY, representa una gran preocupación y más aún cuando se han incrementado los métodos que atentan contra la protección de datos y afectan a la confidencialidad, integridad y disponibilidad; estas particularidades se ha convertido en incremento de la necesidad por adoptar normas, controles, políticas y alternativas que llevan a realizar la gestión proactiva o reactiva de los eventos, amenazas e incidentes informáticos con el fin controlar el impacto que afectan el normal funcionamiento administrativo y operativo en cada uno de los sitios remotos de la institución.

Realizar el análisis de funcionalidad y utilidad de los programas de seguridad que conforman un SOC, y que resulta de gran necesidad e importancia, ya que se puede llegar a determinar si son las más apropiadas e idóneas para la institución; en este sentido se deben realizar el análisis específicamente de: IDS-WAZHU, SIEM-SPLUNK, NGF PALO ALTO, FIREWALL-SHOREWALL.

Es importante indicar que en el mercado existen una variedad de herramientas que realizan las funciones antes indicadas por lo tanto se propone realizar una comparativa sobre ventajas y desventajas al usar software libre o bajo licencias; y también se propone definir los requisitos en base a los conocimientos que se deben adquirir para poder administrar estas herramientas (Riola, 2022)

2.1 Fundamentos teóricos aplicados

Intrusion Detection System (IDS)

Según Cózar (2020) Sistema de Detección de Intrusos permite detectar algunos eventos que son considerados como sospechosos o inapropiados para los sistemas informáticos; esta detección puede realizarla de manera manual al verificar el tráfico de

paquetes datos en la red y los log´s o registros de los sistemas; esta herramienta realiza una detección automática de proceso de la información que se relaciona con vulnerabilidades.

Los Intrusion Detection System o detección de intrusiones IDS son aplicaciones que se usan para poder determinar accesos que no se encuentran autorizados a un sistema de información, un ordenador o a una red, en otras palabras, están en la capacidad de monitorizar el tráfico de datos entrante y lo correlacionan con una serie grupos de datos almacenados que se encuentra actualizada de firmas de ataque que son conocidas.

Ante los diferentes tipos de actividades que resultan sospechosas, este sistema emite una prevención de alerta a los administradores del sistema de seguridad, quienes están en la capacidad de tomar acciones o correcciones oportunas.

Estas alarmas accesos pueden ser considerados como ataques que son esporádicos realizados por usuarios con mala intención o repetidos cada determinado momento, y son realizados con herramientas automáticas. Estos IDS´s sólo tienen la capacidad de detectar múltiples accesos que resultan sospechosos y suelen emitir alertas para anticiparse a posibles intrusiones o intentos de penetración a los sistemas; pero no tratan de mitigar la intrusión, su actuación es reactiva.

IDS bajo software libre

Según Mahecha (2022), los sistemas IDS bajo software libre en un inicio puede cubrir en parte lo que se refiere al proceso de recolección de eventos; también este sistema en lo posible como un nivel inicial, puede ser mejorado y adaptado a las necesidades institucionales y pues también es una para problemas de asignación de presupuestos pequeños al que muchas empresas pequeñas y medianas se enfrentan diariamente.

IDS con licencia

Los sistemas IDS bajo licencias tienen características más avanzadas que facilita la gestión y por otro lado el soporte que brindan, son las diferencias básicas que hacen que las soluciones pagadas o con subscripción se diferencien de las que son bajo software libre; las actualizaciones en firmas comerciales de amenazas son inmediatas.

Security Information Event Management (SIEM)

Los SIEM son herramientas que poseen la capacidad de correlacionar, concentrar y gestionar los eventos o registros de los sistemas o dispositivos el cual hace posible la detección de patrones que pueden significar algún tipo de incidente de seguridad (Contreras, 2020)

Un SIEM, o correlacionador de eventos de seguridad no puede faltar y siempre debe estar presente en un SOC; la finalidad es realizar un análisis de esta herramienta como correlacionador de eventos de seguridad SIEM, con la finalidad de detectar rápidamente las amenazas y eventos maliciosos frente a posible ataques o reportes de seguridad. Esta acción resulta muy significativa como resultado del aumento de millones de procesos que tienen los sistemas y (Fortra, 2018), la automatización de millones de procesos de datos y la imperativa necesidad de fomentar las normas que se encuentran vigentes para su cumplimiento.

SIEM bajo software libre

Según Fortra (2018), los sistemas SIEM de código abierto pueden proporcionar una funcionalidad o utilidad específicamente básica que puede resultar ideal para empresas pequeñas que inician sus operaciones y están comenzando a analizar los eventos de los sistemas de protección y seguridad. Pero con el paso inexorable del tiempo, muchos analistas de un SOC afirman que el software de un SIEM de código abierto requiere demasiado trabajo manual, de tal manera deja de ser una opción viable para poder mantenerlo y a medida que la empresa va creciendo; ocurre que las organizaciones ya sean públicas o privadas crecen más de lo que su solución en código abierto las puede acompañar en la línea de tiempo.

SIEM con licencia

En la misma proporción que la tecnología ha venido evolucionando, los sistemas SIEM se han convirtieron en herramientas o software bajo soporte o con licencias y están dirigidos a grandes empresas. Estas soluciones poseen características avanzadas interesantes, pero la complejidad que conlleva la implementación y el soporte o mantenimiento que conlleva, suelen ser proyectos inviables para empresas más pequeñas.

Firewall bajo software libre

Según Osvaldo (2020), es un sistema que se puede ubicar entre dos redes puede ser la red privada u organización y el internet y, que puede aplicarse o establecer una política de seguridad a través de una regla definida.

Next Generation Firewall NGF bajo licencia

Firewall de próxima generación, son equipos appliance de última tecnología, que en el ámbito de las aplicaciones, usuarios y contenidos permiten analizar los paquetes de datos, protocolos de comunicación, y el tráfico de entrada o salida y que pasa por los puertos de este equipo; realiza un análisis para detectar el comportamiento adecuado de los equipos finales que forman parte de la infraestructura de networking (Palo Alto, s.f.)

Los NGF son específicamente un cortafuego o firewall que tiene incorporado algunas funcionalidades adicionales de seguridad como son herramientas de antivirus, antispam, antispyware, sistemas de detección de intrusos, entre otras soluciones que actúan en el ámbito de seguridad y permiten minimizar y detectar riesgos, amenazas o vulnerabilidades.

2.2 Descripción de la propuesta

Al realizar el estudio de funcionalidad de las herramientas de seguridad instaladas en el Security Information Center, se realiza las respectivas tablas comparativas entre funcionalidades de las herramientas de un SOC (Tabla 1) se plantea la funcionalidad de herramientas de un SOC, (Tabla 2) se plantean ventajas/desventajas del uso de las herramientas que se encuentran bajo software libre y software con licencia, (Tabla 3) se plantean desventajas de las herramientas que se encuentran bajo software libre y software con licencia, (Tabla 4) se plantean ventajas/desventajas de un IDS, (Tabla 5) se plantean ventajas /desventajas de un SIEM; llegando a la conclusión que las herramientas en mención son importantes para realizar una respuesta inmediata de incidentes informáticos y poder detectar vulnerabilidades y amenazas en la infraestructura crítica de la institución.

También se considera que para el uso de software libre o bajo licencias es muy importante considerar el alcance del proyecto, análisis presupuestario, número de usuarios, tamaño de la organización; sin duda los dos tipos de tecnologías son valederas, pero todo dependerá del análisis antes mencionado.

Tabla 1

Funcionalidad de herramientas de un SOC

Tipos	Funcionalidad
IDS	Sistema que detecta intrusiones o accesos a los sistemas que no están autorizados, se activa una alerta hacia que una alerta a los administradores quienes amenaza o vulnerabilidad.
SIEM	Herramienta de gestión de son los encargados de tomas medidas oportunas ente cualquier eventos y logs de archivos de seguridad, gestiona el análisis de correlación de eventos en tiempo real de los diferentes tipos de alertas generadas por los distintos sistemas.
NGF	Next Generation Firewall, firewall de próxima generación, equipos appliance de última tecnología, que ofrecen un nivel más profundo de seguridad; el ámbito de las aplicaciones, usuarios y contenidos

	permiten analizar los paquetes de datos, protocolos de comunicación, y el tráfico de entrada o salida y que pasa por los puertos de este equipo Es un sistema que se puede ubicar entre dos redes puede ser la red privada u organización y el internet y, que puede aplicarse o establecer una política de seguridad a través de una regla definida.
Firewall	

Fuente: Desarrollo propio basado en varios autores

Tabla 2

Ventajas del uso de software libre y uso de software con licencia

Ventajas	
Software libre	**Software con licencia**
Bajo costo de adquisición y libre uso, es importante para muchas empresas mantener costos bajos, de lo contrario se ve impedido a cumplir sus metas.	Ofrecen gran variedad de funcionalidades cuya característica está dada en un modelo de compra/venta de licencias
Innovación tecnológica, su objetivo es compartir la información trabajando de manera cooperativa. Requisitos de hardware menores y durabilidad de las soluciones	Es un software que es de propiedad de un individuo o empresa. Existen restricciones de su uso de acuerdo a la licencia y su código fuente.
Independencia del proveedor, el software libre garantiza independencia con respecto a los canales de proveedores debido a que se tiene la disponibilidad del código fuente	Control de calidad, las empresas de software propietario poseen estos controles para mejorar su producto. Recursos de investigación, se destinan recursos para la investigación de su producto. Software para servicios que son muy específicos que no se encuentra en ningún otro lado, solamente lo tiene la empresa que lo produce.

Fuente: Desarrollo propio basado en varios autores

Tabla 3

Desventajas del uso de software libre y uso software con licencia

Desventajas	
Software libre	**Software con licencia**
La curva de aprendizaje es mayor, generalmente se tarda más en aprender a usar un software libre	Cursos de aprendizaje costosos, resulta complicado aprender a utilizar sin haber tenido experiencia o tener cursos de capacitación que resultan costosos.
Las herramientas basadas en software gratuito no poseen garantía del fabricante, proviene del autor	Secreto y confidencialidad en el desarrollo del código fuente, es un secreto que se guarda en secreto por la empresa que lo produce.
Es necesario utilizar múltiples recursos sean estos de hardware, software, o recurso humano para la reparación de errores.	Derecho exclusivo de innovación por parte la empresa fabricante
Las versiones de paquetes y archivos gráficos de usuario y de multimedia se están estabilizando	Ilegalidad de copias del software sin licencia para el efecto, sin haber realizado la contratación de licencias necesarias.
La mayor parte de la configuración software libre no es intuitiva	Imposibilidad de compartir el software con otras dependencias.
El usuario debe tener nociones sobre herramientas bajo software libre y también sistemas operativos.	Dependencia a canales de proveedores, y en muchas ocasiones se depende hasta de un solo canal
La curva de aprendizaje es mayor, generalmente se tarda mucho más tiempo en tener conocimiento, experiencia y aprender a usar las herramientas, conjuntamente con los programas o herramientas bajo software libre	
El software libre con sus programas no posee garantía alguna, proviene específicamente del autor	
Es necesario utilizar recursos a la reparación de errores.	

Fuente: Desarrollo propio basado en varios autores

Tabla 4.

Ventajas y desventajas de un IDS

IDS	
Ventajas	**Desventajas**
La herramienta IDS permite visualizar los logs de los eventos de la red en tiempo real en base a la información recopilada	No se encuentran configuradas para realizar una prevención o detener ataques que se pueda detectar
Sistematiza los patrones lógicos de búsqueda en los grupos de paquetes de datos que son enviados al sistema correlacionador	Son completamente vulnerables a los ataques y vulnerabilidades de DDos, que provoca la inoperatividad de la herramienta
Proporciona reglas en sus eventos que informan al administrador los diferentes tipos de ataques y vulnerabilidades	
Detecta diferentes tipos de vulnerabilidades	
Posee una estructura centralizada o descentralizada	
Mucha documentación en la web que se encuentra actualizada	

Fuente: (Cózar, 2020), se respeta el derecho de Autor

Tabla 5.

Ventajas y desventajas de un SIEM

SIEM	
Ventajas	**Desventajas**
Un solo punto de centralización de la correlación de información y eventos	Altos costos de implementación.
Otorga un punto de referencia en común para las alertas de os sistemas	Con respecto al conocimiento el aprendizaje es extenso al formar personal capacitado propio solo para esta tarea
Permite automatizar las tareas, por tal razón y en consecuencia hay ahorro de tiempo y costes	Integración limitada con el resto del sistema.
Se puede realizar por parte de administrador un completo seguimiento de los eventos para detectar anomalías o vulnerabilidades de seguridad	Al ampliar las tareas que realiza el sistema se experimenta una pérdida de control de la información que se ha generado o un acceso limitado con latencia a determinada

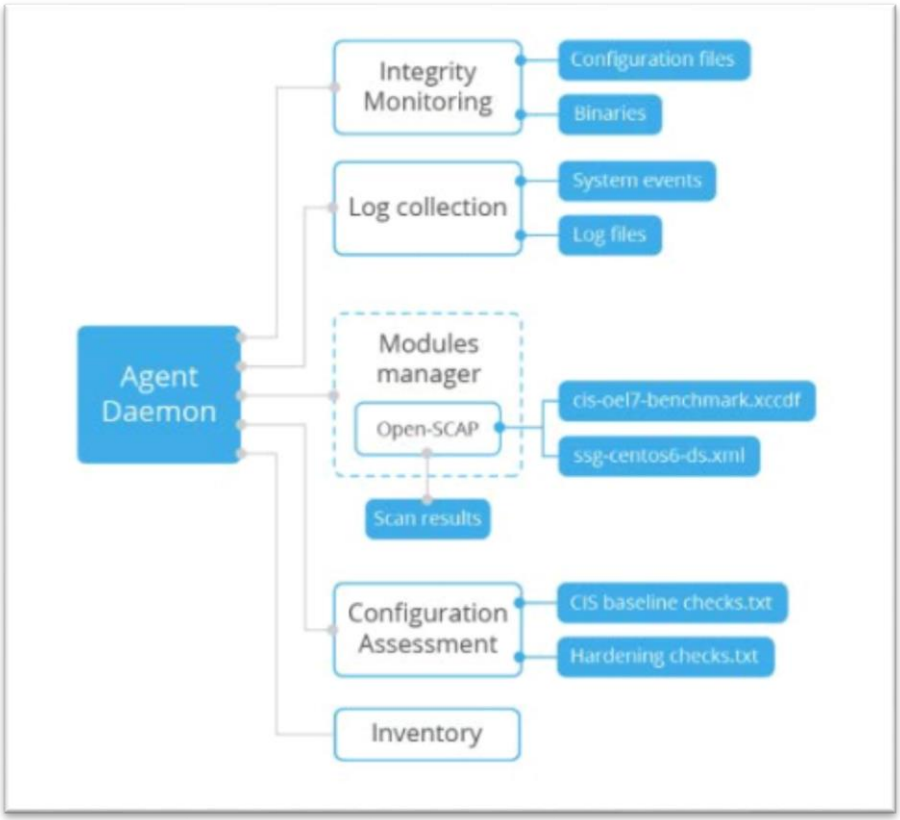
Visualización de datos históricos alo largo del tiempo. Muestra al administrador la existencia de vulnerabilidades	información y una fatiga por la alta recepción de notificaciones.

Fuente: (INCIBE, 2023), se respeta el derecho de autor

a. Estructura general

Figura 1.

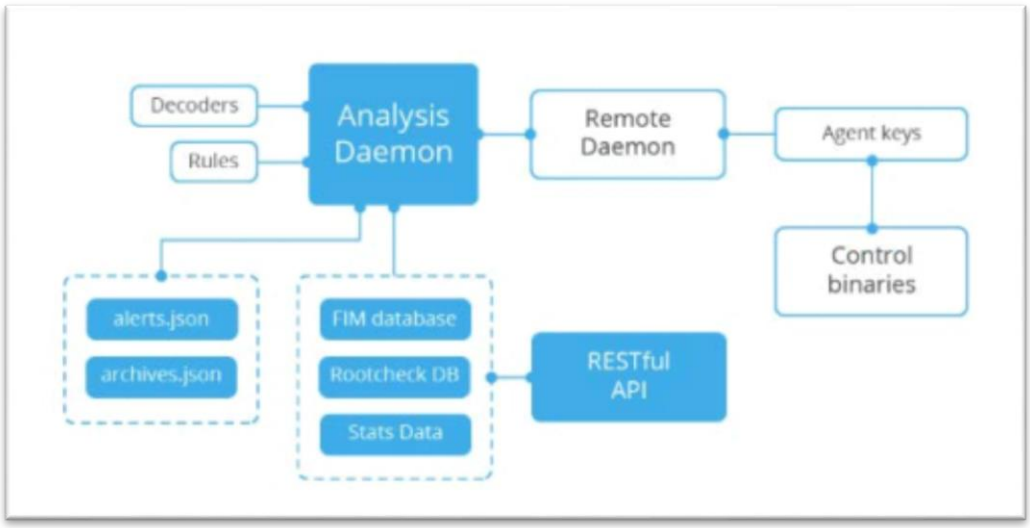
Estructura del agente-Wazuh



Nota: Cózar (2020)

Figura 2.

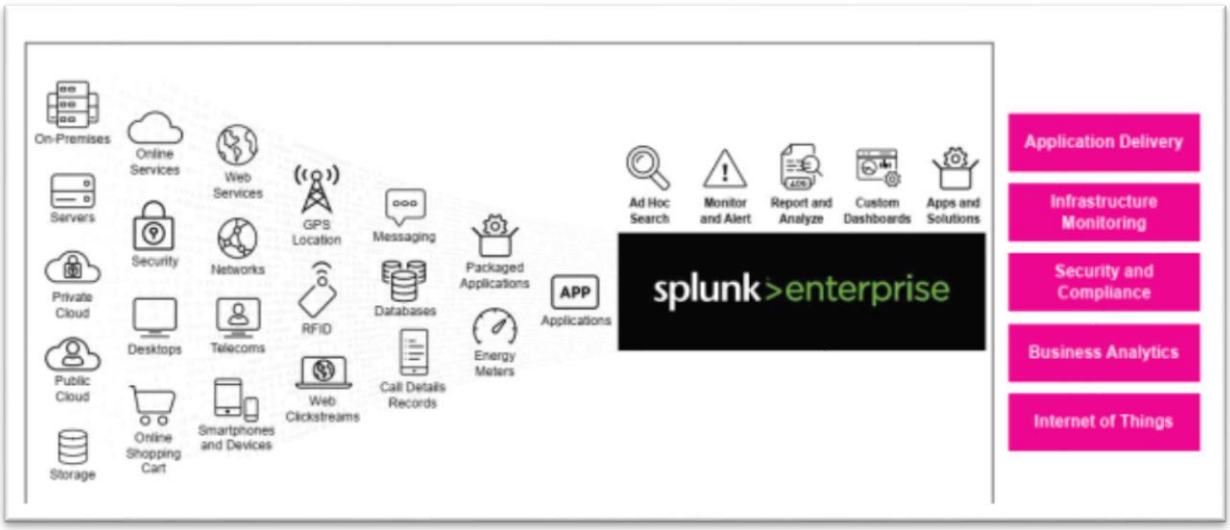
Estructura del server-Wazuh



Nota: Cózar (2020)

Figura 3.

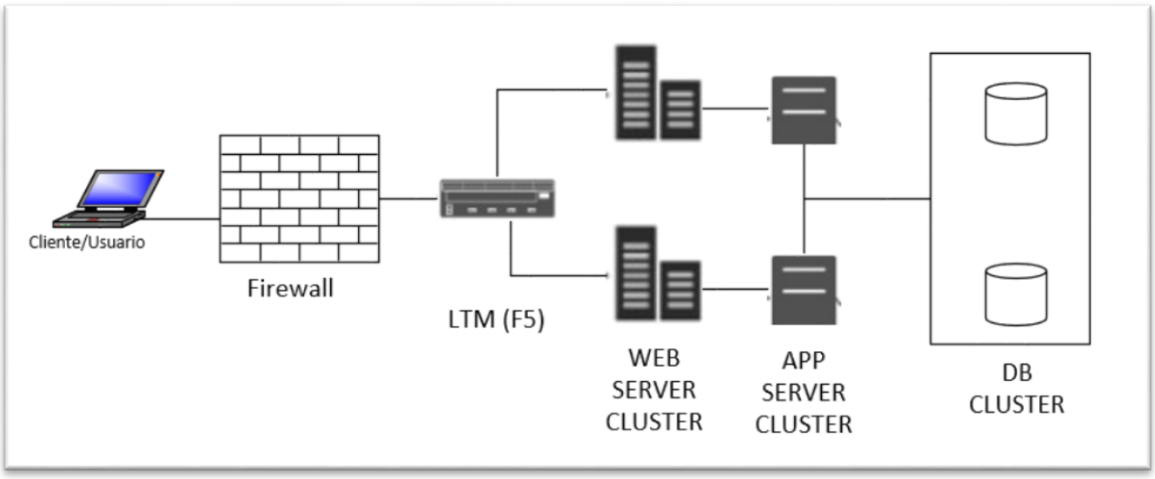
Estructura de un sistema splunk



Nota: Hidalgo (2023)

Figura 4.

Estructura de un firewall



Nota: Cedeño (2020)

b. Explicación del aporte

Al revisar la imagen de figura (1) se observa la infraestructura del agente wazuh, en lo que respecta la figura (2) que corresponde a la estructura del servidor de wazuh, en la figura (3) se aprecia la conformación de la estructura del sistema splunk y el última figura de observa la estructura de un firewall; tomando en cuenta las funcionalidades de estas herramientas que son viables para un SOC; del igual manera en la figura se puede observar las múltiples ventajas/desventajas del uso de software libre y de softwares bajo licencia.

c. Estrategias o técnicas

En el desarrollo se utilizó técnicas y análisis en base a los conceptos ya conocidos y desarrollados por otros trabajos de investigación, sin embargo, al realizar referencias a herramientas de seguridad que son de empresas privadas, se tomó como referencia las especificaciones que describen en los brochure, manuales de administración, sitios web entre otras.

2.3 Validación de la propuesta

IDS– Wazhu

Wazuh es un programa informático que realiza análisis de seguridad y permite analizar, recolectar, agregar e indexar datos para realizar la detección de amenazas, intrusiones o comportamientos extraños o anómalos.

Análisis IDS-Wazuh

Se eligió que esta herramienta Wazuh forme parte del SOC por estas razones:

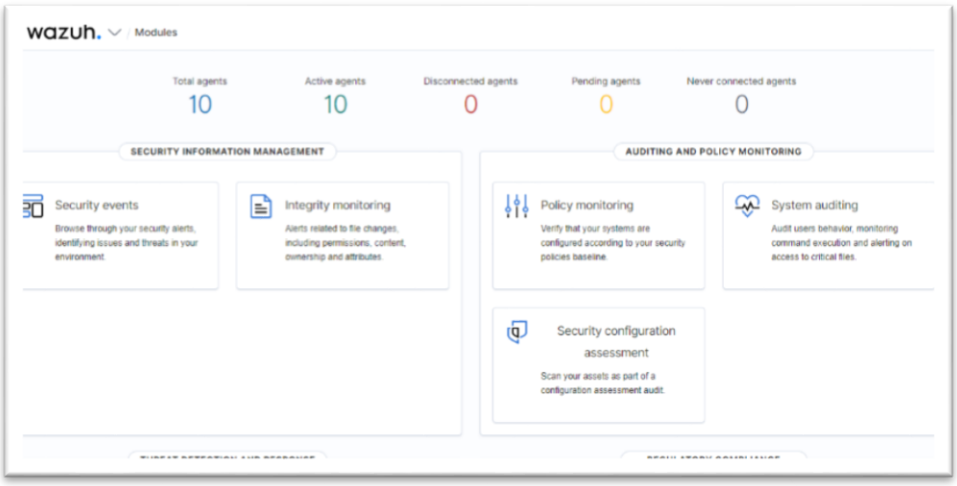
- Es una herramienta de código abierto, que previene, detecta y da respuesta a amenazas.
- No es un sistema limitado, ya que con su agente se monitorea sus activos con mayor riesgo
- Fácilmente escalable, y se paga solo por soporte
- Ofrece el cumplimiento de los controles o normativas relacionados con la seguridad para el cumplimiento de las mismas
- Tiene un agente que se instala en los puntos supervisados
- Tiene un motor de búsqueda y analítica avanzada Elastick Stack

Wazuh proporciona las siguientes características:

- **Análisis de Seguridad:** Esta herramienta analiza los datos de seguridad y detecta intrusiones o amenazas
- **Detección de intrusos:** Los agentes de esta herramienta wazuh realizan un scanner de los sistemas monitorizados para detectar malware, rootkits o archivos anómalos sospechosos, cabe indicar que pueden encontrar datos y procesos que no se observan, protocolos de networking en escucha que no se encuentran registrados y diferentes respuestas a peticiones de los procesos del sistema.
- **Análisis de datos de logs:** La función de agente de dicha herramienta Wazuh es muy importante, dan lectura a los registros de los archivos de las programas o sistemas del SO y luego se transmiten de manera segura al server principal y guardarlos para poder realizar un análisis basado en reglas; las mismas que reflejan si los sistemas o aplicaciones tienen algún tipo de errores o falencias en la configuración, registros de vulnerabilidades o logran su cometido en actividades de vulnerabilidad, incumplimientos de políticas de seguridad o algún otro tipo de problemas de seguridad.

Figura 5.

Características de los módulos de wazuh

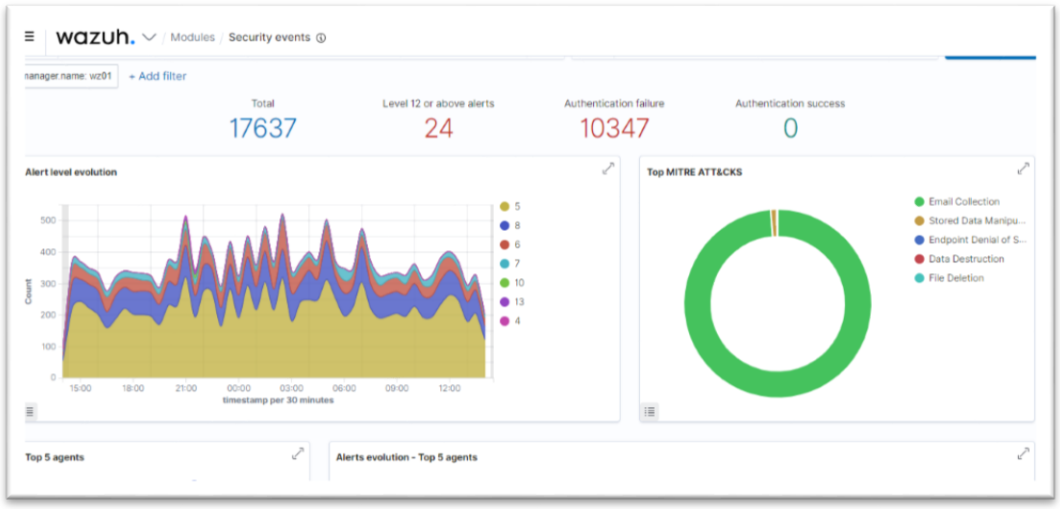


Nota: *Imagen propia de wazuh institucional*

- **Monitorización de la integridad de los archivos:** Monitorea los archivos del sistema y posee la capacidad de identificar algún tipo de cambio en el contexto del contenido, algún tipo de permisos, el dueño del fichero y atributos. Puede identificar de forma nativa o selectiva los usuarios, aplicaciones o sistemas que están siendo utilizados.
- **Detección de Vulnerabilidades:** Estos agentes que se instalan en los equipos o sistemas que se desean monitorear envían la información del software hacia el server, a su vez se correlaciona o verifican el proceso de bases de datos donde muestra las vulnerabilidades comunes que diariamente se actualizan, para identificar el archivo o programa vulnerable conocido. El avance de las vulnerabilidades de forma automática ayuda gestionar y recuperar los puntos vulnerables en los activos que resultan críticos y se utilizan para tomar acciones pertinentes y correctivas que son necesarias antes de que sean vulneradas o explotadas por los atacantes.

Figura 6.

Eventos de seguridad wazuh



Nota: Imagen propia de wazuh institucional

- **Respuesta a incidentes:** Esta herramienta realiza un monitoreo del sistema y de la configuración de sus servicios para verificar que se están cumpliendo con los estándares de seguridad y políticas básicas. Los agentes realizan escaneos en algunas ocasiones para detectar las aplicaciones que son vulnerables, o no se encuentran con los últimos parches o configuradas de forma insegura.
- **Cumplimiento normativo:** Wazuh cumple con algunos controles de seguridad que son de gran importancia para poder cumplir con los diferentes estándares y normativas.
- **Monitorización de la seguridad en la nube:** Wazuh colabora en el monitoreo de la infraestructura de información en la infraestructura de nube como amazom, AWS, azure y google cloud.
- **Seguridad en contenedores:** Proporciona monitoreo de la seguridad en los equipos y configuración en contenedores con tecnología Docker; verifican su estadística relacionada con el comportamiento y detectan amenazas vulnerabilidades.

Componentes de Wazuh

Wazuh se ha convertido en una herramienta integral, en la cual se observan tres componentes necesarios y principales como: OSSEC HIDS, Open SCAP, Elastic-Stack

OSSEC HIDS: Es un sistema (Open Source Host Intrusion Detection Sytem) de detección de intrusos HIDS cuya función es la de detectar, visualizar y monitorear las correlaciones de múltiples eventos de seguridad. Se describe un agente multiplataforma que

transmiten datos del sistema que son mensajes de logs o registro, hashes de ficheros y anomalías detectadas a un gestor centralizado, para posterior a esto, los datos se analizan y procesa, y da como resultado las alertas de seguridad.

OpenSCAP: Es un intérprete de ordenes o comandos que se utiliza para revisar las configuraciones del sistema de archivos y detectar sistemas o servicios vulnerables; está diseñada para el cumplimiento de estándares de seguridad.

Elastic Stack: Es una herramienta que se encuentra formado Filebeat, Elasticsearch y Kibana que utiliza para recolectar, igualar, indexar, almacenar, rastrear y mostrar datos de registros de archivos del sistema y proporciona un entorno gráfico web, mediante control de los eventos que permite realizar análisis avanzados.

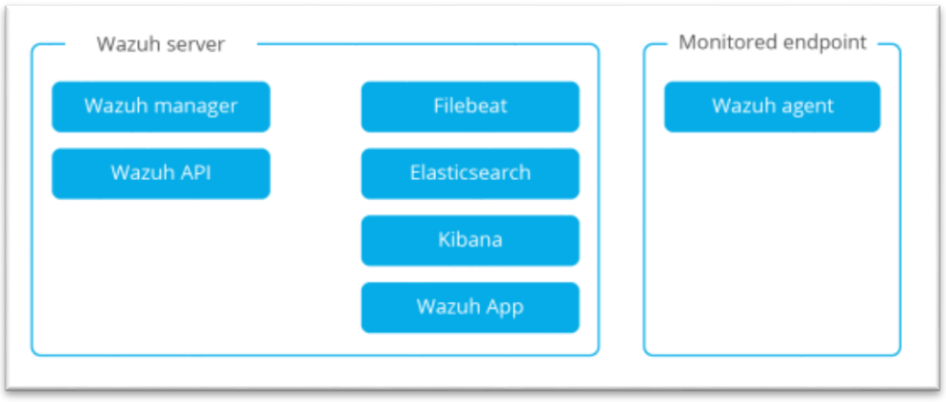
Arquitectura de Wazuh

Esta herramienta posee dos componentes centrales y que son principales a instalar: el manager de Wazuh y Elastic Stack; por esta razón hace que esta herramienta permita dos tipos de arquitectura:

Arquitectura centralizada: Se instalan en el server de Wazuh y Elastic Stack uno o más servers en diferentes sistemas.

Figura 7.

Arquitectura centralizada de la herramienta Wazuh

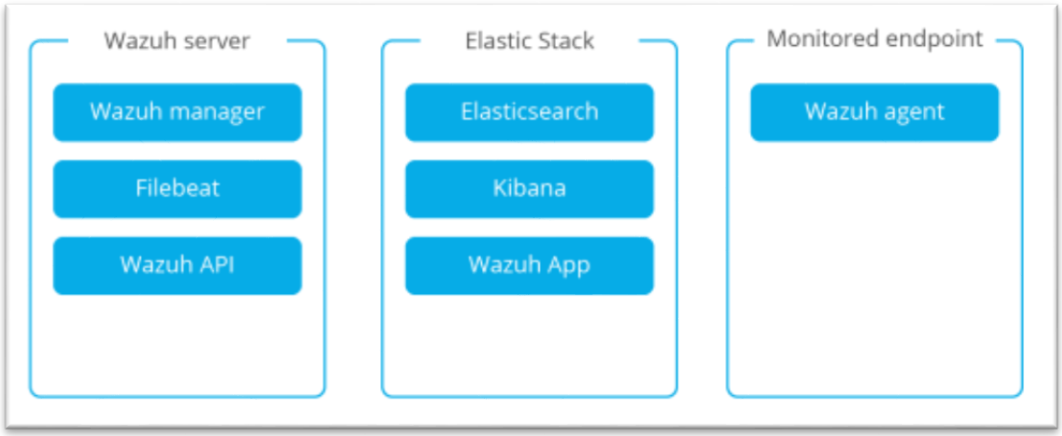


Fuente: (Cózar, 2020), se respeta derechos de Autor

Arquitectura distribuida: Se instalan en el server de esta herramienta Wazuh y el cluster de Elastic Stack (uno o más servers) en diferentes sistemas.

Figura 8.

Arquitectura distribuida Wazuh



Nota:: Cózar (2020)

Análisis SIEM-SPLUNK

Según Hidalgo (2023), Splunk está compuesto de una infraestructura de ingesta y análisis de procesos de millones de datos que almacena muchos caracteres en grupos de información indexada, para posterior ser consultada a través del lenguaje de comuniación Search Language Processing.

Según Pastor (2022), Splunk es un SIEM que integra la información y permite detectar y responder de manera inmediata a los ataques tanto de usuarios internos como externos y reduce la gestión de las múltiples amenazas minimizando el riesgo. Colabora para que los equipos obtengan visibilidad e inteligencia de seguridad, permite supervisar continuamente, la respuesta a incidentes informáticos, y las operaciones del SOC.

Splunk posee una plataforma donde almacena y visualiza los datos que utiliza índices de información y no base de datos la misma que permite almacenar accede a los datos que se guardan en la infraestructura de splunk.

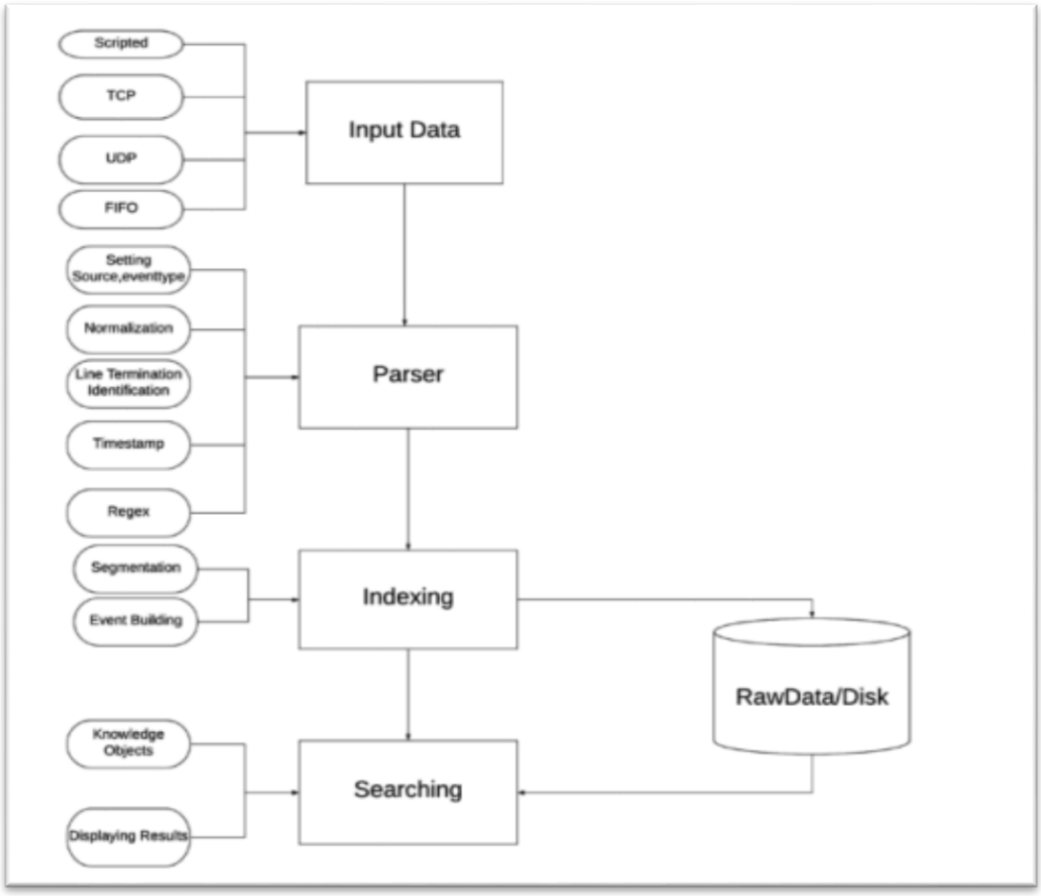
El ciclo de permanencia que se relaciona con la vida de los datos en esta herramienta inicia por la fase de ingesta, en la que con diferentes protocolos de comunicación sobre los ficheros en el SO se recopilan diferentes grupos de datos, en la siguiente fase se otorga a los datos recibidos, de una infraestructura específica para las tipologías de eventos

La siguiente fase es el almacenamiento de los datos y se realizan grupos de los eventos indexados en el disco, los mismos que se forman algunos tipos diferentes de grupos y que van en función del tiempo de acceso al grupo de información.

Por último, la etapa final del ciclo es la etapa de búsqueda en la cual se realiza las consultas respectivas de los datos en relación a las estructuras creadas de los tipos de los eventos.

Figura 9.

Ciclo de vida de eventos de Splunk



Fuente: Hidalgo (2023) se respeta derechos de Autor

Splunk puede desempeñarse como uno, varios o todos los roles que son indispensables para realizar la ejecución de las etapas de los eventos de seguridad, los roles más importantes de Splunk son:

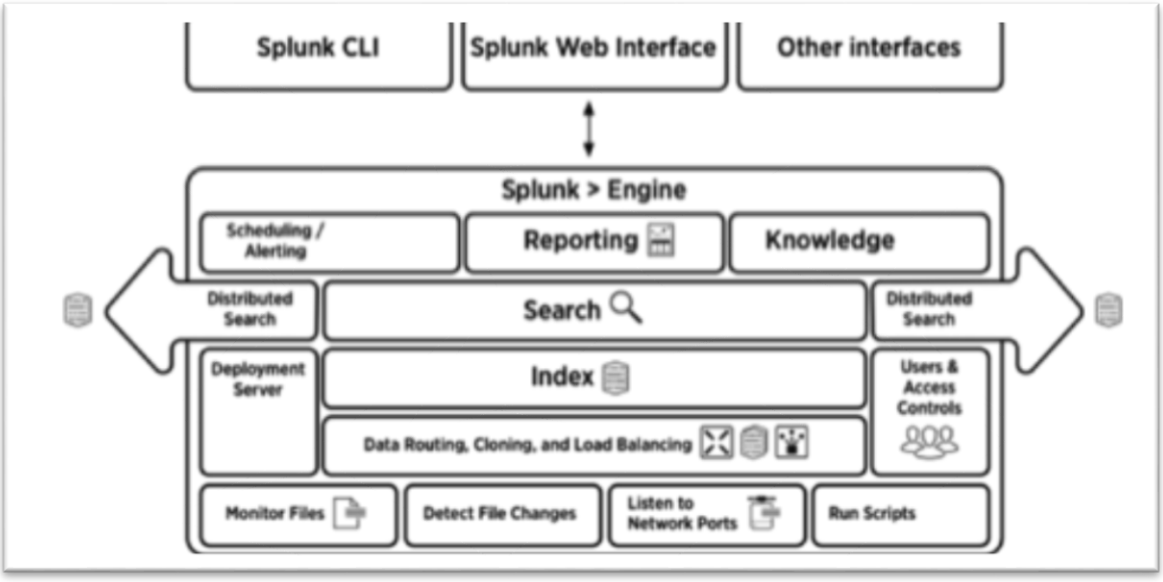
Arquitectura de Splunk

Splunk posee una arquitectura interna que permite tener sus funcionalidades distribuidas, de esta manera permite separar las capas que conforman el sistema, es importante indicar como esta herramienta transforma los datos en eventos, este procesamiento lo realizan el servidor que tiene el rol de Indexer, para cada grupo de procesamiento de datos se encargada de comprimir estos datos en crudo y crea índices direccionando a los datos y ficheros de metadatos, los índices son punteros de cada uno de los términos que aparecen.

La instalación, configuración e implementación de Splunk que es una gran solución o herramienta, ya que a través del almacenamiento de los índices conjuntamente con el grupo de datos realiza búsquedas de manera rápidas en gran volumen de datos, debido a que cada índice se guarda en un grupo de datos en crudo para realizar la búsqueda, la capacidad de proceso es entregada entre la diversidad de elementos donde se almacena la información.

Figura 10.

Arquitectura de Splunk



Fuente: (Hidalgo, 2023), se respeta derechos de Autor

La ventaja principal que se puede observar en esta arquitectura está en poder desplegar todas las capacidades ofrecidas en un único nodo y partiendo de esto se podrán configurar varios nodos para elegir roles diferenciados en el caso de despliegues más complejos.

Elastic Stack Elastic Stack

Es un conjunto de herramientas tecnológicas que ejercen su funcionalidad en la ingesta de datos, almacenamiento y localización sobre grandes cantidades de datos, los principales sistemas que forman parte de Elastic Stack son:

Logstash es un motor recolección de datos cuya función es la de realizar la ingesta, transformación y normalización de todos los datos previos a ser almacenados, entre sus cualidades este motor se caracteriza por la amplitud de integraciones con diferentes tecnologías.

Elastic Search es un motor de búsqueda y analítica cuya función principal es la de almacenar todo el conjunto de datos, así como su consulta, tiene similitud en el proyecto de software libre Apache Lucene

Kibana es el programa web que interactúa como interfaz de usuario que permite visualizar los datos de elasticksearch y navegar en el elastic stack, actuando como punto de unión entre las mismas.

Hadoop Distributed File System (HDFS)

Según Hidalgo (2023) es el componente principal de un sistema HADOOP, que consta de un sistema de ficheros distribuido y permite almacenar grandes cantidades de datos tanto de logs normalizados como de logs sin normalizar; entre las principales ventajas que tiene este sistema está en la replicación de los datos indexados y por tanto existe tolerancia a fallos, así como también la gran escalabilidad horizontal.

HDFS tiene una capa lógica de abstracción que permite a cualquier programa o aplicativo pueda acceder a los datos almacenados en cualquier lugar donde se encuentren, esta tecnología funciona con la división de la información en bloques y distribuidos a través de los nodos que conforman el clúster.

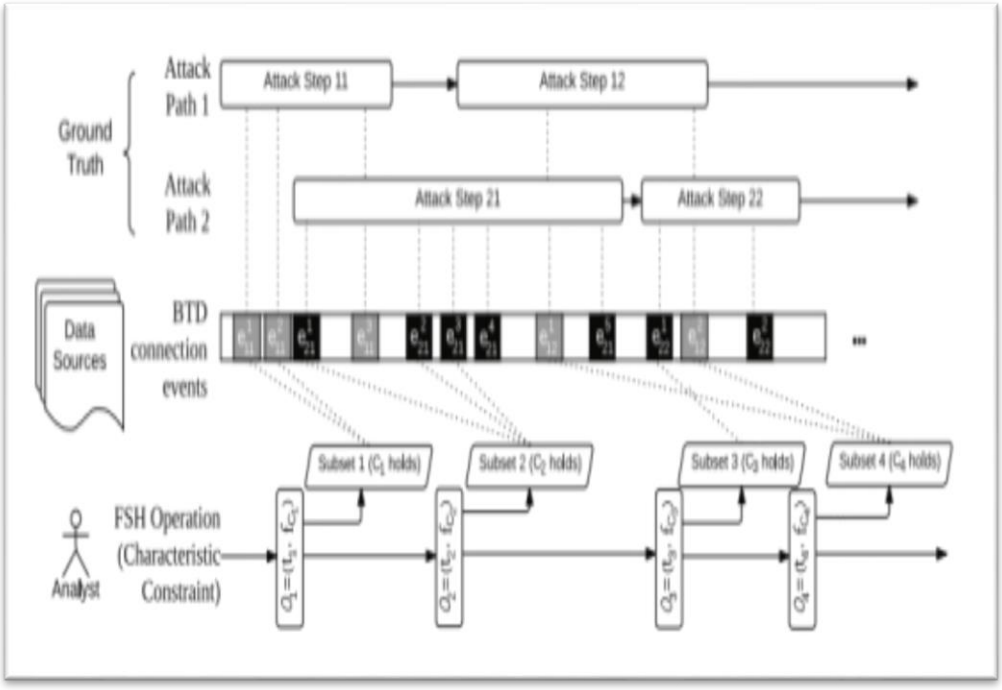
Investigación de métodos de detección de amenazas

Reglas de Correlación

Las reglas de correlación de datos están formadas por expresiones lógicas que generan acciones o eventos definidos, las reglas de correlación son llevadas a cabo por búsquedas mediante el tipo de lenguaje inherente que le corresponde a cada tecnología, un patrón de ataque está comienza con una serie de pasos donde cada uno de ellos sigue un orden

Figura 11

Regla de correlación de eventos



Fuente: (Hidalgo, 2023), se respeta derechos de Autor

En resumen, las reglas definidas poseen claras ventajas en varios supuestos como la detección de amenazas ya conocidas, en la cual los patrones de eventos de cualquier tipo de ataques son conocidos y de acuerdo al analista de seguridad pueden ser trasladados a lógicas de detección.

Análisis – NGF-Palo Alto

De acuerdo lo que manifiesta (Alto, 2022), muchos cambios se ha dado en la mayoría de aplicaciones y al mismo tiempo las amenazas han evolucionado, la respuesta sobre la conducta del usuario, y la infraestructura de enlaces tradicional de la redes internas o externas, han transformado la seguridad que se había mantenido de manera tradicional que desde un inicio han realizado los firewalls tradicionales que su tecnología era en puertos o filtros de red. En todo momento en el ambiente cotidiano laboral los usuarios acceden a un sin número de aplicadores conjuntamente con una gama de dispositivos. La expansión de los data center, virtualización, y herramientas basadas en la nube, ha rediseñado las autorizaciones de acceso hacia las aplicaciones sin que esto pueda interrumpir a la protección de la red.

Capacidades de NGF

• **Identificación de aplicaciones, no de puertos:** Los NGF clasifican el tráfico de datos tan pronto como llega al firewall y es capaz de identificar el identificativo de la aplicación,

indistintamente del puerto o protocolo de comunicaciones. Son asumidas por esa identidad única como principios base de todo el sin número de políticas que se enmarcan a la seguridad.

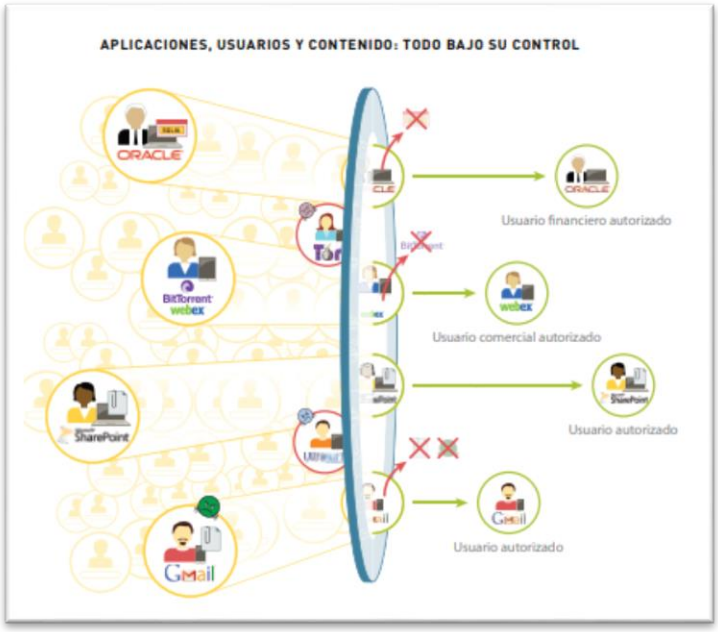
• **Vinculación de la aplicación a la identidad del user:** No está direccionada a la dirección con protocolo IP, no importa la ubicación o del dispositivo**,** es la información del usuario, grupos, directorios, para implementar políticas de habilitación que debe ser razonables para todos los usuarios, indistintamente de la ubicación o del sitio del dispositivo.

• **Prevención de todas las amenazas:** Tanto conocidas como desconocidas**,** previene y bloquea vulnerabilidades conocidas como: malware, exploit, spyware y sitios web o URL maliciosos realizando un análisis del tráfico y otorgando una protección dirigida y automática contra vulnerabilidades desconocidas o selectivas.

• **Simplificación de la administración de políticas.** Habilita de una manera segura las apps y reduce tareas administrativas gracias a herramientas gráficas, como la generación unificado de políticas, plantillas.

Figura 12.

Bloqueo de app, user y cont



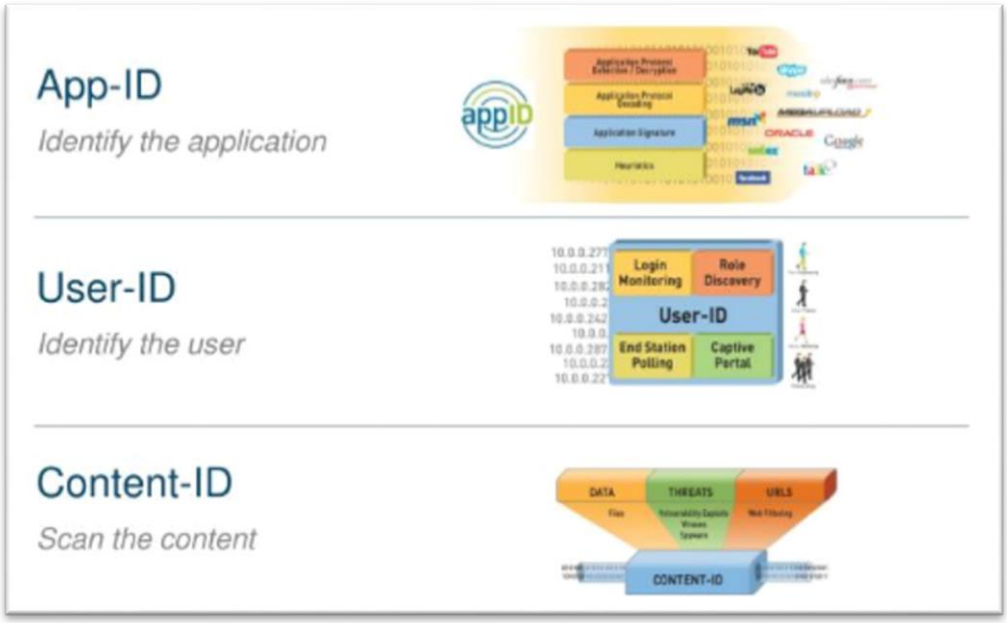
Fuente: (Palo Alto, s.f.), se respeta derechos de Autor

Protección de aplicaciones habilitadas

El acceso a diferentes aplicaciones de una manera segura y sin riesgo alguno es importante y de esta manera el implementar políticas que pueden específicas o generales que permite bloquear archivos maliciosos conocidas o desconocidas; permitir la transferencia de archivos y la actividad de la navegación web se introduce la tecnología de App-ID.

Figura 13.

Bloqueo de app, user y cont

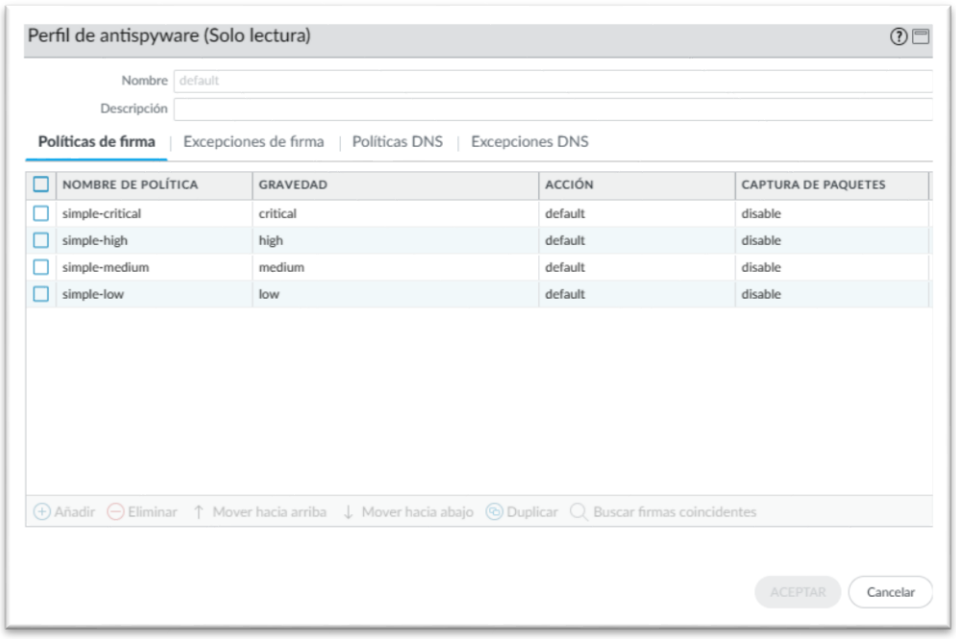


Fuente: (Palo Alto, s.f.), se respeta derechos de Autor

• **Bloqueo de amenazas conocidas:** Permite el bloqueo de direcciones IP, antivirus y anti-spyware de red debido a que posee un motor de búsqueda y exploración que se relacionan en flujos de datos y que protegen a la red de un sin número de amenazas y vulnerabilidades. El sistema de prevención de intrusiones (IPS) tiene sistemas que están activados contra exploits de amenazas, sobrecarga de búfer, ataques de denegación de servicio. La capa de seguridad de antivirus y anti-spyware que bloquea millones de variantes de malware, así como cualquier tráfico “command-and-control” generado por malware, virus en formato pdf y malware oculto en archivos que se encuentran comprimidos o tráfico web (comprimido HTTP/HTTPS).

Figura 14.

Ventana de amenazas antispyware en NGF Palo Alto

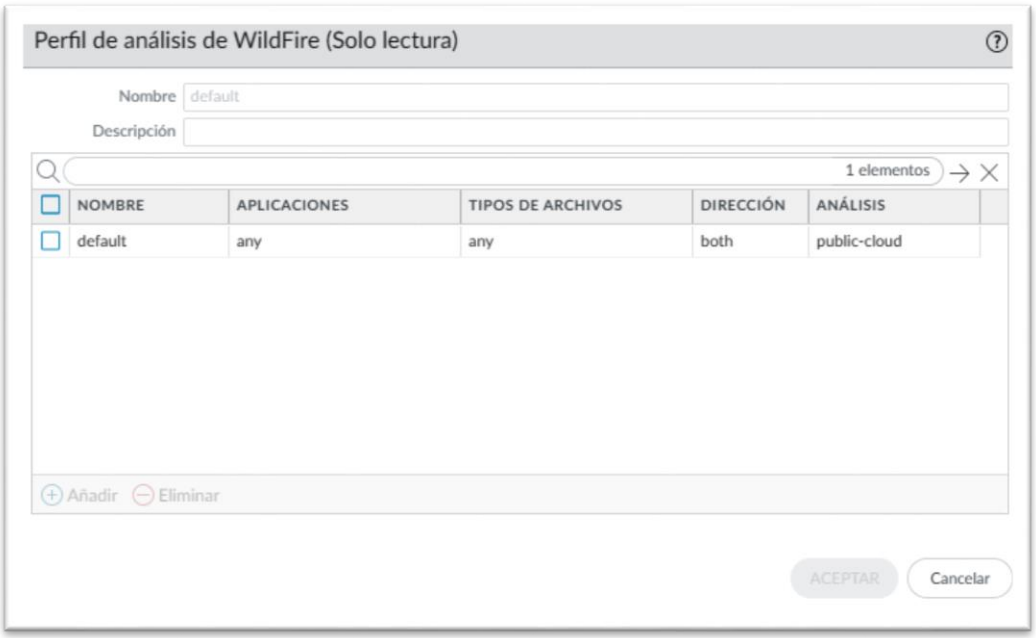


Fuente: server propio institucional Palo Alto 2023

• **Bloqueo de malware:** Wildfire es una potente herramienta que bloquea el malware desconocido o selectivo que es identificado y analizado por WildFire, que instantáneamente ejecuta y observa los archivos conocidos. WildFire verifica más de cien comportamientos maliciosos y el resultado se envía directamente al administrador en forma de alerta.

Figura 15.

Análisis de Wildfire

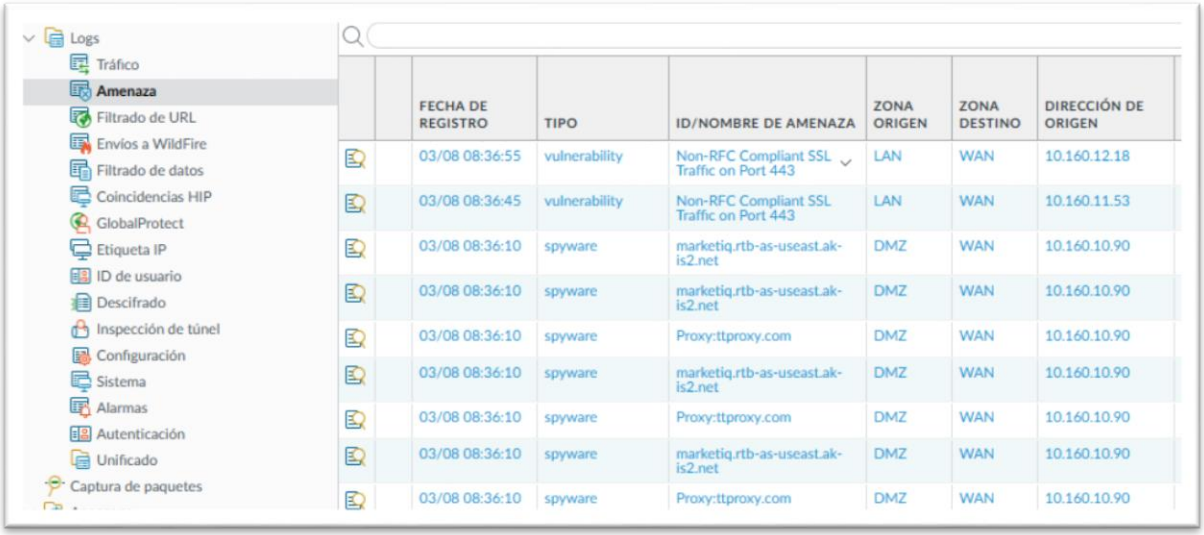


Fuente: server propio institucional Palo Alto 2023

• **Identificación de hosts infectados por bots.** App-ID tiene la capacidad de clasificar todas las aplicaciones, en todos los puertos de comunicación sean en TCP o UDP, incluido cualquier tráfico desconocido, que pueda indicar daños, anomalías o amenazas en su red. El informe de botnet que está relacionado en comportamiento de paquetes, relaciona el tráfico desconocido, las consultas de dominio de nombre y el sitio web sospechoso con varios comportamientos de red que son inusuales, para revelar dispositivos que probablemente estén infectados con malware. Los resultados se evidencian en una lista de hosts potencialmente infectados que podrían tratarse como posibles miembros de una botnet.

Figura 16.

Logs de host infectados



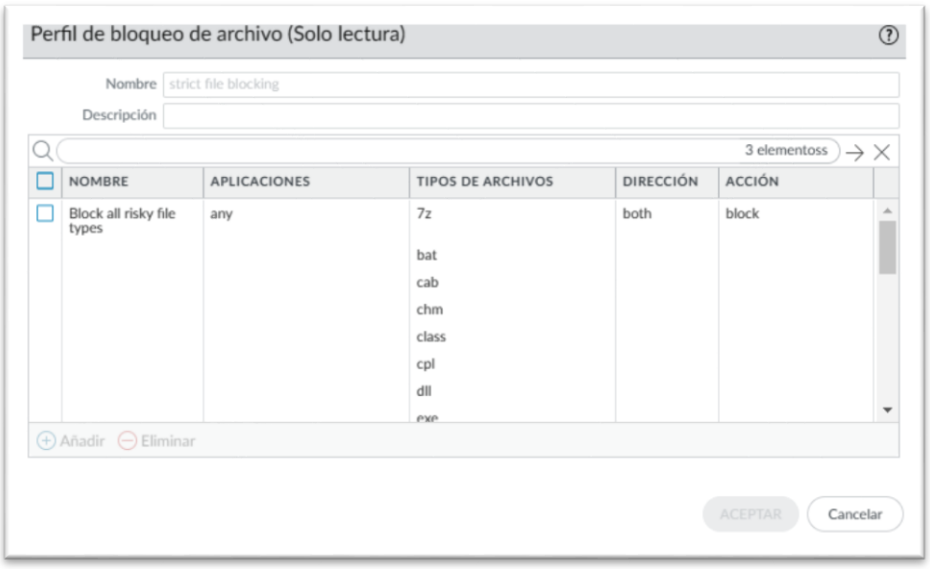
FECHA DE REGISTRO	TIPO	ID/NOMBRE DE AMENAZA	ZONA ORIGEN	ZONA DESTINO	DIRECCIÓN DE ORIGEN
03/08 08:36:55	vulnerability	Non-RFC Compliant SSL Traffic on Port 443	LAN	WAN	10.160.12.18
03/08 08:36:45	vulnerability	Non-RFC Compliant SSL Traffic on Port 443	LAN	WAN	10.160.11.53
03/08 08:36:10	spyware	marketiq.rtb-as-useast.ak-is2.net	DMZ	WAN	10.160.10.90
03/08 08:36:10	spyware	marketiq.rtb-as-useast.ak-is2.net	DMZ	WAN	10.160.10.90
03/08 08:36:10	spyware	Proxy:ttproxy.com	DMZ	WAN	10.160.10.90
03/08 08:36:10	spyware	marketiq.rtb-as-useast.ak-is2.net	DMZ	WAN	10.160.10.90
03/08 08:36:10	spyware	Proxy:ttproxy.com	DMZ	WAN	10.160.10.90
03/08 08:36:10	spyware	marketiq.rtb-as-useast.ak-is2.net	DMZ	WAN	10.160.10.90
03/08 08:36:10	spyware	Proxy:ttproxy.com	DMZ	WAN	10.160.10.90

Fuente: server propio institucional Palo Alto 2023

• **Limitación de transferencias de datos:** También se conocen como archivos no autorizados, que cumplen las funciones de filtrado de datos y permiten a los administradores de sistemas otorgar políticas que reduzcan los riesgos que tienen relación con las transferencias de archivos y datos no autorizadas. Los mismos que se pueden controlar explorando el interior del archivo en lugar de verificar la extensión del archivo, para determinar si se debe permitir la transferencia o no. Los archivos ejecutables, que se encuentran en descargas “drive-by download”, se pueden bloquear para dar protección a la red de la propagación de software malicioso oculto.

Figura 17.

Limitación de block de archivos

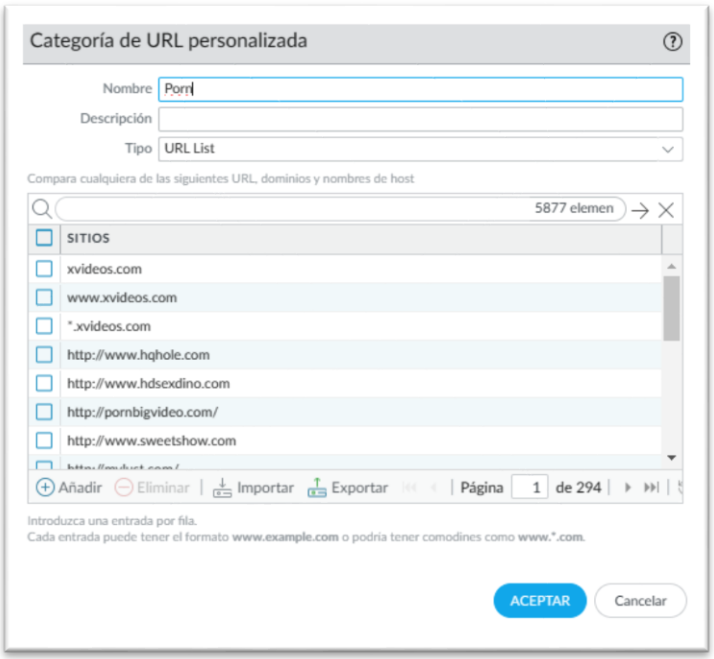


Fuente: server propio institucional Palo Alto 2023

• **Control de la navegación web.** Un motor de filtrado de sitios web o direcciones URL totalmente integrado permite a los administradores aplicar políticas micho más específicas de navegación por Internet, complementando la visibilidad de las aplicaciones y las políticas de control. Además, las categorías de URL se pueden integrar en las políticas para proporcionar una mayor granularidad en el control.

Figura 18.

Bloqueo de sitio web por categoría de URL

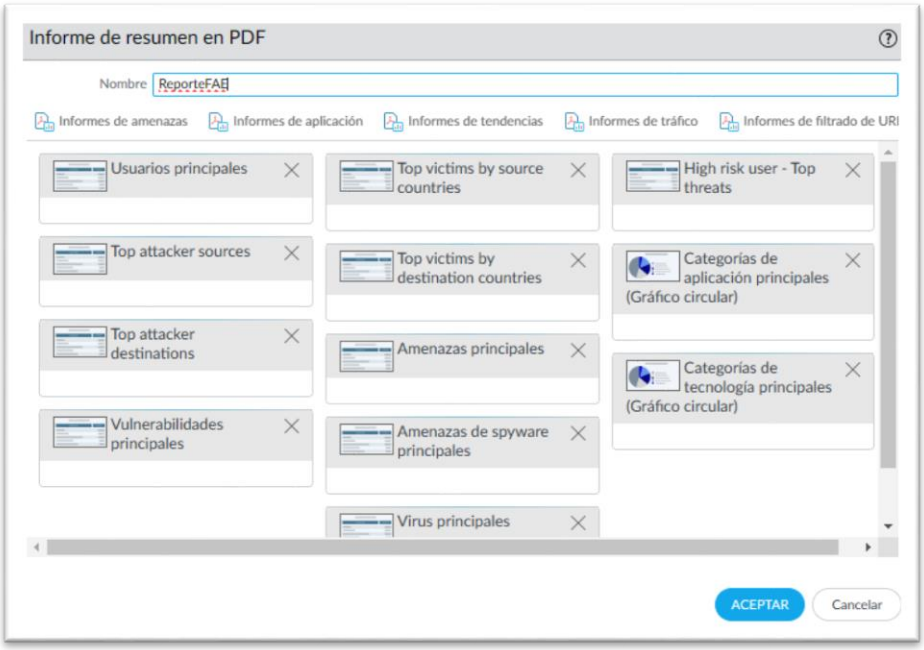


Fuente: server propio institucional Palo Alto 2023

• **Generación de informes:** los informes predefinidos se pueden realizar cambios de acuerdo a las características que se encuentran definidas en la herramienta, o bien pueden personalizarse o desplegarse en un solo informe con el fin de adaptarse a los requisitos específicos, los informes se pueden exportar a formatos conocidos y se pueden ejecutar y enviar por correo electrónico de forma programada.

Figura 19.

Ventana Gestión de informes



Fuente: server propio institucional Palo Alto 2023

• **Generación de logs:** el filtrado de paquetes de datos de logs en tiempo real ayuda a la rápida investigación forense de cada sesión que viaja por la red. Los resultados de filtro de log pueden exportarse archivos conocidos o enviarse a un servidor syslog de correlacionador de eventos como un SIEM para poder archivarlo fuera de línea o realizar análisis adicionales.

Figura 20.

Logs de tráfico de navegación en NGF

	FECHA DE REGISTRO	TIPO	ZONA ORIGEN	ZONA DESTINO	IP ORIGEN	USUARIO DE ORIGEN	GRUPO DE DIRECCIONES DINÁMICAS DE ORIGEN	IP DESTINO	GRUPO DE DIRECCIONES DINÁMICAS DE DESTINO	GRUPO DE USUARIOS DINÁMICOS	PUER DEST
	03/08 18:22:45	end	LAN	WAN	10.160.11.209			142.250.78.161			443
	03/08 18:22:45	end	LAN	WAN	10.160.11.209			172.217.30.214			443
	03/08 18:22:45	end	LAN	WAN	10.160.10.1			38.90.226.20			80
	03/08 18:22:45	end	LAN	WAN	10.160.12.115			64.68.121.175			443
	03/08 18:22:45	end	DMZ	WAN	10.160.10.90			8.8.8.8			53
	03/08 18:22:45	end	LAN	DMZ	10.160.10.1			10.160.10.90			53
	03/08 18:22:45	end	DMZ	WAN	10.160.10.90			8.8.8.8			53
	03/08 18:22:45	end	DMZ	WAN	10.160.10.90			8.8.8.8			53
	03/08 18:22:45	end	LAN	DMZ	10.160.13.130			10.160.10.90			53
	03/08 18:22:45	end	LAN	DMZ	10.160.10.1			10.160.10.90			53
	03/08 18:22:45	end	LAN	DMZ	10.160.10.1			10.160.10.90			53
	03/08 18:22:45	end	LAN	DMZ	10.160.13.23			10.160.10.90			53

Fuente: server propio institucional Palo Alto 2023

Análisis Shorewall

Shorewall es el programa basado en software libre que actúa como firewall, específicamente es un filtro de red que bloquea tráfico hasta la capa 4 de transporte del modelo OSI, donde interactúan los puertos y protocolos de comunicación TCP/UDP

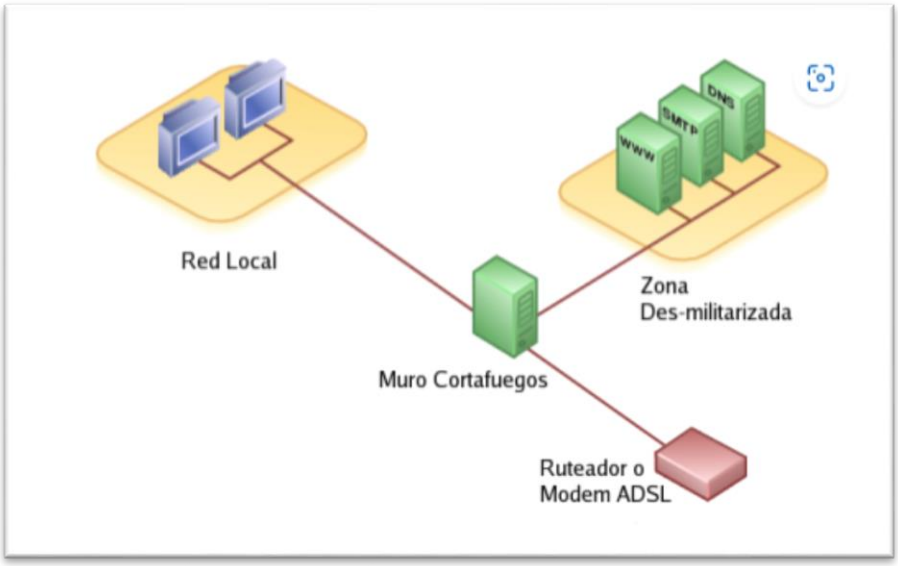
Se trata de un programa de software de alto nivel que permite realizar la instalación configuración y administración de un programa que actúa como muro cortafuegos, se necesita que se configuren ciertos datos en algunos ficheros de la herramienta en texto simple y éste a su vez creará las reglas de cortafuegos correspondientes a través de IPTables. Shorewall es uno de ellos y permitir utilizar un sistema de firewall dedicado, o como también sistemas de múltiples funciones como puerta de enlace.

Las desventajas de estas herramientas es que son muy simples en su protección y muy generales en sus políticas por lo tanto es posible detectarlos, no tienen la facilidad de ofrecer nada de información sobre ataques o vulnerabilidades, y están completamente diseñados para detectar ciertos comportamientos o patrones lógicos y sobre todo depende de la habilidad del administrador para aplicar sus políticas y reglas del firewall.

Según (Shorewall, 2022) es una herramienta robusta de nivel elevado para la configuración de muros virtuales o cortafuegos; Shorewall plantea que es necesario definir cierta información en los ficheros del shorewall en modo de texto que son simples, y éste a su vez puede crear las reglas respectivas de contafuegos que corresponden a iptables.

Figura 21.

Imagen de un firewall



Fuente: elaboración propia (2023)

Funciones de Shorewall

NAT: Network Address Translation o Traducción de dirección de red, también se le conoce como regla de enmascaramiento de protocolo de direccionamiento IPv4, quiere decir que las direcciones de origen y/o destino de paquetes de protocolo IP son sobre escritas cuando atraviesan el dispositivo de encaminamiento-router o muro cortafuegos.

Se utiliza para permitir a un sin número de anfitriones en una Red Privada con rango de direcciones IP para que dicha red privada acceda hacia Internet utilizando solo una única dirección IP pública.

DNAT: Destination Network Address Translation o también llamado traducción de dirección de red de destino, es la función mediante la cual se pública un servicio o sistema desde una red privada o red LAN; es decir que está permitido redirigir puertos de comunicación en TCP/UDP a direcciones IP de red privada; esto quiere decir que puede permitir a un usuario en Internet alcanzar un puerto en una Red Privada.

Equipamiento lógico necesario.

Se requerirán los siguientes paquetes:

iptables: Programa que controla el código del núcleo de Linux para filtrar los paquetes de un entorno de tráfico de red

iproute: Esquema de privilegios que se encuentran programadas y configuradas para utilizar las capacidades de enrutamiento en sus diversos protocolos de gestión de redes del núcleo de Linux..

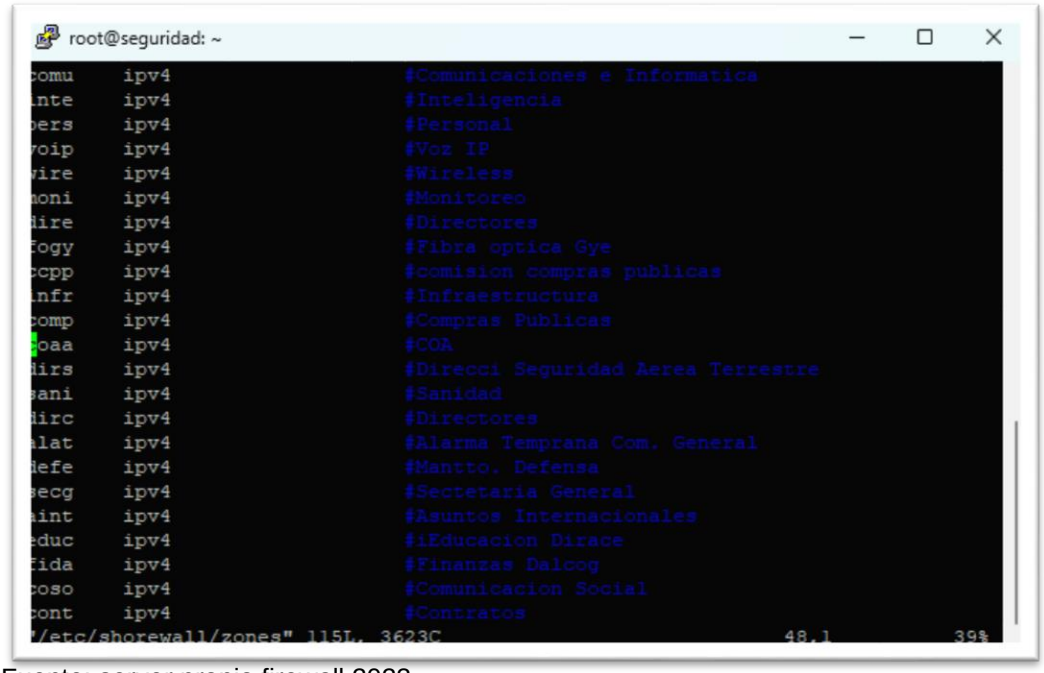
shorewall: Shoreline Firewall.

/etc/shorewall/shorewall.conf: Fichero general donde se encuentra la configuración de la herramienta Shorewall, en Este se activa el servicio y funciones que se requiera utilizar.

/etc/shorewall/zones: Este fichero es utilizado para definir las zonas lógicas que se marcan por caracteres de texto con el tipo de direccionamiento IP y que se utilizará en el muro cortafuegos.

Figura 22.

Ventana /etc/shorewall/zones de shorewall



Fuente: server propio firewall 2023

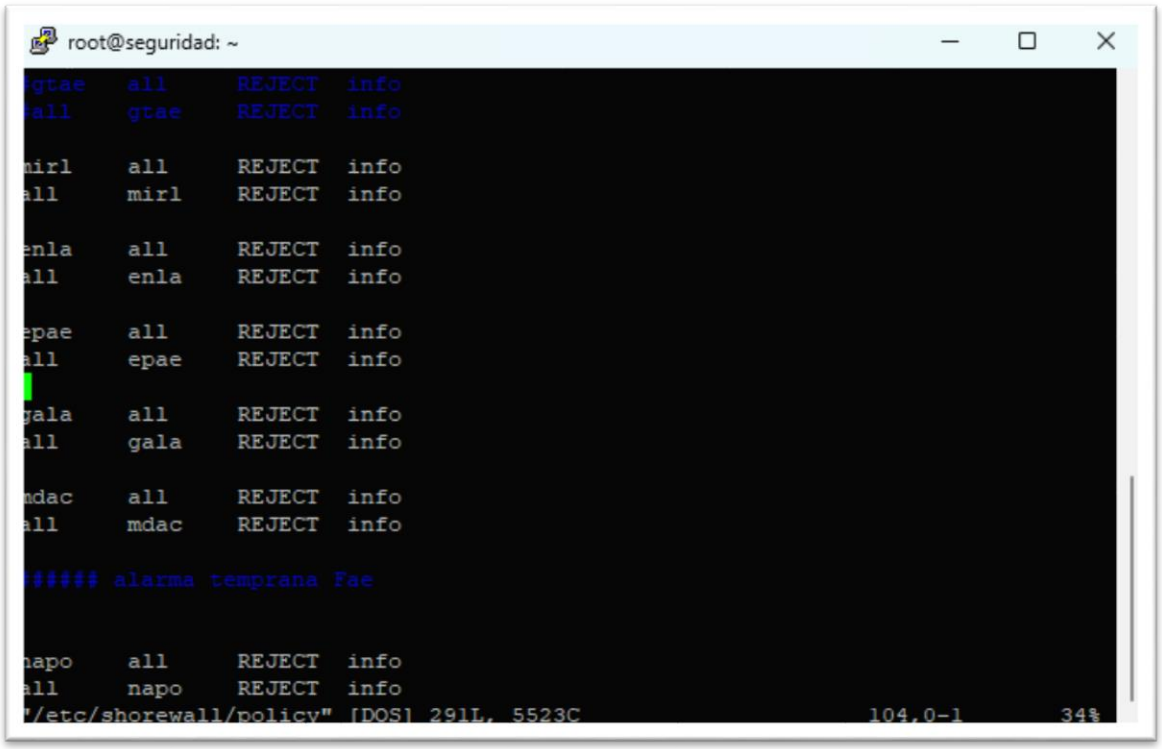
/etc/shorewall/interfaces: Este fichero es utilizado para poder definir cuál es la configuración de las interfaces de red que corresponden a una zona lógica del muro cortafuegos en particular y las opciones de configuración que se requieran para cada una de éstas.

/etc/shorewall/masq: En este fichero se configura para utilizar y definir cuáles son los dispositivos que se puede utilizar para los enmascaramientos de direcciones IP.

/etc/shorewall/policy: Este fichero se utiliza para poder configurar y determinar las políticas predeterminadas para cada zona lógica del muro cortafuegos con respecto al resto de zonas.

Figura 23.

Ventana de fichero de políticas de shorewall



Fuente: server propio firewall 2023

/etc/shorewall/blrules: En este fichero se utiliza para poder definir reglas para bloquear las direcciones IP o bloques de direcciones IP que se requiere poner en lista negra.

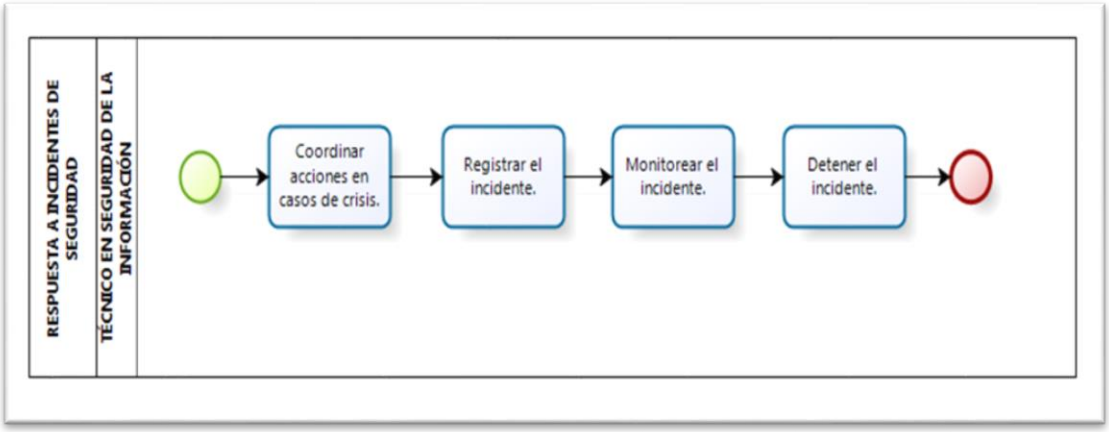
/etc/shorewall/rules: En este fichero se utiliza para poder definir las reglas apertura o cierre de puertos.

Cabe indicar que, las soluciones con shorewall se encuentran basada en software libre y toman un enfoque para la prevención de amenazas y vulnerabilidades ya que cada función, firewall, IPS, filtrado de URL, etc. Puede explorar el tráfico de red de origen y destino sin compartir contexto, de tal forma que resulta más predecible al comportamiento evasivo de los paquetes.

Proceso para detallar un evento o reporte

Figura 24

Proceso para levantar un reporte



Actividad a cumplir

Actividad	Rol	Descripción
1. Establecer procedimientos para la gestión de incidentes de seguridad en la infraestructura crítica digital de la empresa XY	Jefe Dpto. de Ciberoperaciones	Consiste en elaborar el manual de en el cual se establece los procedimientos para la gestión de incidentes.
2. Realizar el monitoreo de eventos de seguridad y de disponibilidad de servicios.	Jefe de la sección de seguridad	Consiste en listar los servicios, aplicaciones, servidores, etc que deben ser monitoreados en base a los servicios de infraestructura crítica digital de la empresa XY
3. Analizar patrones de comportamiento anormales y de controles de seguridad.	Técnicos de Monitoreo	Consiste en analizar la información sobre el comportamiento, característica o descripción de una amenaza para verificar el comprometimiento de equipos con malware, para prevenir futuros ataques.
4. Disponer cumplimiento de controles de seguridad.	Técnicos de Monitoreo	Con el uso de herramientas de monitoreo se reciben alertas y advertencias de eventos que podrían atentar contra la disponibilidad, integridad y confidencialidad de la infraestructura crítica digital de la empresa XY, por lo cual se dispone la reconfiguración y/o implementación de restricciones en los equipos informáticos.
5. Seguimiento a controles de seguridad.	Técnicos de Monitoreo	Consiste en realizar un seguimiento periódico de los eventos detectados por las herramientas de monitoreo y la implementación de los controles dispuestos.

6. Realizar el registro del incidente.	Técnico de Resolución de incidentes	Consiste en registrar un incidente reportado incidente en la herramienta de gestión de incidentes.
7. Realizar la clasificación y priorización del incidente.	Técnico de Resolución de incidentes	Consiste en realizar un análisis del incidente reportado, clasificarlo según su tipo, darle prioridad de acuerdo con el impacto y asignar a un técnico su tratamiento.
8. Analizar la base de conocimiento para tratar el incidente.	Técnicos de Resolución de incidentes	Consiste en verificar si el incidente se encuentra en la base de conocimientos, según su tipo para su inmediata resolución.
9. Establecer medidas de contención	Técnicos de Resolución de incidentes	Consiste en realizar las gestiones técnicas para solventar el incidente y darle solución.
10. Remitir Informe de resolución del incidente	Técnicos de Resolución de incidentes	Consiste en elaborar el informe técnico de las gestiones realizadas de la gestión del incidente.
11. Ejecutar el trabajo de investigación de informática forense.	Técnicos de Resolución de incidentes	Consiste en realizar el trabajo de informática forense en el ambiente configurado.
12. Elaborar informe de investigación de hallazgos informáticos	Técnicos de Investigación Forense Informática	Consiste en realizar un informe técnico de las acciones realizadas y hallazgos en el trabajo forense.
13. Recopilar informes de la gestión de monitoreo, gestión de incidentes, entrenamiento y análisis forense.	Técnicos de Investigación Forense Informática	Consiste en elaborar un informe ejecutivo de la gestión de defensa.
14. Elaborar informe ejecutivo de actividades de Defensa, para evaluar desempeño.	Técnicos de Investigación Forense Informática	

PROCEDIMIENTO PARA ANÁLISIS DE VULNERABILIDADES.

- **PROPÓSITO:** Contar con el registro de causas de posibles amenazas, los daños y consecuencias que éstas puedan producir en la seguridad de la información de la empresa XY.
- **ALCANCE:** Empresa XY

A continuación, el detalle de las actividades que componen el procedimiento de Análisis de Vulnerabilidades:

Actividad	Rol	Descripción	Documento
Analizar vulnerabilidades en la red.	Técnico de Seguridad de la Información.	Consiste en la verificación de posibles accesos que altere y cambie el normal desarrollo de la infraestructura de red.	Ninguno
Realizar test de penetración interna.	Técnico de Seguridad de la Información.	Consiste en verificar posibles vulnerabilidades a los usuarios de la red LAN de los usuarios de la empresa XY	Ninguno
Realizar test de penetración externa.	Técnico de Seguridad de la Información.	Consiste en verificar posibles vulnerabilidades que estén dirigidos desde la red WAN e Internet en la empresa XY	Ninguno
Explotar vulnerabilidades detectadas (Ethical Hacking).	Técnico de Seguridad de la Información.	Una vez identificadas las posibles intrusiones a la infraestructura de red, se verifica que tipo de información fue afectada.	Ninguno
Recomendar correctivos a las vulnerabilidades detectadas (hardening).	Jefe Dpto. Seguridad de la Información.	Consiste en corregir las fallas encontradas en la red y en los usuarios.	Ninguno

Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 1.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
IDS	Sistema que detecta intrusiones o accesos a los sistemas que no están autorizados	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre un IDS	Fuente bibliográfica	Permitió verificar la funcionalidad de la herramienta de seguridad en un SOC	
SIEM	Herramienta de gestión de análisis de eventos de correlación de eventos en tiempo real.	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre un SIEM	Fuente bibliográfica	Permitió verificar la funcionalidad de la herramienta de seguridad en un SOC	

SOFTWARE LIBRE	Sistema operativo o conjunto de herramientas informáticas que no posee dueño ni licencia para utilizarlos	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre software libre	Fuente bibliográfica	Permitió conocer la ventaja y desventaja del uso de herramientas con software libre, para poder recomendar la ideal.
SOFTWARE CON LICENCIA	Sistema operativo o conjunto de herramientas informáticas que se realiza un cntrato de pago por su uso	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre software de pago	Fuente bibliográfica	Permitió conocer la ventaja y desventaja del uso de herramientas con licenciamientos, para poder recomendar la ideal.

Fuente: Elaboración propia

CONCLUSIONES

Las amenazas y vulnerabilidades en seguridad de la información están constantemente presentes y actualmente muchas empresas sean públicas, privadas o del sector defensa

Actualmente más organizaciones se ven en la imperiosa necesidad de implementar un SOC, con diferentes tipos de herramientas o soluciones, ya sean en software libre o bajo licencias.

El realizar un análisis de las funcionalidades de cada herramienta a implementar en un SOC, como es IDS-wazuh, SIEM-splunk, Firewall-shorewall y Next Generation Firewall NGT fue de mucha importancia, debido a que es necesario validar la utilidad de cada herramienta para determinar el alcance de las necesidades.

La elección entre software libre o bajo licencia dependerá en su gran mayoría del tamaño de la organización y del presupuesto económico asignado.

Se realizó una tabla comparativa de ventajas y desventajas del uso de las herramientas IDS-wazuh, SIEM-splunk, firewall y NGF

Se elaboró un proceso para levantar un reporte de seguridad de acuerdo a la información recibida por las herramientas que se implementaron en el SOC

RECOMENDACIONES

Responder inmediatamente ante cualquier sospecha de amenaza o vulnerabilidad de los sistemas institucionales

Realizar un afinamiento mucho más granular de las herramientas que se implementaron en el SOC

Mantener como un proceso inicial las herramientas de seguridad bajo software libre para adquirir una curva de aprendizaje y experiencia, pero si la organización crece o se ve afectada por algún tipo de soporte en las herramientas, se recomienda migrar a soluciones con licencia

Mantener constantemente actualizados los sistemas operativos de las herramientas del SOC que son bajo software libre para evitar vulnerabilidades en las mismas

Cumplir con el proceso de reportes de seguridad indicado y mantener dichos reportes cada día para poder evaluar, auditar o recomendar a los directivos sobre temas de seguridad

BIBLIOGRAFÍA

Bibliografía

Abreu, J. L. (2020). El Método de la Investigación. *Daena: International Journal*, 195.

Alonso, C. (5 de Marzo de 2020). *globalsuitesolutions*. Obtenido de globalsuitesolutions: https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

Alto, P. (2022). *Palo Alto*. Obtenido de Palo Alto: https://media.paloaltonetworks.com/documents/datasheet-firewall-feature-overview-es.pdf

Apache, b. (s.f.). *bluehosting host*. Obtenido de bluehosting host: https://docs.bluehosting.cl/tutoriales/servidores/instalacion-y-configuracion-de-la-aplicacion-mod-security-en-apache.html

Arroyo, V. G. (2020). *Que sabemos de Ciberseguridad.* Madrid: CSIC.

BSIGROUP. (4 de Junio de 2022). *bsigroup*. Obtenido de bsigroup: https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

Castillo, G. (30 de Junio de 2022). *Innovación digital 360*. Obtenido de Innovación digital 360: https://www.innovaciondigital360.com/big-data/que-son-y-como-funcionan-los-data-center/

Cedeño. (2020). *CONFIGURACIÓN DEL FIREWALL DE APLICACIONES WEB.* Esmeraldas: Universidad Católica de Esmeraldas.

Chaeyeon Oh, J. H. (2002). A Survey on TLS-Encrypted Malware Network Traffic Analysis. *Applied Sciences*, 1.

CITELIA. (9 de Diciembre de 2019). *citelia*. Obtenido de Citelio conéctate con nosotros: https://citelia.es/blog/que-es-cloud-computing-y-como-funciona/

Contreras, S. (2020). *Actividades de monitoreo y analisis en un Security Operation Center.* Mexico: Universidad Nacional Autonoma de Mexico.

Correa. (enero de 2009). ESTRATEGÍA PARA LA IMPLANTACIÓN DE SOFTWARE LIBRE EN LA ADMINISTRACIÓN PÚBLICA CENTRAL. *ESTRATEGÍA PARA LA IMPLANTACIÓN DE SOFTWARE LIBRE EN LA ADMINISTRACIÓN PÚBLICA CENTRAL*. Quito, Pichincha, Ecuador: Presidencia de la Repúblcia del Ecuador.

Cózar, P. (2020). *Implementación de Wazuh en una organización pública.* España.

Estrada, A. C. (2017). *CIBERSEGURIDAD Una Estratégia Informático / Militar.* Madrid: Darfe.

ETICENTRE. (30 de Agosto de 2019). *ETICENTRE*. Obtenido de ETICENTRE: https://www.eticentre.org/objetivos-desarrollo-sostenible/industria-innovacion-e-infraestructuras/

Fernandez, Y. (6 de Marzo de 2020). *Ayuda le proteccion datos*. Obtenido de Ayuda le proteccion datos: https://ayudaleyprotecciondatos.es/2022/02/11/encriptacion-datos/#:~:text=La%20encriptaci%C3%B3n%20de%20datos%20es%20un%20proces

o%20de,la%20informaci%C3%B3n%20mientras%20viaja%20del%20emisor%20al%20receptor.

Fortra. (19 de septiembre de 2018). *SIEM open source vs. SIEM empresaria:¿cuál es adecuado para su empresa?* Obtenido de SIEM open source vs. SIEM empresaria:¿cuál es adecuado para su empresa?: https://www.fortra.com/es/blog/siem-open-source-vs-siem-empresarial-cual-es-el-adecuado-para-su-empresa

Fueyo, D. R. (2020). *Implementación de las operaciones y gestión de un SOC en una institución financiera partiendo desde cero utilizando soluciones SIEM.* España.

Giner, G. J. (2020). Conpetencias profesionales para lograr el éxito laboral. *Business Review*, https://www.escueladenegociosydireccion.com/revista/business/rr-hh/competencias-profesionales-para-lograr-el-exito-laboral/.

Hidalgo, G. (2023). *Implementaci´pon de Security Data Lake con Splunk.* España: Universida Oberta de Catalunya.

INCIBE, I. N. (2023). *Boletin Informativo INCIBE.* España: Unión Europea.

INTEDYA. (1 de Septiembre de 2019). *INTEDYA*. Obtenido de INTEDYA INTERNATIONAL DYNAMIC ADVISORS: https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

ISACA. (2021). The Evolution of Security. *ISACA JOURNAL*, 1.

KIONETWORKS. (14 de Junio de 2022). *KIONETWORKS*. Obtenido de KIONETWORKS: https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center

Klusaité, L. (7 de Abril de 2022). *NordVPN*. Obtenido de NordVPN: https://nordvpn.com/es/blog/seguridad-cloud-computing/

Lascano, S. (2022). *Evalucaión de tecnologías UTM y NGF para la detección de vulnerabildiades en la red.* RIOBAMBA: ESPOCH.

Lewis Mahecha, R. N.-M. (2022). Factores Clave en la evaluación del software libre o propietario para su uso en organizaciones militares y de defensa. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 1-2.

Martínez, E. (21 de Abril de 2021). *Seguridad en América*. Obtenido de Seguridad en América: https://www.seguridadenamerica.com.mx/noticias/articulos/27438/soluciones-de-seguridad-en-data-centers

Maxwell, J. A. (2019). *Diseño de investigación cualitativa.* Barcelona: Gedisa S.A.

MINTEL. (17 de Mayo de 2021). Política de Ciberseguridad. *Política de Ciberseguridad*. Quito, Pichincha, Ecuador: pagina 23.

Moes, T. (25 de Marzo de 2018). *SoftwareLab*. Obtenido de SoftwareLab ORG: https://softwarelab.org/es/que-es-un-firewall/

Natalie, C. (2020). *FIREWALL DE APLICACIONES WEB mODSECURITY PARA PREVENIR DIVERSOS ATAQUES HACIA APLICACIONE WEB ALOJADOS EN SERVER OPEN SOURCE.* ESMERALDAS: PONTIFICIA UNIVERSIDAD CATÓLICA DEL EUADOR ESMERALDAS.

NORMA ISO. (25 de Junio de 2019). *normaiso27001*. Obtenido de normaiso27001: https://advisera.com/27001academy/es/que-es-iso-27001/

Osvaldo, C. (2020). Firewall / Cortafuegos. *net.report*, 180.184.

Palo Alto, N. (s.f.). *paloaltonetworks*. Obtenido de paloaltonetworks: https://media.paloaltonetworks.com/documents/datasheet-firewall-feature-overview-es.pdf

Pastor, M. (2022). *Implementación de un SOC con la herramienta SIEM Elastic Security.* Valencia: Vetsin.

Pathak, A. (7 de Abril de 2022). *geekflare*. Obtenido de geekflare: https://geekflare.com/es/hardware-vs-software-cloud-firewall/

Ramírez, A. (1 de Junio de 2022). *Community*. Obtenido de FS Community: https://community.fs.com/blog/what-is-a-data-center-firewall.html

Riola. (2022). Factores clave en la evaluacipon del software libre o propietario para su uso en las organizaciones militares y de defensa. *RISTI, Revista Ibérica se sistemas y Técnologias de informacao*, 335.

Sánchez, F. (17 de Febrero de 2019). *Smartekh*. Obtenido de Smartekh: https://blog.smartekh.com/4-de-las-principales-problematicas-y-riesgos-en-los-data-center

Shorewall. (2022). *iptables made easy shorewall*. Obtenido de iptables made easy shorewall: https://shorewall.org/

Tocino, A. B. (2022). *Integración de un Centro de Operaciones de Seguridad con Componentes de Código Abierto.* España: Universidad de Catambria.

Urzola, A. M. (2020). Metodos indictivo, deductivo y teoría de la pedagogía crítica. *Petrogrifos, Revista Crítica Transdisciplinar*, 38.

Zambrano, G. A. (2019). DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN. *(Tesis de Ingeniería).* Universidad Tegnologica Israel, Quito.