UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS:

Security Onion como herramienta de Auditoría de Redes en la Universidad Nacional de San Cristóbal de Huamanga, 2023.

Para optar el título profesional de:

INGENIERA DE SISTEMAS

PRESENTADO POR:

Bach. Kimberlly Nena BARRAZA TUDELA

ASESOR:

Mg. Ing. Hubner JANAMPA PATILLA

AYACUCHO - PERÚ

2024

DEDICATORIA

A la Sra. A. Nena Tudela González y el Sr. Antonio D. Barraza Subia, mis progenitores, y a todos aquellos que tenían el anhelo de ver este trabajo terminado.

A todos aquellos que buscan información y respuestas respecto a Security Onion y auditoría de redes ya que este trabajo puede ayudar.

A tí, que no te dedican ni una canción (ahora podrás presumir que te dedicaron un trabajo de investigación).

AGRADECIMIENTO

A la Santísima Trinidad que es un solo Dios, a mis padres, a mis seres queridos, a todas las personas que conocí a lo largo de mi vida, en vista que ayudaron a forjar a la persona que soy ahora.*

Al Dr. Ing. Hubner Janampa Patilla por su paciencia durante todo el tiempo que se realizó este trabajo.

*A Junior Anderson Pulido Palomino que no tenía la obligación de leer la tesis pero decidió realizarlo para ver si encontraba errores** garrafales (para hacerme bullying) y vaya que las encontró, a pesar de no estar con gafas.*

A Eyder C.B. requiescat in pace.

A Andy Antonhy Luya Arcce, que tenía reunión de trabajo pero se escapó y llegó a la sustentación.

**Amigos, ustedes también cuentan.*
***Ya fueron corregidos.*

RESUMEN

En un entorno global cada vez más interconectado, la seguridad de las redes es crucial para garantizar la integridad, la confidencialidad y la disponibilidad de la información. Este estudio aplicado, descriptivo y experimental se centra en la implementación de Security Onion como herramienta de auditoría de redes en la Universidad Nacional de San Cristóbal de Huamanga (UNSCH), con el propósito de mejorar su postura de seguridad implementando ciertas salvaguardas recomendadas según los controles CIS.

Los resultados muestran que la implementación de Security Onion permite detectar actividades sospechosas en la red de la ciudad universitaria, lo que brinda una visión más completa de las actividades de la red, facilita la identificación de incidentes y posibilita una mejor capacidad de respuesta.

Este estudio no solo proporciona un marco para la mejora continua de la seguridad de la red perteneciente a la UNSCH, sino que también puede aplicarse a otras instituciones que buscan fortalecer su seguridad cibernética ya que Security Onion demuestra ser una solución efectiva para la monitorización y detección de amenazas, contribuyendo de manera significativa a la protección de activos digitales e informáticos y a la confidencialidad de la información en entornos académicos, además, resalta la relevancia de la proactividad en ciberseguridad.

Palabras clave: auditoría de redes, monitorización de seguridad, Security Onion, gestión de logs, IDS, seguridad de redes.

ABSTRACT

In an increasingly interconnected global environment, network security is crucial to ensure the integrity, confidentiality and availability of information. This applied, descriptive and experimental study focuses on the implementation of Security Onion as a network auditing tool at the San Cristóbal de Huamanga National University (UNSCH), with the purpose of improving its security posture by implementing certain recommended safeguards according to CIS controls.

The results show that the implementation of Security Onion enabled the detection of suspicious activity on the university's city network, providing a more complete view of network activity, facilitating incident identification, and enabling a better response capability.

This study not only provides a framework for the continuous improvement of the UNSCH's network security, but can also be applied to other institutions seeking to strengthen their cyber security as Security Onion proves to be an effective solution for monitoring and detecting threats, contributing significantly to the protection of digital and IT assets and the confidentiality of information in academic environments, it also highlights the relevance of proactivity in cybersecurity.

Keywords: network auditing, security monitoring, Security Onion, logs management, IDS, network security.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En un mundo cada vez más interconectado, la seguridad de las redes se ha convertido en un aspecto crítico para garantizar la integridad, confidencialidad y disponibilidad de la información. Las instituciones educativas, como la Universidad Nacional de San Cristóbal de Huamanga (UNSCH), dependen de redes seguras para respaldar sus actividades académicas y administrativas.

La auditoría de redes se presenta como una herramienta fundamental para evaluar la seguridad de estas infraestructuras, detectando posibles vulnerabilidades, amenazas e intrusiones. Este trabajo de investigación tiene como objetivo principal implementar Security Onion como herramienta de auditoría de redes para la UNSCH en el año 2023.

Para alcanzar este objetivo, se abordan tres aspectos clave: la monitorización de seguridad, la gestión de logs y los sistemas de detección de intrusos.

La monitorización de seguridad es esencial para identificar y analizar eventos de seguridad en tiempo real. Este estudio explora cómo Security Onion facilita dicha monitorización, lo que permite una respuesta oportuna a posibles amenazas y anomalías en la red de la UNSCH.

La gestión de logs se centra en la recopilación, el almacenamiento y el análisis de los registros de eventos generados por dispositivos y aplicaciones en la red. Security Onion se posiciona como una herramienta eficaz en esta área, ya que proporciona una visión integral de las actividades en la red y facilita la identificación de incidentes de seguridad.

Por último, los sistemas de detección de intrusos son cruciales para identificar actividades maliciosas. Se analizará cómo Security Onion mejora la capacidad de la UNSCH para proteger sus activos digitales y salvaguardar la confidencialidad de la información mediante estos sistemas que tiene incluidos.

En conclusión, este trabajo de investigación se centra en la implementación de Security Onion como herramienta de auditoría de redes en la UNSCH para fortalecer su seguridad y mejorar su capacidad para hacer frente a desafíos en materia de ciberseguridad.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA

De acuerdo con IBM et al. (2024), Check Point (2024) y Fortinet (s.f.), durante el año 2023 se observaron cambios drásticos en el panorama de la ciberseguridad debido a la evolución de los ciberataques. Aunque se registró un notable descenso de los ataques de ransomware a empresas en comparación con el año 2022, las amenazas cibernéticas continuaron captando la atención de entidades gubernamentales y del público en general.

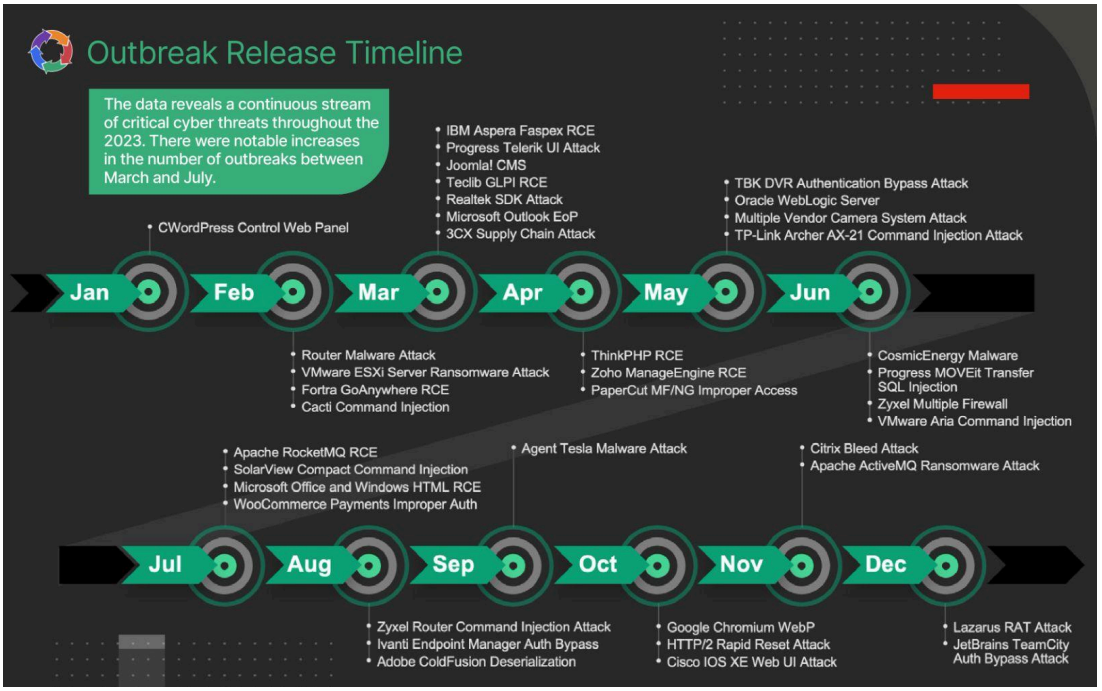
Fortinet, a través de su FortiGuard Labs, revela un flujo continuo de ciberamenazas críticas a lo largo del año. El periodo con mayores aumentos en el número de brotes fue de marzo a julio de 2023, siendo marzo el mes con el mayor número de brotes, como se muestra en la Figura 1. También se descubrió que el número de vulnerabilidades activamente atacadas con ataques generalizados aumentó un 15 % en comparación con 2022 (ver Figura 2).

Los informes de IBM y Check Point destacan varios puntos críticos:

- Los sectores de la educación, la administración pública y la sanidad siguen siendo los principales objetivos de los ciberataques: Si bien existe un pequeño descenso reciente en el número de ataques contra estos sectores, las instituciones educativas siguen recibiendo demasiados intentos de ataque semanales (ver Figura 3). Algunos ataques han formado parte de campañas de mayor envergadura, como los que afectaron a la Universidad Johns Hopkins y al Sistema Universitario de Georgia, que se vieron comprometidos por el ransomware CL0P a través del software de transferencia de archivos gestionado MOVEit.
- Incremento del 71% en ataques con credenciales válidas: El abuso de cuentas válidas se convirtió en el punto de entrada más común, representando el 30% de los incidentes atendidos por X-Force de IBM.
- Reducción del 11.5% en incidentes de ransomware empresarial: A pesar de seguir siendo comunes, los incidentes de ransomware disminuyeron, posiblemente porque las grandes organizaciones están optando por la restauración en lugar de pagar rescates. No obstante, los ciberdelincuentes utilizan «sitios de la vergüenza» para exponer a las víctimas.

Figura 1

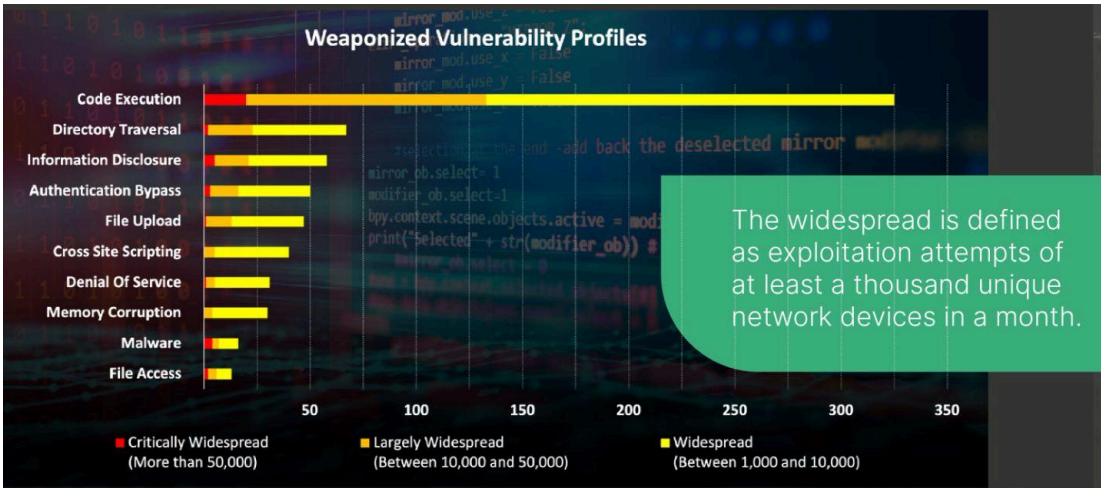
Línea de tiempo de la apariciòn de los brotes



Nota. Adaptado de *Outbreak Release Timeline* [Figura], por Fortinet, s.f.

Figura 2

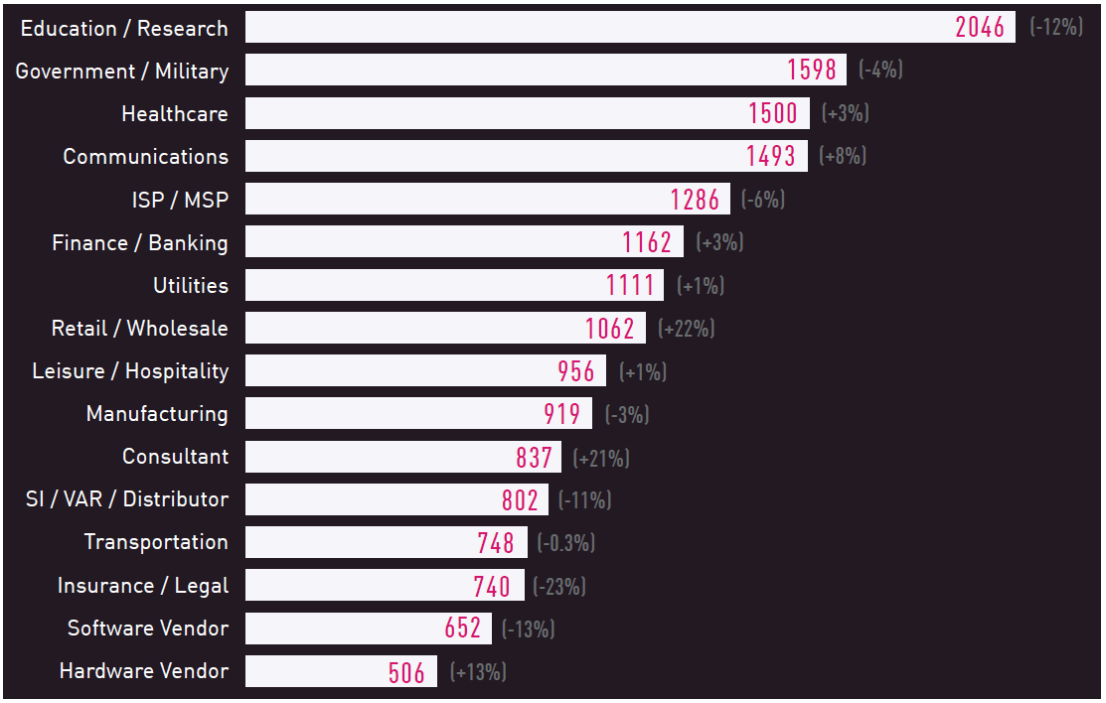
Perfiles de vulnerabilidad atacados



Nota. Adaptado de *Weaponized Vulnerability Profiles* [Figura], por Fortinet, s.f.

Figura 3

Media mundial de ataques semanales por sector en 2023



Nota. Lo que se muestra dentro de los corchetes es el porcentaje de variación con respecto a 2022. Adaptado de *Global Average of weekly attacks per organization by Industry in 2023* [Figura], por Check Point, 2024.

- El 30% de las vulnerabilidades en aplicaciones web están relacionadas con errores de configuración de seguridad: Las pruebas revelaron que los errores de configuración de seguridad fueron los riesgos más frecuentes.
- Aumento del 32% en robos y filtraciones de datos: Este método se convirtió en el impacto más común, lo que indica una preferencia creciente entre los ciberdelincuentes por obtener beneficios económicos a través del robo de datos.
- Incremento del 266% en el uso de infostealers (ladrones de información, especialmente de credenciales): Se observó un aumento significativo en la actividad de infostealers como Rhadamanthys, LummaC2 y StrelaStealer.
- El 32 % de los incidentes involucraron el uso malicioso de herramientas legítimas: Casi un tercio de los incidentes resueltos por X-Force involucraron el uso de herramientas legítimas para actividades maliciosas.
- El 84 % de los incidentes en infraestructuras críticas podrían haberse evitado: La mayoría de estos incidentes podrían haberse mitigado con buenas prácticas de seguridad.

Check Point también señaló un aumento en el hacktivismo, utilizado ahora por gobiernos en conflictos internacionales, y la explotación de vulnerabilidades en dispositivos de red como routers y switches. Además, la inteligencia artificial se ha convertido en una herramienta tanto para atacantes como para defensores en el ámbito de la ciberseguridad.

A nivel del continente americano, Check Point (2024) ha identificado que, durante el año 2023:

- El 27% de las organizaciones fueron afectadas por malware multipropósito: Destacan FakeUpdates y Qbot, utilizados para el robo de datos y extorsión.
- El 9% de las organizaciones sufrieron robos de información: El malware infostealer, como AgentTesla, continúa siendo prevalente, operando bajo el modelo de malware como servicio (MaaS).
- 8% de las organizaciones fueron afectadas por criptominería ilegal: Aunque disminuyó en 2023 debido a la baja en las tasas de Bitcoin y la dificultad creciente de la minería, sigue siendo una amenaza multifacética que aprovecha la capacidad de las GPU y usa funcionalidades maliciosas. La infraestructura en la nube también sigue siendo un objetivo para la explotación de la minería de criptomonedas.
- 7% de los dispositivos móviles fueron afectados: AhMyth Android es un troyano de acceso remoto (RAT), utilizado como base para ataques. Se encontró una variante llamada AhRat en una aplicación llamada 'iRecorder-Screen Recorder' en Google Play Store con más de 50,000 descargas. La aplicación original era inofensiva, pero posteriormente se le agregaron características maliciosas, como la captura de pantalla, grabación de sonido y exfiltración de datos.
- Nuevo caso de ransomware en el ecosistema Android: Las aplicaciones SpyLoan fueron distribuidas a millones de usuarios en Sudamérica a través de Google Play Store. Este malware recopila datos personales y financieros de las víctimas y las extorsionaba y acosaba con estos datos para obtener beneficios económicos.

Figura 4

Porcentaje de organizaciones afectadas por tipo de malware y porcentaje de prevalencia respectiva en América durante el año 2023

Nota. Comenzando por la izquierda: a) Porcentaje de organizaciones afectadas por tipo de malware, b) Malware multipropósito más prevalente, c) Principales programas maliciosos de robo de información (infostealers), d) Principales programas maliciosos de minería de criptomonedas (cryptominers) y e) Principales programas maliciosos para móviles. Adaptado de *Percentage of organizations affected by malware type in the Americas in 2023* [Figura], *Most prevalent multipurpose malware in the Americas—2023* [Figura], *Top infostealer malware in the Americas—2023* [Figura], *Top cryptomining malware in the Americas—2023* [Figura] y *Top mobile malware in the Americas—2023* [Figura], por Check Point, 2024.

En el contexto peruano, hasta noviembre de 2023, la información obtenida por Quispe (2023) revela que los ataques más frecuentes se debieron a troyanos, que tienen como objetivo controlar el dispositivo del usuario para robar y apoderarse de

sus datos. Además, el phishing creció tres veces más de lo habitual, lo que subraya la necesidad urgente de mejorar las prácticas de seguridad.

La Universidad Nacional de San Cristóbal de Huamanga (UNSCH) no es ajena a estos problemas, cabe mencionar que si bien en la ciudad universitaria no se produjo un ataque de ransomware, sí sucedió en la red de su sede administrativa en 2022 y afectó a los servidores que alojaban los sistemas SIGA y SIAF, lo que es un importante antecedente y evidencia que la infraestructura de red de la UNSCH, al igual que la de muchas otras instituciones, debe hacer frente a desafíos significativos en términos de seguridad de la información.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

¿Cómo Security Onion es una herramienta de Auditoría de Redes para la UNSCH, 2023?

1.2.2. Problemas específicos

A. ¿Cómo Security Onion es una herramienta de auditoría de redes basada en la monitorización de seguridad para la UNSCH, 2023?
B. ¿Cómo Security Onion es una herramienta de auditoría de redes basada en la gestión de logs para la UNSCH, 2023?
C. ¿Cómo Security Onion es una herramienta de auditoría de redes basada en sistemas de detección de intrusos para la UNSCH, 2023?

1.3. OBJETIVOS

1.3.1. Objetivo general

Implementar Security Onion como herramienta de auditoría de redes para la UNSCH, 2023.

1.3.2. Objetivos específicos

A. Ejecutar Security Onion como herramienta de auditoría de redes basada en la monitorización de seguridad para la UNSCH, 2023.
B. Ejecutar Security Onion como herramienta de auditoría de redes basada en la gestión de logs para la UNSCH, 2023.

C. Ejecutar Security Onion como herramienta de auditoría de redes basada en sistemas de detección de intrusos para la UNSCH, 2023.

1.4. HIPÓTESIS DE LA INVESTIGACIÓN

Creswell (2022) reconoce que la investigación cualitativa a menudo se basa en la exploración y la emergencia de patrones y temas a partir de los datos, sin partir de hipótesis preconcebidas. En concordancia con lo anteriormente mencionado, esta investigación adopta un enfoque cualitativo con el objetivo de explorar y comprender un contexto particular, por lo que no se han formulado hipótesis.

CAPÍTULO II
MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Security Onion se ha utilizado ampliamente por profesionales y académicos en la industria de la seguridad informática, como demuestran investigaciones como la de Mobeen et al. (2021), titulada «A Review on Security Onion Tools for Intrusion Detection», y la de Heenan y Moradpoor (2016), titulada «Introduction to Security Onion». Estos estudios han demostrado que Security Onion es una herramienta altamente influyente en la gestión de la seguridad de redes. Los autores revisaron las herramientas que ofrece Security Onion para analizar e inspeccionar paquetes de red, lo que brinda a los analistas de seguridad una sólida protección del sistema. Los autores concluyeron que Security Onion es una plataforma que permite a los analistas configurar la monitorización y la generación de informes en entornos de detección de intrusiones en red, lo que demuestra su utilidad para la auditoría y la gestión de la seguridad de las redes en general.

Además, en el artículo científico titulado «Using and Configuring Security Onion to detect and prevent Web Application Attacks» de Deuble & Shinberg (2012), citado por los autores mencionados anteriormente, se destaca cómo esta herramienta protege los entornos de aplicaciones web contra vulnerabilidades comunes como XSS e inyecciones SQLi.

Gonzales et al. (2015) analizaron Security Onion en su artículo teórico-práctico «Using Security Onion for Hands-On Cybersecurity Labs», en el que examinan el uso de Security Onion como entorno para la formación en ciberseguridad, en línea con el Marco Nacional de la Fuerza de Trabajo de Ciberseguridad de los Estados Unidos. Esto demuestra que es una herramienta fiable y eficaz en los campos de la seguridad de la información y la auditoría de redes. Además, resaltan que enseñar a los estudiantes de carreras tecnológicas a manejar esta herramienta los prepara mejor para ingresar en el mercado laboral, lo que representa una ventaja adicional para la UNSCH en términos de formación de sus estudiantes de Ingeniería de Sistemas.

Hickman (2016), en su investigación titulada «Gaining Visibility on the Network with Security Onion: A Cyber Threat Intelligence Based Approach», tiene como objetivo proporcionar una guía para asegurar adecuadamente las redes. Destaca que las organizaciones pequeñas y medianas pueden aprovechar Security Onion para detectar y analizar el comportamiento malicioso en la red y generar datos e información que describen las distintas etapas de la Cyber Kill-Chain. El modelo Cyber Kill-Chain, desarrollado por Lockheed Martin (2015), describe las diferentes etapas de un ciberataque. Estos datos pueden ser utilizados por las organizaciones para detectar y mitigar los efectos de los ciberataques.

Como se puede apreciar, la capacidad de Security Onion para proporcionar información relevante y procesable ha sido ampliamente demostrada.

2.2. MARCO TEÓRICO

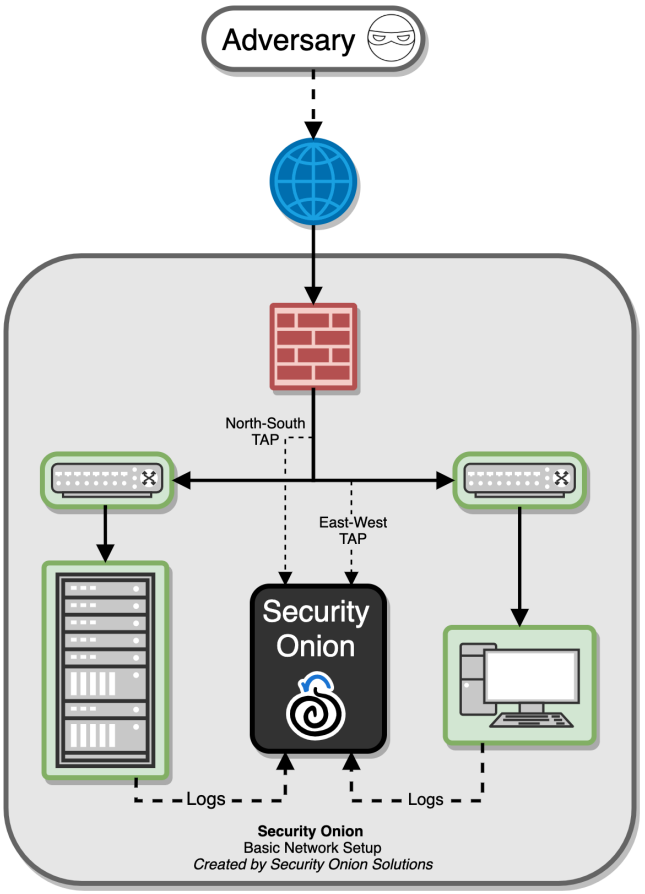
2.2.1. Security Onion

De acuerdo a la investigación realizada por Heenan & Moradpoor (2016), Security Onion es una plataforma orientada a la detección de intrusos basada en la distribución Ubuntu que contiene múltiples IDS's basados tanto en host (HIDS) como en red (NIDS). Proporciona detección basada en host en forma de OSSEC HIDS, y detección basada en red con la elección de Snort, Suricata y Bro NIDS. Esta plataforma puede configurarse en un servidor maestro con múltiples sensores o como un despliegue autónomo o híbrido, por lo que es extremadamente adaptable.

En la Figura 5 , tomada de la documentación oficial de Security Onion, vemos a esta plataforma en una red empresarial tradicional, aquí Security Onion puede servir para monitorizar el tráfico norte/sur y detectar a un adversario que entra en un entorno, estableciendo mando y control, o quizás exfiltración de datos. También se puede monitorizar el tráfico este/oeste para detectar movimientos laterales. Security Onion puede consumir los registros de sus servidores y estaciones de trabajo para que pueda buscar en todos los registros de su red y host al mismo tiempo.

Figura 5

Security Onion en una red empresarial tradicional con un cortafuegos, estaciones de trabajo y servidores



Nota. Adaptado de *Basic Network Setup*, de Security Onion Solutions, Security Onion 2.3. Documentation (https://docs.securityonion.net/en/2.4/introduction.html).

A continuación se describe lo básico respecto al uso, configuración, monitoreo, registro, gestión de seguridad y otros aspectos de esta distribución.

2.2.1.1. Uso de Security Onion

En nombre de la ISLE (The National University Information Security Lab Environment), Gonzales et al. (2015) ofrecen una visión general del entorno virtual de pruebas para tareas de formación en ciberseguridad. Proporciona ejemplos de ataques, como malware, botnet y tráfico honeypot, entre otros. El objetivo es proponer un marco para la ciberdefensa nacional y académica utilizando Security Onion.

2.2.1.2. Configuración de Security Onion

En el trabajo de investigación de Deuble & Shinberg (2012) se resume un conjunto de laboratorios que prueban varias vulnerabilidades de aplicaciones web, incluyendo Cross Site Scripting (XSS), inyección SQL (SQLi) e inyecciones del sistema operativo, contra una máquina virtual de aplicaciones web en el cual Security Onion muestra las capacidades de sus herramientas y servicios para proteger un entorno.

2.2.1.3. Monitoreo y registro

Meyer & Cid (2008) detectan ataques en aplicaciones web a partir de archivos de registro de solicitud del usuario y de respuesta, por lo que al ser reconocidos pueden ser bloqueados evitando explotaciones.

En otro estudio hecho por Gupta & Leune (2012) se explora la funcionalidad de análisis y generación de informes de las herramientas proporcionadas por Security Onion para sugerir un marco de alerta, registro y supervisión que se utilizará para garantizar que se cumplen los requisitos en términos de seguridad y niveles de servicio. Este estudio proporciona la sugerencia de que Security Onion es una solución adecuada para individuos u organizaciones que no tienen un gran presupuesto de seguridad.

2.2.1.4. Gestión de la seguridad

Hjelmvik (2015), en un taller práctico realizado por el Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST) de las Fuerzas Armadas Alemanas examina el uso de Security Onion para el análisis de intrusiones en redes y sistemas. Explora ataques diferentes y demuestra su capacidad de captura y análisis.

2.2.1.5. Taxonomía de Security Onion

La taxonomía de Security Onion, de acuerdo al estudio de Mobeen et al. (2021) se basa en tres categorías principales: métodos de despliegue, tipos de datos y herramientas.

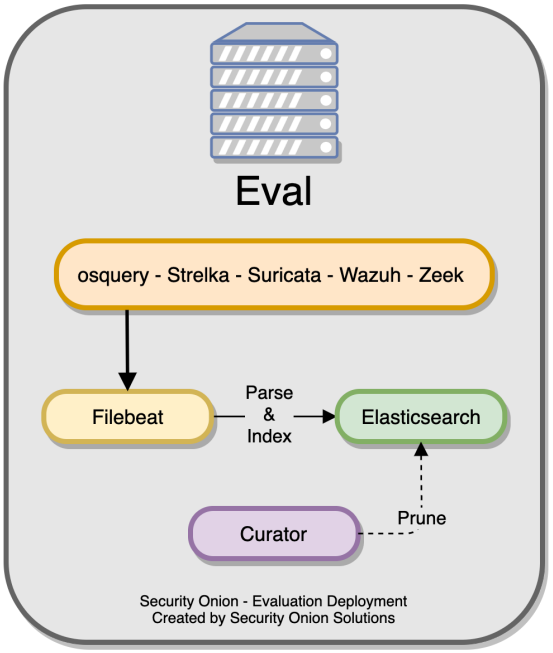
> ***Métodos de despliegue.*** Security Onion, según su documentación oficial, ofrece cuatro opciones de despliegue: importación, evaluación, independiente y distribuido.

La primera opción es la más sencilla. Utiliza un nodo de importación que es una caja independiente que ejecuta los componentes suficientes para importar archivos pcap mediante el comando *so-import-pcap* o archivos *evtx* mediante *so-import-evtx.*

La segunda, es un poco más complicada que la anterior porque tiene una interfaz de red dedicada a husmear tráfico en vivo desde un puerto TAP o span. Los procesos monitorizan el tráfico en esa interfaz de sniffing y generan logs. Como se observa en la Figura 6, Filebeat recoge esos registros y los envía directamente a Elasticsearch donde son analizados e indexados. El modo de evaluación está diseñado para una instalación rápida para probar temporalmente Security Onion. No está diseñado para su uso en producción.

Figura 6

Despliegue de evaluación



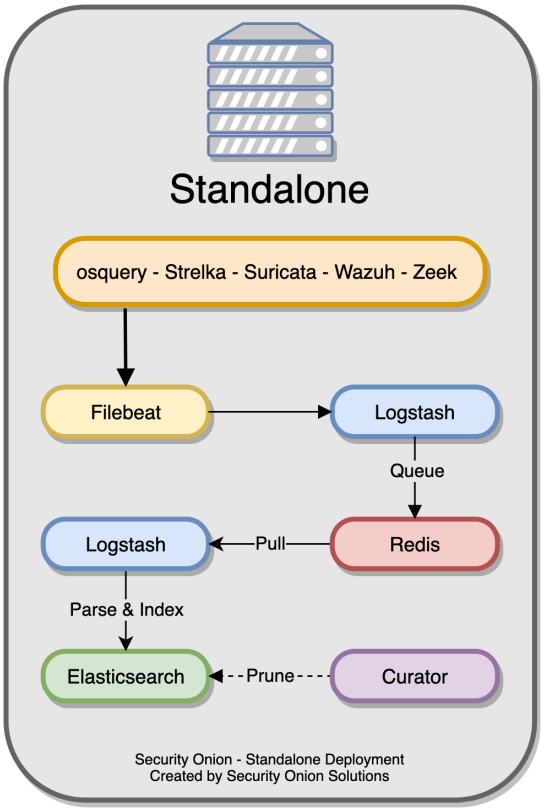
Nota. Adaptado de Security Onion - Evaluation Deployment, de Security Onion Solutions, Security Onion 2.3. Documentation (https://docs.securityonion.net/en/2.4/architecture.html#evaluation).

La opción de despliegue independiente es similar a la de evaluación en que todos los componentes se ejecutan en un solo equipo. Sin embargo, en lugar de que Filebeat envíe los registros directamente a Elasticsearch, los

envía a Logstash y este los envía a Redis para ponerlos en cola. Un segundo canal de Logstash extrae los registros de Redis y los envía a Elasticsearch, donde se analizan e indexan, este proceso está plasmado en la Figura 7. El despliegue independiente se utiliza normalmente para pruebas, laboratorios, POC o entornos de muy bajo rendimiento. No es tan escalable como un despliegue distribuido.

Figura 7

Despliegue independiente



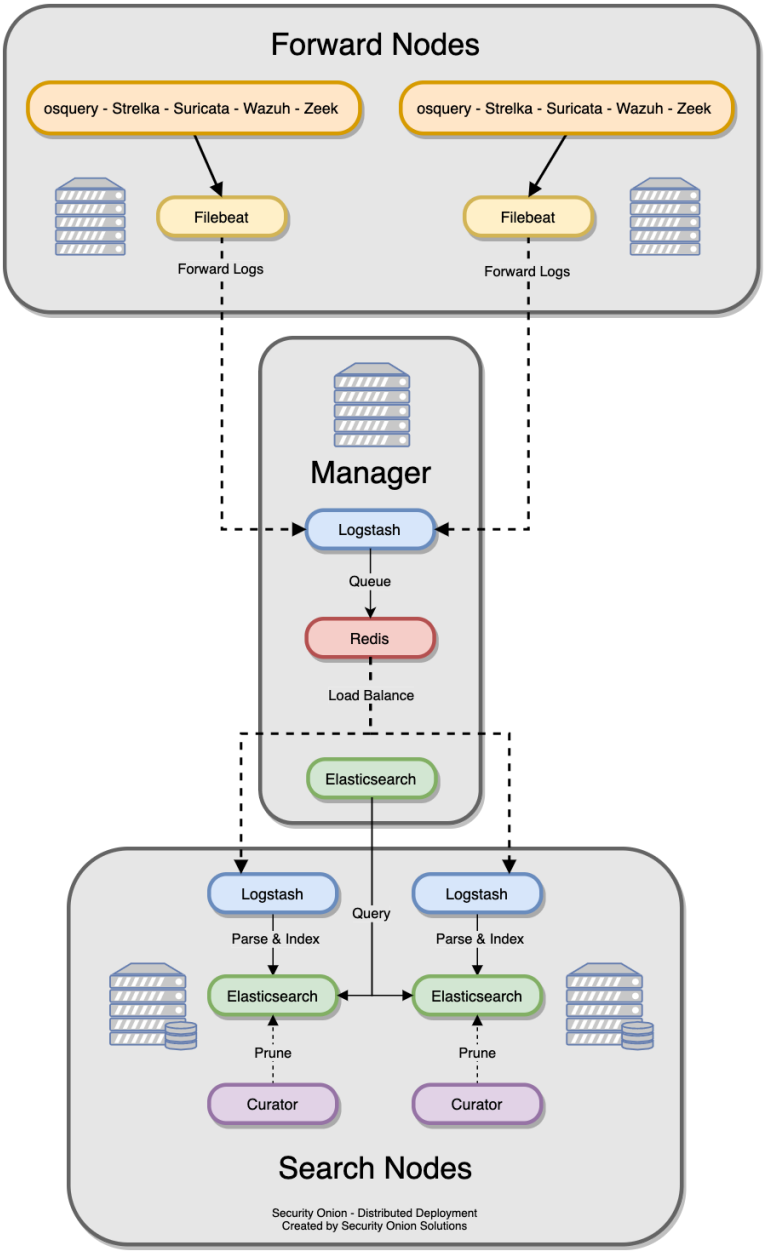
Nota. Adaptado de *Security Onion - Standalone Deployment*, de Security Onion Solutions, Security Onion 2.3. Documentation (https://docs.securityonion.net/en/2.4/architecture.html#standalone).

Por último tenemos al despliegue distribuido que se ejecuta en una sola máquina servidor o nodo gestor, también existen uno o más nodos de reenvío que, a su vez, ejecutan componentes de sensor de red y uno o más nodos de búsqueda que ejecutan componentes de búsqueda Elastic, luego la información solicitada se devuelve al cliente, muestra de esto la encontramos en la Figura 8. Se debe tener en cuenta que todo el tráfico

entre el cliente y el servidor está cifrado. Este tipo de despliegue puede tener un coste inicial más elevado, pero ofrece una mayor escalabilidad y rendimiento, ya que basta con añadir más nodos para gestionar más tráfico o fuentes de registro.

Figura 8

Despliegue distribuido



Nota. Adaptado de *Security Onion - Distributed Deployment*, de Security Onion Solutions, Security Onion 2.3. Documentation (https://docs.securityonion.net/en/2.4/architecture.html#distributed).

Tipos de datos. De acuerdo a Bejtlich (2013), los datos de monitorización de seguridad pueden clasificarse en:

- **Datos de sesión.** Son los datos resumidos asociados a una conversación de red. Se basan en las IP de origen y destino, los puertos y el protocolo de la capa de transporte.
- **Paquetes completos capturados.** También llamados datos de contenido completo registran todo el tráfico de red y detallan exactamente lo que se comunicó. Los datos se escriben en disco, normalmente en formato PCAP.
- **Datos de transacción.** Se sitúan entre los datos de sesión y la captura de paquetes completa. Captura los detalles asociados a las peticiones y respuestas.
- **Datos de alerta.** Son producidos por los sistemas de prevención de intrusiones (IPS). Las alertas se producen cuando el tráfico de red coincide con ciertas condiciones para las que los IPS están configurados para responder.
- **Datos estadísticos.** Los datos de alerta pueden ser procesados para producir datos estadísticos. Por ejemplo, ¿cuántas peticiones por segundo recibe normalmente este servidor web? ¿Cuántas peticiones DNS por segundo se hacen desde dentro? ¿Con qué frecuencia se conecta un usuario a ese sistema? ¿Existen ciclos en los patrones de datos basados en lapsos de tiempo?
- **Metadatos.** Los metadatos se utilizan para aumentar los datos del NSM. Se recogen directamente mediante la geolocalización, las puntuaciones de reputación y las titularidades asociadas a las direcciones IP.

Herramientas. A continuación, se enumeran las herramientas de Security Onion, aclarando que la información al respecto se ha extraído de sus respectivas documentaciones oficiales.

- **Wazuh.** Es una solución de supervisión de la seguridad gratuita, de código abierto y preparada para pequeñas y grandes empresas. Permite detectar amenazas, supervisar la integridad, responder a incidentes y cumplir la normativa.

Esta herramienta es utilizada por Security Onion como Sistema de Detección de Intrusiones en el Host (HIDS) en cada uno de los nodos.

- **Stenographer.** Como se menciona en su documentación oficial, es una solución de captura de paquetes cuyo objetivo es enviar rápidamente todos los paquetes al disco y, a continuación, proporcionar un acceso sencillo y rápido a subconjuntos de esos paquetes.
- **Suricata.** Es un motor de detección de amenazas de red gratuito de código abierto que se caracteriza por su madurez, velocidad y robustez. Utiliza un poderoso y extenso lenguaje de reglas y firmas para inspeccionar el tráfico de red, y cuenta con un sólido soporte de scripts Lua para la detección de amenazas complejas.
- **Intrusion Detection Honeypot (IDH).** Es, de acuerdo al promotor de este concepto, Chris Sanders, un recurso de seguridad colocado dentro del perímetro de una red que genera alertas cuando es sondeado o atacado. Estos sistemas, servicios y tokens convencen al atacante de interactuar y alertan de la interacción sin que este lo sepa, lo que permite investigar el ataque posteriormente.
- **Zeek.** Anteriormente conocido como Bro, es un analizador de tráfico de red pasivo y de código abierto. Puede ser utilizado como monitor de seguridad de red (NSM) con el objetivo de ayudar en las investigaciones de actividades sospechosas o maliciosas. Admite una amplia gama de tareas de análisis de tráfico más allá del ámbito de la seguridad, como la resolución de problemas y la medición del rendimiento.
- **Strelka.** Es un sistema de exploración de archivos en tiempo real basado en contenedores utilizado para la caza y detección de amenazas, además de la respuesta a incidentes. Su propósito es realizar la extracción de archivos y la recopilación de metadatos a gran escala. Está basada en el diseño establecido por Laika BOSS de Lockheed Martin y otros proyectos similares.

- **Elasticsearch.** Este motor de búsqueda y análisis distribuido y abierto basado en Lucene[1] está diseñado para procesar texto, números, fechas, datos de geolocalización y otros. Es capaz de abordar una amplia variedad de casos de uso en tiempo real. Algunos ejemplos incluyen el análisis de logs, la monitorización de la infraestructura, la búsqueda de documentos y el análisis de tendencias de redes sociales.
- **ElastAlert.** Es un framework sencillo que brinda alertas sobre anomalías, picos u otros patrones de datos en Elasticsearch y OpenSearch.
- **osquery.** Es un marco de instrumentación de sistemas operativos para Windows, OS X (macOS) y Linux. Expone a estos como bases de datos relacionales de alto rendimiento, lo que le permite escribir consultas SQL para explorar sus datos.

  Se debe elegir osquery en Security Onion si desea algunas acciones de respuesta en vivo y tal vez un transporte ligero de registros. Un buen ejemplo es un portátil itinerante donde el volumen de registros es bajo y es posible que desee enviar sus registros a otro nodo dedicado.
- **Sysmon.** Es un servicio del sistema operativo Windows y un controlador de dispositivo que supervisa y controla la actividad en el registro de eventos del SO. Proporciona información detallada sobre la creación de procesos, conexiones de red y cambios en el tiempo de creación de archivos, lo que incluye el registro de la creación de archivos en directorios inusuales o el uso de comandos de red poco comunes. Además, es capaz de detectar actividades sospechosas, como intentos de explotación de vulnerabilidades conocidas o cambios en la configuración del sistema.
- **Kibana.** Es una herramienta de visualización de datos de código abierto que ofrece una interfaz de usuario intuitiva para explorar y analizar la información almacenada en Elasticsearch. Con Kibana,

[1] Lucene es una biblioteca de búsqueda de texto completo de código abierto escrita en Java. Fue desarrollada originalmente en 1999 por Doug Cutting, quien más tarde también creó Hadoop. Proporciona una API de búsqueda potente y flexible que permite a los desarrolladores indexar y buscar grandes cantidades de texto. Se utiliza en muchos proyectos de búsqueda y recuperación de información, desde pequeñas aplicaciones de búsqueda hasta grandes sistemas de búsqueda web y empresariales.

los usuarios pueden crear gráficos, diagramas y mapas interactivos a partir de los datos, lo que facilita la identificación de patrones y tendencias. También permite crear paneles personalizados para monitorear en tiempo real los indicadores clave de rendimiento (KPI) de una organización y compartirlos con otros miembros del equipo de manera sencilla.

2.2.2. Auditoría de redes

Auditar no es sólo ejecutar un montón de herramientas de hackeo para intentar entrar en la red. De hecho, este término se refiere, de acuerdo al artículo de N-able Solutions ULC and N-able Technologies (2020), al proceso de recopilación, análisis y estudio de datos de red con el propósito de evaluar la salud de la misma, lo que proporciona a las empresas u organizaciones información sobre el éxito de sus operaciones de control y gestión de red, especialmente en lo que respecta a las normativas de cumplimiento internas y externas.

2.2.2.1. Redes y su seguridad

Red informática. Según la definición otorgada por Shin (2021), la red informática representa un conjunto de enlaces de comunicación cableados e inalámbricos a través de los cuales una variedad de componentes de hardware y software intercambian datos e información. Una red puede ser tan pequeña como la instalada en una casa y tan grande como Internet, que abarca todo el planeta.

Términos clave de la seguridad de redes y la ciberseguridad. Antes de desarrollar las siguientes secciones es conveniente entender, en términos generales, algunos términos clave básicos.

- **Amenaza.** Son peligros que pueden causar daño si actúan sobre un objetivo individual u organizativo y son técnicamente intensivas (por ejemplo, software malicioso) o menos técnicas (por ejemplo, estafas, ingeniería social). La fuente de la amenaza puede ser externa (por ejemplo, atacantes del ciberespacio), interna (por ejemplo, empleados descontentos) o relacionada con la cadena de suministro (por ejemplo, un proveedor de piezas). Cuando el actor de la amenaza actúa contra una organización, esta amenaza en acción se

convierte en un ataque. Así pues, existe una sutil diferencia entre la amenaza como potencial y el ataque como acción, aunque ambos términos se utilicen con frecuencia indistintamente.

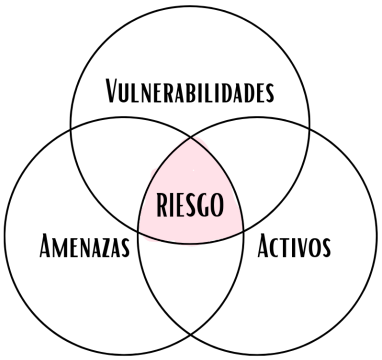
Aquí se encuentran el malware, el spam y el phishing.

- **Agente de amenaza o atacante.** También llamado adversario, es un individuo que lleva a cabo una amenaza o ataque, y puede ser una entidad externa o interna. Si el actor de la amenaza consigue su objetivo, se producen consecuencias/daños en la organización víctima, algunas de las cuales son: el robo de datos, pérdidas financieras, pérdida de reputación, debilitamiento de la confianza de los clientes e incluso la pérdida de vidas.
- **Vector de amenaza/ataque.** Es un camino, punto de entrada o ruta que un agente de amenaza explota para activar la amenaza. Es decir, se supone que el vector en sí es benigno por diseño, pero los atacantes abusan de él para lanzar amenazas. Por ejemplo, un adversario puede enviar malware (es decir, una amenaza) adjuntándolo a un correo electrónico (es decir, un vector de amenaza). Existen muchos vectores de amenaza pero el correo electrónico sigue siendo el principal vector de amenaza.

  Los vectores de amenaza no están destinados a ser peligrosos, sino que simplemente se convierten en un canal o conducto explotado por el actor de la amenaza para entregar amenazas, montando un ataque.
- **Vulnerabilidad.** Es una forma de debilidad con probabilidades de ser explotada. Cualquier organización tiene, inevitablemente, vulnerabilidades. Pueden ser defectos relacionados con el software instalado, sea desarrollado internamente o adquirido a un proveedor. También puede producirse debido a falta de políticas o procedimientos relacionados a la seguridad.
- **Riesgo.** Se refiere al potencial de pérdida o daño cuando un actor de amenaza explota una o más vulnerabilidades del objetivo. Por lo general, el nivel de riesgo se mide en función de las amenazas, las vulnerabilidades y los activos (véase la Figura 9).

Figura 9

Riesgo visto en función de amenazas, vulnerabilidades y activos



- **Seguridad.** Es un proceso continuo de protección de una persona, una organización o una propiedad (como un sistema informático) o un archivo frente al acceso no autorizado.

  Según Kizza (2020), un objeto puede estar en un estado físico de seguridad o en un estado teórico de seguridad. En un estado físico, una instalación es segura si está protegida por una barrera como una valla, tiene zonas seguras tanto dentro como fuera y puede resistir la penetración de intrusos. Un estado teórico de seguridad, comúnmente conocido como pseudo seguridad o seguridad a través de la oscuridad (STO), es una falsa esperanza de seguridad. Muchos creen que un objeto puede ser seguro siempre y cuando nadie fuera del grupo central de implementación tenga conocimiento de su existencia. Esta seguridad se basa sólo en una filosofía.

Tipos de amenaza. De acuerdo a Shin (2021), el esquema taxonómico de los tipos de amenazas, mostrado en la Tabla 1, se basa en el principal mecanismo empleado. Las categorías no son necesariamente excluyentes entre sí, ya que lo más probable es que un adversario combine múltiples técnicas para lograr su objetivo.

Tabla 1

Principales mecanismos de amenazas o ciberataques

Mecanismo de amenaza	Definición
Ingeniería social	Los atacantes o actores de la amenaza engañan a la víctima para que entregue información privada o visite un sitio maligno.
Inyección de un software malicioso	Los atacantes o actores de la amenaza distribuyen malware que infligen los daños previstos. Algunos problemas causados pueden ser: - Molestias - Atasco del servidor de correo - Denegación de servicio (DoS) - Pérdida de datos - Agujeros abiertos para que otros accedan a la máquina
Aprovechamiento de una configuración de seguridad débil o errónea	Los atacantes o actores de amenazas aprovechan la falta de configuración de seguridad de un sistema, su configuración débil o mal realizada.
Abuso de una función de red o de un protocolo	Los actores de amenazas o atacantes lanzan un ataque aprovechando las características funcionales incorporadas en un protocolo de red.
Explotación de los fallos de diseño y/o desarrollo del software	Los actores de amenazas o atacantes descubren fallos técnicos de un programa de software (por ejemplo, un navegador o un sistema operativo) para aprovecharse de ellos.
Compromiso de las protecciones criptográficas	Los actores de amenazas o atacantes intentan neutralizar la tecnología de seguridad (por ejemplo, la criptografía) o su protección (por ejemplo, datos cifrados en reposo o en tránsito).
Rastreo de paquetes	Los atacantes o actores de amenazas insertan un dispositivo en la red que le permita ver los paquetes de datos en busca de un paquete de datos Telnet o FTP (o un paquete de alguna aplicación que tiene inicios de sesión sin cifrar, es decir, en forma legible para el ser humano) para obtener el nombre de usuario y la contraseña en uno de los componentes de la red. Algunos rastreadores de paquetes o ataques de rastreo son: - Ataque de hombre en el medio (Man in the middle - MitM), conocido también como ataque en ruta. - Envenenamiento de caché ARP - Salto de VLAN

Tipos de vulnerabilidades. No existe una lista definitiva de las fuentes de vulnerabilidades, pero en este trabajo de investigación se clasificaron de manera general en cuatro tipos como se muestra en la Tabla 2, tomando en cuenta la propuesta de Shin (2021).

Tabla 2

Cuatro grandes tipos de vulnerabilidades

Tipo	Definición
Vulnerabilidades de software	Se trata de defectos en el sistema operativo, la aplicación de la organización, el navegador web o sus complementos u otro programa de productividad o comunicación. Como resultado de un mal diseño y/o desarrollo del software, los defectos permiten a los atacantes o agentes de amenaza aprovecharse de ellos (por ejemplo, saltarse las medidas de seguridad).
Débil o mala configuración	Algunas vulnerabilidades se deben a una configuración de seguridad deficiente o incorrecta. Por ejemplo, si el administrador de un sistema utiliza credenciales por defecto simples o por defecto, al desplegar nodos de red, esto se convierte en una invitación a los problemas.
Vulnerabilidades de hardware	Las limitaciones en la capacidad del hardware pueden convertirse en una fuente de vulnerabilidades. Por ejemplo, un servidor web que acepta y procesa peticiones de clientes cuya capacidad de CPU o memoria es limitada no podrá resistir un ataque DDOS (denegación de servicio distribuida). Otro ejemplo, si los ordenadores servidores y/o los dispositivos intermediarios se sitúan en un lugar que no está físicamente protegido, facilitará que un agente de amenazas (por ejemplo, alguien con información privilegiada) acceda físicamente a los recursos de hardware y a los activos de datos almacenados.
Vulnerabilidades no técnicas	Son cuestiones operativas y de gestión de riesgos. Algunos ejemplos son la debilidad en la gestión de activos (por ejemplo, la falta de documentación), la ausencia de políticas y procedimientos de seguridad o una existencia incompleta. También existen vulnerabilidades del lado humano ante las estafas de phishing y ciberamenazas debido a su limitada exposición a iniciativas de formación y concienciación sobre ciberseguridad.

Seguridad de red. Es una rama de la informática mucho más amplia que la seguridad informática por lo que implica diseños matemáticos más detallados de protocolos criptográficos, de comunicación, de transporte y de intercambio, así como las mejores prácticas. Su objetivo es crear un entorno en el que una red, incluidos todos sus recursos o elementos, los datos que

contiene tanto en almacenamiento como en tránsito, y sus usuarios estén protegidos. Sin embargo, como menciona Jackson (2010), "la seguridad es un proceso, no un producto".

2.2.2.2. Ataques a la seguridad de red

Una red de campus, como la red de la Universidad Nacional de San Cristóbal de Huamanga es vulnerable a muchos tipos de ataques de red.

Chakraborty et al. (2020) mencionan que los ataques a la seguridad de la red son actividades ilegales llevadas a cabo por actores no autorizados contra activos informáticos privados, corporativos o gubernamentales con el fin de destruirlos, modificarlos o robar datos sensibles.

Existen principalmente dos tipos de ataques a la red: el ataque pasivo y el ataque activo.

Ataque pasivo. Tiene como objetivo principal robar información sensible, lo que ocurre sin el conocimiento de la víctima. Estos ataques son difíciles de detectar y, por tanto, de proteger la red. A continuación se mencionan algunos ataques pasivos existentes, de acuerdo a Laurent & Bouzefrane (2015).

- **Análisis del tráfico.** El atacante detecta la ruta de comunicación entre el emisor y el receptor.
- **Monitorización.** El atacante puede leer los datos confidenciales, pero no puede editarlos ni modificarlos.
- **Espionaje.** Este tipo de ataque se produce en la red móvil ad-hoc, donde básicamente el atacante descubre alguna información secreta o confidencial de la comunicación.

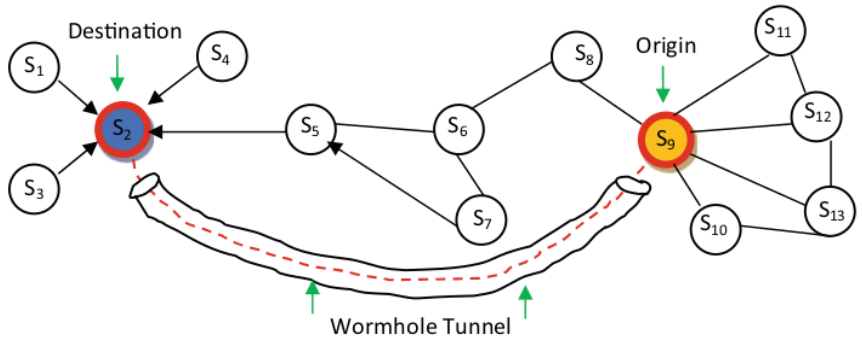
Ataque activo. Este tipo de ataques se producen de tal manera que notifican a las víctimas que sus sistemas han sido comprometidos. Como resultado, la víctima puede interrumpir la comunicación con la otra parte. De acuerdo a Vinod et al. (2018), algunos de los ataques activos son los siguientes:

- **Modificación.** El nodo malicioso realiza alteraciones en la ruta de encaminamiento. Esto provoca que el remitente envíe mensajes a través de una ruta larga, lo que causa un retraso en la comunicación. Se trata de un ataque a la integridad.

- **Agujero de gusano.** Este ataque también se denomina ataque de túnel. Un atacante recibe un paquete en un punto. Luego lo tuneliza a otro nodo malicioso de la red. Esto hace que un principiante asuma que ha encontrado el camino más corto en la red, como se muestra en la Figura 10.

Figura 10

Ataque de agujero de gusano

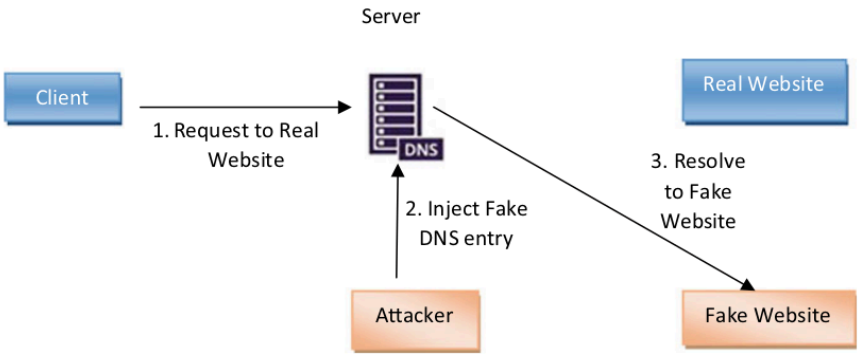


Nota. Adaptado de *Wormhole*, de *The "Essence" of Network Security: An End-to-End Panorama* (p.8), por M. Chakraborty et al., 2020, Springer Nature Singapore.

- **Fabricación.** Un nodo malicioso genera un mensaje de enrutamiento falso que provoca la generación de información incorrecta sobre la ruta entre dispositivos. Se trata de un ataque a la autenticidad.
- **Suplantación.** Un nodo malicioso falsea su identidad para que el remitente cambie su topología. Se ve un ejemplo gráfico en la Figura 11.

Figura 11

Suplantación

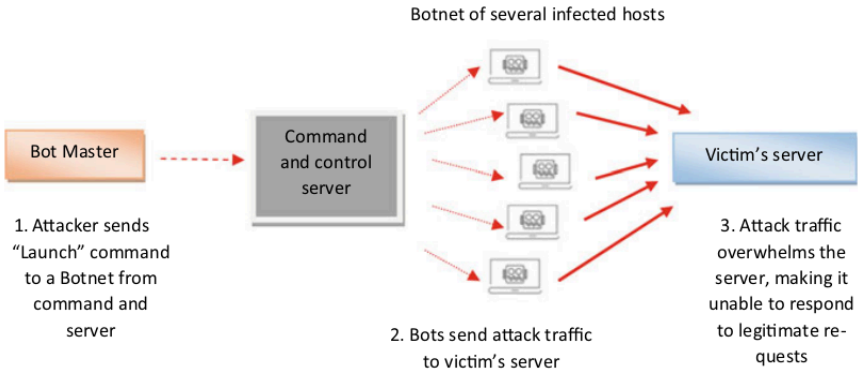


Nota. Adaptado de *The "Essence" of Network Security: An End-to-End Panorama* (p.8), por M. Chakraborty et al., 2020, Springer Nature Singapore.

- **Denegación de servicios.** Este ataque consiste en que un nodo malicioso envía un mensaje a otro y consume el ancho de banda de la red, tal como en la Figura 12.

Figura 12

Ataque de denegación de servicio

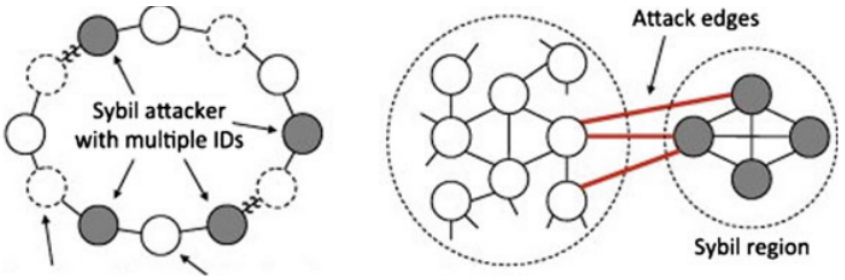


Nota. Adaptado de *The "Essence" of Network Security: An End-to-End Panorama* (p.9), por M. Chakraborty et al., 2020, Springer Nature Singapore.

- **Sinkhole (ataque al servicio).** Este tipo de ataque impide que la estación base obtenga información completa y correcta. Un nodo malicioso intenta extraer los datos o paquetes de todos sus nodos adyacentes. Este ataque puede provocar la pérdida de paquetes, la alteración selectiva o el reenvío de datos.
- **Sibila.** Este ataque está relacionado con las copias múltiples del nodo malicioso. Un nodo malicioso envía en secreto su clave encubierta a otros nodos maliciosos que luego la utilizan para atacar a las víctimas mediante el enrutamiento múltiple. De este modo, la red de nodos maliciosos aumenta, lo que incrementa la posibilidad de ataques. La probabilidad de selección de una ruta por parte del nodo malicioso aumentará en la red, un ejemplo de esto se puede observar en la Figura 13.

Figura 13

Ataque Sibila o Sybil



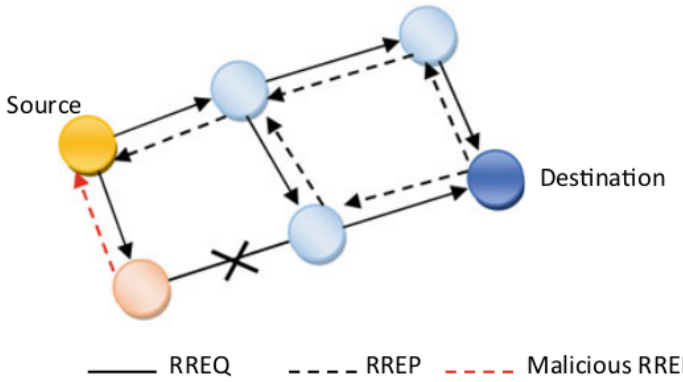
Nota. Adaptado de *The "Essence" of Network Security: An End-to-End Panorama* (p.10), por M. Chakraborty et al., 2020, Springer Nature Singapore.

Ataque avanzado. Es un ataque en el que un usuario no autorizado accede a una red y permanece en él durante un largo periodo de tiempo sin ser detectado. Son especialmente peligrosas para las empresas, ya que terceros tienen acceso continuo a sus datos sensibles. Algunos ejemplos de estos ataques son los mencionados a continuación:

- **Ataque de agujero negro.** Un atacante nota la mejor ruta de enrutamiento hacia el nodo cuyos paquetes quiere interceptar. Primero, utiliza el protocolo basado en inundación para listar la solicitud de una ruta del emisor llamada Routing Request (RREQ); segundo, crea un mensaje de respuesta llamado Routing Replay (RREP) indicando que tiene el camino más corto hacia el receptor. Como este mensaje llega al iniciador antes que la respuesta del nodo real, este considerará que es el camino más corto hacia el receptor. De este modo, se crea una ruta falsa maliciosa. Un ejemplo gráfico se presenta en la Figura 14.

Figura 14

Ataque de agujero negro



Nota. Adaptado de *The "Essence" of Network Security: An End-to-End Panorama* (p.10), por M. Chakraborty et al., 2020, Springer Nature Singapore.

- **Ataque apresurado (Rushing attack).** Cuando el emisor envía el paquete al receptor, el atacante altera el paquete y lo reenvía al receptor. El atacante realiza el duplicado y envía la copia al receptor una y otra vez por lo que el receptor asume que los paquetes provienen del emisor.
- **Ataque de repetición.** Ocurre cuando un nodo malicioso repite los datos o los retrasa de tal forma que se retransmiten y en ese momento un atacante intercepta la información.
- **Ataque bizantino.** De acuerdo al estudio realizado por Saini & Singh (2016), entre el emisor y el receptor, un conjunto de nodos transitorios modifican algunas de las tareas para crear bucles de enrutamiento adicionales, descartar paquetes legítimos e incluso intentar enviar paquetes a través de una ruta no óptima. Esto produce una perturbación o privación de los servicios de encaminamiento/enrutamiento.
- **Ataque de revelación de ubicación.** Los atacantes analizan el tráfico entre las partes comunicantes para comprender la estructura de la red, al revelar la ubicación de los nodos o la configuración de la infraestructura de red, recopila esa información como un mapa de rutas y luego planifica otros escenarios de ataque.

- **Ataque de intermediario (Man-in-the-middle Attack).** También llamado ataque de secuestro, en el que el atacante altera y retransmite en secreto las comunicaciones entre dos partes legítimas sin su conocimiento.

Software malicioso o malware. Según Disso & Younas (2018), se trata de software utilizado o creado para perturbar el funcionamiento de los ordenadores, recopilar información sensible y obtener acceso a sistemas informáticos privados.

Es un término general utilizado para referirse a una variedad de formas de software hostil, intrusivo o molesto que se propaga de diversas formas para crear estragos y robar información sensible. Los daños que causan son graves y pueden provocar pérdida de datos, robo de cuentas, daños a través de botnets, pérdidas financieras, etc. Como se muestra en la Tabla 3, existen diversos tipos de malware que pueden provocar estos daños.

Tabla 3

Visión general de los tipos de malware más usuales

Tipo de malware	Definición
Virus	Programa o fragmento de código que se carga en nuestro ordenador sin nuestro conocimiento y se ejecuta en contra de nuestros deseos. Los virus pueden replicarse a sí mismos y auto-copiarse en otros discos para propagarse a otros ordenadores. Pueden ser molestos o enormemente destructivos para nuestros archivos.
Caballo de Troya	No se replica ni se copia a sí mismo, sino que causa daños o compromete la seguridad del ordenador. Un Caballo de Troya es enviado o transportado por otro programa y puede llegar en forma de un software ùtil. A menudo se utilizan para capturar nuestros inicios de sesión y contraseñas.
Gusano	Es un programa informático autorreplicante que se propaga a través de una red y puede enviar copias de sí mismo a otros nodos, sin necesidad de intervención del usuario. Puede causar graves daños, como la ralentización o el colapso de los sistemas, el robo de información confidencial o la infección de otros equipos. Un ejemplo conocido de gusano informático es el gusano "ILOVEYOU", que se propagó por correo electrónico en el año 2000.

Spyware o software espía	Se instala en los ordenadores con el objetivo de recopilar información de los usuarios sin su conocimiento y transferirla de forma clandestina a terceros involucrados en actividades ilícitas. El spyware suele permanecer oculto al usuario y puede ser difícil de detectar.
Zombie	Toman el control de los ordenadores de las víctimas y los utilizan para crear una red con la que atacar a otros ordenadores conectados a ellos para realizar otros actos maliciosos.
Phishing	Son ataques en forma de mensaje inocente que engaña a la víctima para que proporcione información valiosa y secreta, como los datos de su cuenta bancaria, el identificador de usuario y la contraseña de un sitio web, etc. El mensaje puede indicar que si no se accede a un sitio web y no se facilita la información requerida, la cuenta puede quedar inactiva y los datos o el dinero pueden ser confiscados.
Spam	Es un correo electrónico no solicitado y no deseado. Se utiliza mucho para multiplicar troyanos, virus y otros programas maliciosos.
Adware	Abreviatura de advertising-supported software; se encarga de mostrar publicidad de forma automática. A menudo, el adware se instala en el sistema informático sin conocimiento del usuario y puede ser difícil de eliminar. Además de ser una molestia, puede ralentizar la velocidad del sistema, disminuir la estabilidad y seguridad, y exponer a los usuarios a otros tipos de malware. Ejemplos comunes son los anuncios emergentes en sitios web o software y a menudo se incluyen en versiones "gratuitas" de programas y aplicaciones.
Ransomware	Es un tipo de malware que mantiene cautivo un sistema informático y exige un rescate. A menudo, restringe el acceso al ordenador mediante la encriptación de los archivos del disco duro o bloqueando el sistema y mostrando mensajes amenazantes que intentan forzar al usuario a pagar al creador del malware para recuperar el acceso a su ordenador. Un ejemplo de mensaje de ransomware es el siguiente: *¡ATENCIÓN! Sus archivos personales han sido cifrados. Si desea recuperarlos, debe seguir nuestras instrucciones. No intente eliminar el programa o descifrar los archivos por su cuenta, esto puede causar la pérdida permanente de sus datos.*

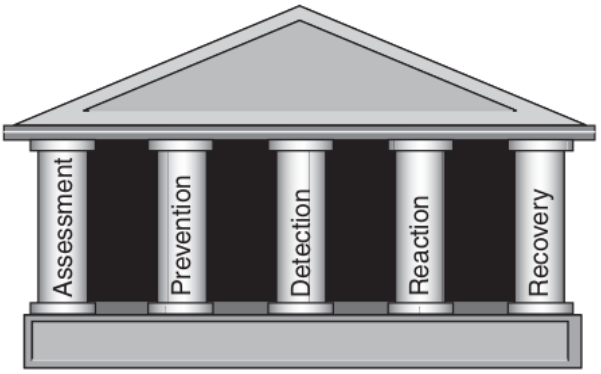
2.2.2.3. Principios de la auditoría de redes

Tal como menciona Jackson (2010), la auditoría es uno de los aspectos más importantes del mantenimiento de un sistema o red ya que ofrece la oportunidad de poner a prueba su seguridad y compararla con las normas y reglamentos por lo que se deben tener en cuenta ciertos conceptos fundamentales.

Pilares de la seguridad. Para entender la seguridad y la auditoría debemos ser capaces de identificar cómo se relaciona todo conceptualmente. La seguridad es uno de los pocos temas que afecta a todos los aspectos de una empresa. Desde el centro de datos hasta la sala de descanso, cada función de una empresa tiene su propia lista de cosas que deben protegerse de un cierto nivel de riesgo. Gestionar el riesgo es uno de los factores más importantes a la hora de desarrollar una estrategia para proteger a las personas, la tecnología y los datos. Para centrar los esfuerzos de seguridad y hacerlos manejables es conveniente desglosar los diversos aspectos de la seguridad en los cinco pilares de la seguridad como se puede ver en la Figura 15.

Figura 15

Cinco pilares de la seguridad



Nota. Adaptado de *Network security auditing* (p.27), por Chris Jackson, 2010, Cisco Press.

- **Evaluación.** El primer paso para proteger los activos de una organización es evaluar el entorno. Esto nos permitirá comprenderlo y, a su vez, identificar las áreas, activos, procedimientos, entre otros, que la empresa considera más importantes y son más sensibles a la interrupción o al robo.

  Jackson (2010) menciona que este proceso implica formular preguntas concretas. Lo primero es estudiar el terreno (tecnología disponible) para determinar si es adecuado construir. También debemos saber si la zona es propensa a las inundaciones (amenazas). ¿Con qué frecuencia se inunda (frecuencia de las

amenazas)? ¿Dispone de los permisos adecuados (leyes y normativas)? ¿Cuáles son las normas de la obra (política y procedimiento)? Formular preguntas similares sobre la seguridad de la empresa permite examinar diversos escenarios para identificar puntos débiles en las defensas o los procedimientos.

Las evaluaciones no son algo que se hacen una vez y luego se olvidan, sino que deben realizarse periódicamente a medida que cambian las necesidades de la organización o se introducen nuevos servicios y tecnologías. De este modo, se ponen a prueba las políticas y los procedimientos para asegurar que aún son adecuados.

- **Prevención.** Abarca controles administrativos, operativos y técnicos. La prevención no se consigue sólo con tecnología, sino también con políticas, procedimientos y concienciación.

  Las políticas y procedimientos deben documentarse y aplicarse de forma estricta y con consecuencias en caso de infracción. Las buenas prácticas de seguridad pueden ayudar a prevenir la mala configuración, que es uno de los métodos más comunes que utilizan los atacantes para comprometer un sistema. Ayudar a los usuarios a entender lo que está permitido y lo que no, además de una aplicación coherente y justa, contribuye en gran medida a reducir el riesgo general para una empresa.

  Los controles técnicos de seguridad, como los cortafuegos o los sistemas de prevención de intrusiones, desempeñan un papel importante a la hora de mantener segura una red, pero no son una bala de plata que se pueda conectar y esperar que resuelva todos los problemas de seguridad.
- **Detección.** Este proceso es imprescindible e implica la identificación de la existencia o inexistencia de una violación de la seguridad o una intrusión. Sin mecanismos de detección adecuados se corre el riesgo de no saber si la red se ha visto comprometida por lo que no sería factible formular una reacción adecuada que permita recuperar los servicios o activos lo antes posible.
- **Reacción.** Cuando la prevención y la detección son eficaces, el tiempo de reacción se reduce considerablemente.

El objetivo es reducir al mínimo el tiempo que transcurre desde la detección hasta la respuesta, de modo que se minimice la exposición al incidente. Una reacción rápida depende de la prevención y la detección para proporcionar los datos y el contexto necesarios para reconocer una violación de la seguridad.

Aunque la organización no disponga de un equipo especializado, un poco de previsión, planificación y la forma de reaccionar ante un incidente pueden marcar la diferencia.

- **Recuperación.** La recuperación consiste en determinar qué ha fallado y volver a poner en marcha los sistemas sin abrir la misma vulnerabilidad o condición que causó el problema en primer lugar. ¿Se parchea la vulnerabilidad explotada y se recuperan los datos de la copia de seguridad o hay un fallo mayor en los controles de seguridad que permitió que se produjera el incidente? ¿Cuál fue la razón por la que el sistema se vio comprometido? ¿Cómo fallaron los controles técnicos? ¿Hubo un error de configuración? La fase de recuperación no termina con la puesta en línea del sistema. También está la determinación de los cambios que deben introducirse en los procesos, procedimientos y tecnologías para reducir la probabilidad de que se produzca el mismo incidente en el futuro. En este proceso de la auditoría, se debe asegurar que la organización tenga un plan de recuperación que aborda estas cuestiones.

Programa de seguridad. Las políticas, procedimientos y normas representan la base de un programa de seguridad. Son los documentos que detallan quién, qué, cuándo y cómo proteger los activos y recursos de la empresa. Sin embargo, muchas organizaciones siguen sin disponer de un conjunto formal de políticas y procedimientos para la seguridad de la información por lo que aumenta el riesgo de que ocurran cosas malas con los datos.

Una parte esencial de la auditoría consiste en examinar las políticas, procedimientos y normas de una organización para asegurarse de que son completas, aplicables y se cumplen.

Tabla 4

Bases de un programa de seguridad en una organización

Base de un programa de seguridad	Descripción
Políticas	Definen el porqué se aplica la medida de seguridad, qué se protege y a quién se aplica; deben ser claras, concisas y libres de ambigüedades. Se puede pensar en ellas como el plano para construir la estructura del programa de seguridad. Como mínimo, una buena política de seguridad incluye lo siguiente: - Propósito: Porqué existe la política. - Ámbito: A quién o a qué se aplica la política. - Declaración de política: Los requisitos, detalles específicos sobre lo que está permitido o prohibido. No debe estar abierta a interpretaciones. - Aplicación: Proporciona un punto de aplicación para la disciplina o el enjuiciamiento en caso de incumplimiento. - Términos y definiciones: Aclaración de la terminología utilizada en la declaración de la política. - Historial de revisiones: Resumen de los cambios introducidos en la política, con fecha de modificación, persona o grupo que inició el cambio y un resumen de lo que se modificó.
Procedimientos	Son instrucciones detalladas sobre cómo debe aplicarse una política y proporcionan un manual de operaciones. Cada política debe incluir un documento de procedimiento complementario. Los elementos generales que los conforman son: - Propósito: Explica por qué existe el procedimiento y cuál es la política de origen. - Alcance: Explica quién es el responsable de la ejecución del procedimiento y a qué situación o tecnología se aplica. - Advertencias: Incluye advertencias de seguridad o protección que deben seguirse para mantener la integridad. - Pasos del procedimiento: Procedimientos detallados que deben seguirse para configurar o aprovisionar la tecnología cubierta por el procedimiento. - Historial de revisiones: Resumen de cambios y fecha de la última actualización o revisión del procedimiento.
Normas o estándares	Dictan los controles o configuraciones necesarios que se consideran las mejores prácticas para crear procedimientos. Afortunadamente, hay muchas normas bien documentadas disponibles en los organismos de normalización.

Controles de seguridad. Son los bloques para construir un programa de seguridad, son herramientas que se implementan para proteger la

integridad, confiabilidad y disponibilidad de los activos importantes y los datos.

La clasificación general de los controles de seguridad puede determinarse en tres grandes grupos: administrativos, técnicos y físicos.

- **Administrativos:** Se enfocan en la gestión de personas y procesos para disuadir del fraude o comportamiento indebido a través de políticas y procedimientos.
- **Técnicos:** Son esenciales para prevenir y hacer cumplir comportamientos en la red o en los recursos informáticos. Estos controles pueden ser implementados para asegurar la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Además, deben ser revisados y actualizados periódicamente para garantizar su eficacia. Dentro de los controles técnicos encontramos: sistemas de prevención de intrusiones (IPS), sistemas de prevención de intrusiones en host (HIPS), control de acceso basado en roles (RBAC) o cualquier otro mecanismo para aplicar políticas.
- **Físicos:** Están diseñados para restringir el acceso a dispositivos y zonas sensibles. Incluyen sistemas de acceso con tarjeta llave, videovigilancia, guardias, verjas, etc.

Manejo de riesgos. ¿Cuánta seguridad es “suficiente seguridad”? Esta es una pregunta que atormenta a los responsables del departamento de TI porque no hay respuestas fáciles. La mayoría de las organizaciones responden a esta pregunta implantando un programa de gestión de riesgos. No obstante, cada programa es único porque no existe un sólo enfoque para proteger los activos y datos corporativos.

Para realizar un buen manejo de riesgos es necesario tener en cuenta la evaluación de riesgos, la mitigación de los riesgos y los riesgos en el tiempo.

El tiempo es importante en seguridad porque permite medir la eficacia de las contramedidas en función del tiempo que están expuestas a un suceso concreto. Muchas personas han contribuido a este concepto, pero Winn Schwartau fue el primero en escribir un libro (Time Based Security) aplicando estas técnicas a la seguridad de la información, reiterándolas el

2021 en un artículo de la Cyber Defense Magazine. Él detalla cómo utilizar el tiempo como mecanismo para determinar si las contramedidas son suficientes o no. Esta metodología nos proporciona otra herramienta que pone la estrategia de gestión de riesgos en términos bastante sencillos que pueden ayudar a identificar las áreas que necesitan más atención, la siguiente fórmula puede utilizarse para determinar el tiempo de exposición: Exposición = Detección + Reacción, y la única forma de hacerlo es mediante la evaluación del riesgo.

Tipo de auditorías. Las auditorías pueden dividirse en varios tipos, como una revisión completa de cumplimiento bajo ciertos estándares, un análisis de vulnerabilidades en un sistema específico o una revisión de la política de contraseñas de una organización. En general, la diferencia entre los distintos tipos de auditorías radica en qué basa el auditor sus conclusiones y en lo detallado que es el alcance de la auditoría.

Tabla 5

Tipos de auditoría de redes

Tipo de auditoría	Descripción
Revisión de seguridad	Es la forma más básica de análisis de seguridad y consiste en la emisión de la opinión de un profesional respecto a la seguridad de una organización, es decir, el resultado principal es un informe detallado que incluye recomendaciones para mejorar la seguridad de la organización. Durante este examen se buscan problemas destacados que ayuden a definir el punto de partida para actividades posteriores. Pueden incluirse escáneres de vulnerabilidades, como Nessus, que generan una lista de posibles problemas de seguridad. Sin embargo, estos datos deben analizarse a fondo para determinar en qué se debe actuar. Algunos ejemplos de revisiones de seguridad son: - Prueba de penetración - Exploración de vulnerabilidades - Revisión de la arquitectura - Revisión de políticas - Revisión de la conformidad - Análisis de riesgos

Evaluación de la seguridad	Implica la utilización del resultado de la revisión de seguridad pero también su análisis para determinar la relevancia y criticidad para la organización. En este proceso, se intenta cuantificar el riesgo asociado a los elementos descubiertos para determinar el alcance del problema. La mayor diferencia entre una evaluación y una revisión es la profundidad con la que se examina el sistema y se analizan los resultados. Los ejemplos incluyen: - Evaluación de la vulnerabilidad - Evaluación de riesgos - Evaluación de la arquitectura - Evaluación de políticas
Auditoría de seguridad	La auditoría de seguridad examina la postura de seguridad de una organización en relación con una norma de la industria, como ISO27001 o COBIT, y/o el cumplimiento de normativas como HIPAA o PCI. Este proceso incluye los dos tipos de auditorías anteriores, así como un análisis de las deficiencias encontradas en relación con las normas para medir el grado de cumplimiento de la organización. La auditoría de seguridad considera a las personas, los procesos y/o las tecnologías y los compara con un punto de referencia de forma estandarizada y repetible. Como ejemplos tenemos: - Auditoría de cumplimiento - Auditoría de políticas - Auditoría de procedimientos - Auditoría de riesgos

2.2.2.4. Normas, procedimientos y directrices

La mayoría de los auditores se centran en probar y validar los controles para garantizar su funcionalidad y confiabilidad. Para orientarse en esta tarea, es importante que conozcan fuentes de orientación, plantillas o diseños de muestra que hayan sido validados mediante consenso y pruebas exhaustivas, como señala Jackson (2010). Por lo que, a continuación, se presentan de manera sucinta algunas normas y mejores prácticas que pueden ayudar a los auditores a distinguir entre buenos y malos diseños de seguridad, así como proporcionar arquitecturas de referencia para su comparación.

- ***Serie de normas ISO 27000.*** La serie ISO 27000 son normas de control de seguridad reconocidas internacionalmente para la creación y las operaciones de un Sistema de Gestión de Seguridad de la Información (SGSI). Es un gran recurso para abordar una amplia gama de necesidades de seguridad, desde las normas de tratamiento de datos a la seguridad física, pasando por la política.

- ***Centro para la Seguridad en Internet (CIS).*** **E**s una organización sin fines de lucro dedicada a desarrollar mejores prácticas de seguridad y guías de configuración para empresas. Su objetivo es reducir el riesgo de una protección inadecuada de los sistemas corporativos. El CIS ofrece guías y plantillas de configuración revisadas por expertos, que tanto administradores como auditores pueden utilizar para asegurar y evaluar la seguridad de un sistema específico. Estas guías están redactadas de manera clara y detallada, proporcionando una lista de verificación e incluyen explicaciones sobre la relevancia de cada opción.
- ***Instituto SANS (SysAdmin, Audit, Network, Security):*** Es una valiosa fuente de información gratuita sobre seguridad disponible en Internet. Aunque el enfoque principal de SANS es la formación, también proporciona abundante contenido gratuito relacionado con la seguridad como parte de su misión de compartir conocimientos y experiencia con la comunidad en línea. SANS ofrece una serie de servicios y recursos gratuitos, especialmente útiles para auditores y profesionales de la seguridad. Algunos de ellos incluyen el FAQ de Detección de Intrusiones, SCORE y muestras de políticas de seguridad de SANS, entre otros.
- ***ISACA.*** Es la principal asociación de auditores informáticos, y ha sido fundamental en la recopilación y estandarización de técnicas de auditoría y procesos de gobernanza de seguridad utilizados en la auditoría de TI en la actualidad. ISACA, además de establecer el Instituto de Gobierno de TI y desarrollar COBIT (marco de referencia que ayuda a las organizaciones a establecer prácticas efectivas de gobierno y gestión de TI), ha creado la guía de estándares de facto para evaluar y auditar los controles de TI. Las normas, directrices y procedimientos relacionados con la seguridad de la información para profesionales de auditoría y control se actualizan y revisan periódicamente, brindando a la comunidad de auditores un marco sólido para llevar a cabo sus auditorías.

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN

Según la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2018), la investigación aplicada es una investigación original orientada hacia un objetivo práctico y específico, con el propósito de adquirir nuevos conocimientos. Marotti de Mello & Wood Jr (2019), por su parte, mencionan que implica utilizar los conocimientos existentes con la metodología adecuada para abordar un problema práctico. En este sentido, el tipo de investigación de este proyecto se considera aplicada, ya que se justifica por su propósito práctico y su dependencia de los aportes teóricos de la investigación científica previa.

3.2. NIVEL DE INVESTIGACIÓN

Manjunatha (2019) señala que la investigación descriptiva tiene como objetivo describir las características de una población o fenómeno en estudio, enfocándose más en el "qué" que en el "por qué" del mismo. Para lograrlo, se apoya en técnicas como encuestas, entrevistas, observación y revisión documental, con el fin de estudiar, analizar, describir y especificar situaciones y propiedades del objeto de estudio. Es común que los trabajos de pregrado y maestría se centren en la investigación descriptiva, presentando hechos, situaciones y rasgos característicos del objeto de estudio, o bien, diseñando productos, modelos, prototipos, guías, entre otros, como lo menciona Carrasco (2015). Considerando lo anterior, se puede afirmar que el nivel de este trabajo de investigación es descriptivo.

3.3. DISEÑO DE LA INVESTIGACIÓN

Según Hernández et al. (2014), la investigación experimental es aquella en la que no se manipulan deliberadamente las variables para ver su efecto sobre otras, es decir, se caracteriza por la observación de los fenómenos en su contexto natural.
Por otro lado, Maier et al. (2023) indican que el diseño de una investigación transversal utiliza una instantánea de los comportamientos o variables de interés en un punto específico en el tiempo.

Por lo anterior mencionado, esta investigación tiene un diseño de investigación no experimental de tipo transversal descriptivo.

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

La población está conformada por las herramientas de Auditoría de redes del mundo.

3.4.2. Muestra

La muestra la integra Security Onion como herramienta de Auditoría de redes para la UNSCH, 2023.

3.5. VARIABLES Y DIMENSIONES

3.5.1. Definición conceptual de las variables

3.5.1.1. Security Onion

Es una plataforma de seguridad de red, basada en una distribución de Linux, utilizada para monitorear y analizar la actividad en una red informática con el objetivo de detectar y responder a posibles amenazas de seguridad. Proporciona una suite de herramientas de código abierto diseñadas para la monitorización de seguridad y el análisis de registros.

Monitorización de seguridad.

Consiste en la recopilación y el análisis de información para detectar comportamientos sospechosos o cambios no autorizados en la red, y en definir qué tipos de comportamiento deben activar alertas para tomar medidas al respecto.

Gestión de logs.

Es el proceso sistemático de manejar y analizar los registros que provienen de distintos sistemas o dispositivos dentro de una red.

Sistema de detección de intrusos.

Es un sistema que detecta actividades sospechosas en la red y genera alertas para que la persona responsable tome medidas al respecto.

3.5.1.2. Auditoría de redes

Es un proceso de evaluación y análisis de la infraestructura de red de una organización con el fin de identificar vulnerabilidades, debilidades y riesgos de seguridad.

Análisis de datos.

Es la revisión de los datos generados por una red para identificar patrones, anomalías y posibles problemas de seguridad o rendimiento.

Recopilación de datos.

Es el proceso de reunir información relevante sobre la infraestructura de red de una organización

3.5.2. Definición operacional de las variables

3.5.2.1. Primera variable

Security Onion.

Dimensiones.

- Monitorización de seguridad.
- Gestión de logs.
- Sistema de detección de intrusos.

3.5.2.2. Segunda variable

Auditoría de redes.

Dimensiones.

- Análisis de datos.
- Recopilación de datos.

3.6. TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS

Las técnicas e instrumentos utilizadas en el trabajo de investigación son:

3.6.1. Técnicas

- Análisis de red.

3.6.2. Instrumentos

- Registros de la análisis.

3.7. TÉCNICAS PARA APLICAR LA AUDITORÍA DE REDES

La auditoría de redes es un proceso crítico para garantizar la seguridad, integridad y disponibilidad de la infraestructura de red de la Universidad Nacional de San Cristóbal de Huamanga (UNSCH) y, si bien hay varios marcos de referencia o estàndares en lo que respecta a la seguridad de la informaciòn y que pueden servir como guìa para una auditorìa de este tipo, en el presente proyecto de investigaciòn se ha optado por alinearla con los Controles CIS versión 8 debido a las siguientes razones:

- Enfoque práctico y accesible
    - Los Controles CIS están diseñados para ser prácticos y aplicables. Proporcionan una guía concreta para mejorar la seguridad sin requerir una gran inversión de tiempo o recursos.
    - En contraste, la ISO 27001 y COBIT pueden ser más extensos y complejos. Requieren un enfoque más estructurado y a menudo implican auditorías formales.
- Enfoque basado en amenazas reales
    - Los Controles CIS se basan en amenazas reales y en el análisis de incidentes de seguridad. Esto los hace relevantes para las organizaciones que buscan protegerse contra riesgos específicos.
    - La ISO 27001 y COBIT son más genéricas y no siempre se centran en amenazas específicas.
- Contexto y objetivos de la organización:
    - Si la organización busca una certificación formal, la ISO 27001 podría ser más apropiada.
    - Si busca una mejora gradual y práctica, los Controles CIS pueden ser una excelente opción.

En resumen, los Controles CIS son una opción sólida para organizaciones, como la Universidad Nacional de San Cristòbal de Huamanga que no ha tenido una auditorìa de redes formal y que buscan mejorar su seguridad de manera práctica y basada en amenazas reales como punto inicial.

3.7.1. Controles CIS

De acuerdo al Center for Internet Security, Inc. (2021), los Controles Críticos de Seguridad CIS (CIS Controls®) son un conjunto de buenas prácticas diseñadas para proteger a las organizaciones de los ciberataques más comunes, identificando,

como su nombre lo indica, los puntos críticos para detener los ataques más importantes.

Actualmente estos controles se encuentran en la versión 8, la misma que incluye 18 controles y 153 salvaguardas distribuidos en 3 grupos de implementación (IG) o perfiles, tal como se muestra en la Figura 16 y la Tabla 6.

Figura 16

Controles CIS versiòn 8

Tabla 6

Perfiles de los controles CIS

Denominaciòn del perfil	Caracterìsticas
IG1	➔ Pequeña a mediana organización con experiencia limitada en TI y ciberseguridad para dedicarse a proteger los activos y personal de TI. ➔ La principal preocupación de estas organizaciones es mantener el negocio operativo, ya que tienen una tolerancia limitada de inactividad. ➔ La sensibilidad de la información que ellas tratan de proteger es baja y principalmente incluye información de empleados e información financiera.

 IG2 (incluye IG1)	➔ Emplea a individuos responsables de administrar y proteger la infraestructura de TI. ➔ Se apoyan de múltiples departamentos con distintos perfiles de riesgo en base a la función del puesto y misión. ➔ Almacenan procesos e información sensible sobre el cliente o información empresarial y pueden soportar breves interrupciones de servicios. ➔ La mayor preocupación es la pérdida de la confianza del público si se produce una brecha.
 IG3 (incluye IG2 e IG1)	➔ Una organización IG3 emplea expertos en seguridad los cuales se especializan en diferentes facetas de la ciberseguridad (por ejemplo, gestión de riesgo, pruebas de penetración, seguridad en las aplicaciones). ➔ Los activos e información IG3 contienen información sensible o funciones que están sujetas a supervisión regulatoria y de cumplimiento. ➔ Debe abordar la disponibilidad y la confidencialidad e integridad de los datos sensibles. ➔ La materialización de los ataques puede causar un daño significativo al bienestar público.

A continuación se mencionará cada control con una pequeña descripción de su importancia.

CIS Control 01: Inventario y control de los activos empresariales

Gestionar activamente todos los activos de la organización, especialmente los dispositivos informáticos y de red, conectados a la infraestructura física y aquellos del ambiente de la nube, permite conocer con precisión aquellos que necesitan ser monitoreados y protegidos. Lo que también apoya a la identificación de activos no autorizados y no administrados para los fines correspondientes

CIS Control 02: Inventario y control de activos de software

Los atacantes buscan software vulnerable para explotarlo y obtener acceso no autorizado. Mantener el software actualizado y llevar un inventario del software son medidas de defensa fundamentales para protegerse contra vulnerabilidades conocidas y desconocidas. Identificar el software innecesario reduce los riesgos de seguridad.

CIS Control 03: Protección de los datos

El uso y la gestión adecuados de los datos a lo largo de su ciclo de vida son cruciales. A menudo, las empresas no son conscientes de que los datos

confidenciales están saliendo de su entorno debido a la falta de supervisión. Aunque se producen robos y espionaje, la mayoría de los casos de datos comprometidos son el resultado de un mal entendimiento de las normas de gestión de datos y de errores de los usuarios.

CIS Control 04: Configuración segura de activos y software empresarial

Las configuraciones por defecto suelen centrarse en la facilidad de uso más que en la seguridad. Sin embargo, estas configuraciones por defecto pueden ser explotadas si no se modifican. Es importante gestionar y actualizar continuamente las configuraciones para evitar vulnerabilidades de seguridad y respaldar las necesidades operativas.

CIS Control 05: Administración de cuentas

El acceso no autorizado a los activos o datos de la empresa suele ser más fácil a través de credenciales de usuario válidas que mediante el pirateo informático. Contraseñas débiles, cuentas inactivas y contraseñas compartidas o comprometidas son vulnerabilidades comunes. Las cuentas administrativas y de servicio son siempre el objetivo, y el registro y la supervisión de las cuentas son cruciales para la seguridad.

CIS Control 06: Gestión de control de accesos

Se centra en la gestión del acceso que tienen las cuentas de usuario, garantizando que sólo tengan acceso a los datos y activos empresariales adecuados para su función. Enfatiza la necesidad de una autenticación fuerte para los datos críticos o sensibles del negocio.

CIS Control 07: Gestión continua de vulnerabilidades

Los defensores cibernéticos de las organizaciones necesitan información oportuna sobre las amenazas y deben revisar periódicamente su entorno para identificar las vulnerabilidades antes que los atacantes. Es crucial priorizar las vulnerabilidades en función de su impacto y facilidad de explotación. Si no se evalúa la infraestructura y se corrigen los fallos, aumenta la probabilidad de que los activos se vean comprometidos.

CIS Control 08: Gestión de registros de auditoría

Los registros son esenciales para detectar y comprender la actividad maliciosa. Los atacantes se aprovechan de la falta de análisis de registros por parte de las empresas para ocultar sus acciones, pudiendo controlar las máquinas víctimas durante largos periodos sin ser detectados. Tanto los registros del sistema como los de auditoría son importantes y deben configurarse adecuadamente. El análisis de registros es crucial para responder a incidentes y evaluar el alcance de un ataque.

CIS Control 09: Protección del correo electrónico y navegador web

Los navegadores web y los clientes de correo electrónico son vulnerables a los ataques, ya que interactúan directamente con los usuarios, lo que aumenta el riesgo de revelar credenciales o proporcionar un punto de entrada a los atacantes.

CIS Control 10: Defensas contra malware

El software malintencionado es una peligrosa amenaza en Internet, que evoluciona y se adapta para aprovechar las vulnerabilidades de los dispositivos de los usuarios finales, los archivos adjuntos al correo electrónico, los sitios web y otros. Para combatirlo, las defensas contra el malware deben funcionar en un entorno dinámico e incluir automatización, actualizaciones puntuales e integración con otros procesos, como la gestión de vulnerabilidades y la respuesta a incidentes. Estas defensas deben implementarse en todos los posibles puntos de entrada y activos empresariales para detectar, prevenir o controlar la ejecución de software malicioso.

CIS Control 11: Recuperación de datos

La disponibilidad de los datos es a veces más importante que la confidencialidad, ya que las empresas dependen de datos fiables y accesibles para tomar decisiones empresariales. Los atacantes pueden realizar cambios difíciles de detectar para poner en peligro los activos, lo que acentúa la necesidad de realizar copias de seguridad para recuperar los activos y datos de la empresa.

CIS Control 12: Gestión de la infraestructura de red

Una infraestructura de red segura es crucial para defenderse de los ataques. Esto implica abordar las vulnerabilidades de las configuraciones por defecto, supervisar los cambios y reevaluar las configuraciones actuales. Los atacantes aprovechan los fallos de los dispositivos para acceder a las redes, redirigir el tráfico e interceptar datos. Es necesario reevaluar periódicamente la arquitectura, las configuraciones, los controles de acceso y los flujos de tráfico, ya que las configuraciones de los dispositivos de red se vuelven menos seguras con el tiempo. Las excepciones a las medidas de seguridad deben analizarse y compararse con las necesidades de la empresa.

CIS Control 13: Monitoreo y defensa de la red

Los ciberdelincuentes continúan evolucionando y madurando a medida que comparten o venden información sobre exploits y omisiones de los controles de seguridad.

Las herramientas de seguridad sólo pueden ser efectivas si respaldan un proceso de monitorización continuo que permita al personal recibir alertas y responder rápidamente a los incidentes de seguridad.

Es fundamental que las organizaciones tengan una capacidad de operaciones de seguridad para prevenir, detectar y responder rápidamente a las amenazas cibernéticas antes de que puedan afectarlas.

CIS Control 14: Concientización en seguridad y formación de habilidades

Las acciones individuales influyen significativamente en el éxito del programa de seguridad de una empresa. El comportamiento de los usuarios, como hacer clic en enlaces maliciosos o manejar mal los datos, supone un riesgo mayor que los exploits de la red. Una formación actualizada periódicamente puede mejorar la concienciación sobre la seguridad y desalentar las prácticas inseguras.

CIS Control 15: Gestión de proveedores de servicios

En el mundo interconectado de hoy en día, las empresas dependen a menudo de proveedores y socios para la gestión de datos o de infraestructuras de terceros para ciertas funciones. Sin embargo, evaluar la

seguridad de estos proveedores externos es un reto debido a la falta de una norma universal. Mientras que las grandes empresas pueden examinar de cerca a los proveedores de aplicaciones o de alojamiento en la nube, las más pequeñas suelen correr mayores riesgos. Esto se debe a que las empresas más pequeñas pueden contratar con terceros servicios adicionales o utilizar plataformas de terceros para apoyar sus operaciones principales.

CIS Control 16: Seguridad en el software de aplicación

Las aplicaciones con interfaces fáciles de usar que permitan acceder y gestionar los datos de acuerdo con las funciones organizativas permiten minimizar la interacción del usuario con funciones complejas del sistema, reduciendo así la posibilidad de errores. Estas aplicaciones suelen crearse utilizando una combinación de marcos de desarrollo, bibliotecas y código, en lugar de crearse desde cero. Además, con la prevalencia de las plataformas de software como servicio (SaaS), las organizaciones se enfrentan al desafío de comprender los riesgos asociados, a menudo sin visibilidad del desarrollo y las prácticas de seguridad de estas aplicaciones.

CIS Control 17: Gestión de respuesta a incidentes

La gestión de incidentes cibernéticos implica identificar y responder a amenazas para mitigar daños. Un plan documentado es crucial para la investigación, comunicación y recuperación efectiva tras un incidente. La comunicación es vital para la toma de decisiones empresariales informadas y la reducción del impacto de eventos cibernéticos. El tiempo que tarda en detectarse un ataque es fundamental, ya que los atacantes se integran más en la infraestructura y buscan mantener el acceso.

CIS Control 18: Pruebas de penetración

En el dinámico mundo de la tecnología, las empresas enfrentan constantemente nuevos tipos de ataques cibernéticos. Para mantenerse seguras, deben realizar pruebas periódicas de sus controles, que pueden incluir desde análisis de redes hasta ingeniería social. Las pruebas de penetración son esenciales para descubrir vulnerabilidades y evaluar la efectividad de las medidas de seguridad, diferenciándose de las pruebas de

vulnerabilidad en que estas últimas sólo identifican fallos conocidos sin intentar explotarlos. Los ejercicios de Equipo Rojo complementan estas pruebas simulando ataques reales para probar la resistencia de la empresa ante amenazas específicas.

3.7.1.1. Controles CIS seleccionados

La selección de los controles CIS para este trabajo de investigación se realiza en función de los datos obtenidos mediante el despliegue de tipo EVAL de Security Onion, los cuales se detallarán en la sección *4.3.2. Relación de hallazgos con los Controles CIS.*

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. DESCRIPCIÓN DE LA RED EXISTENTE EN EL CAMPUS UNIVERSITARIO

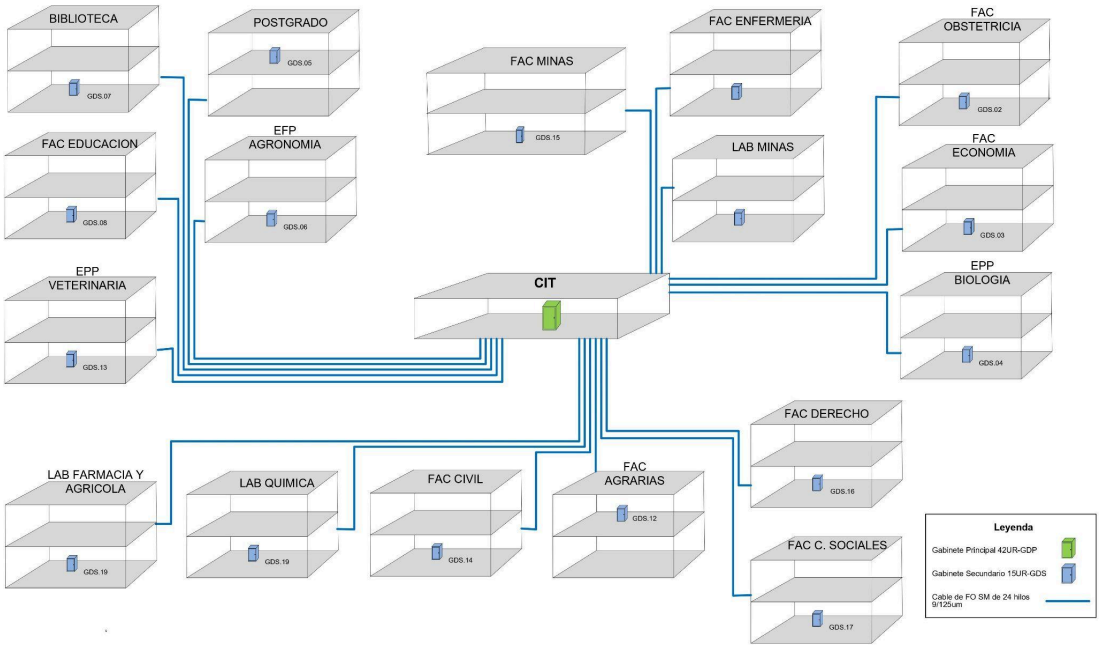
Toda la información mostrada en esta sección está respaldada por documentos o reportes de la Oficina De Tecnologías de Información.

4.1.1. Topología de red

En el Informe técnico final presentado por Cloud IT (2022) se menciona que la topología de la red LAN de la Universidad Nacional de San Cristóbal de Huamanga es de tipo estrella, la misma que tiene como centro al switch core instalado en el data center de la Oficina de Tecnologías de Información (OTI, ex CTI), tal como se puede observar en la Figura 17.

Figura 17

Topología de la red LAN del campus universitario - UNSCH



Nota. Adaptado de *Topología de la red LAN* (p.301), por Cloud IT, 2022.

4.1.2. Sistema de seguridad perimetral

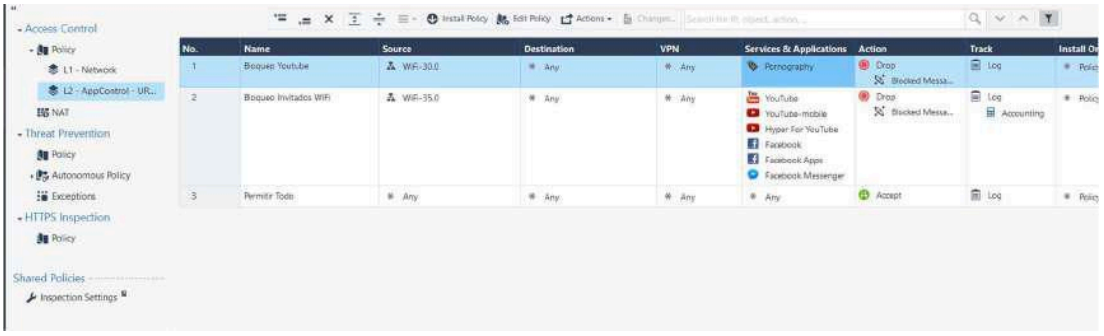
El sistema de seguridad perimetral está compuesto por un firewall Checkpoint, integrado a la red de datos a través de enlace al switch core y al equipo del proveedor de internet, que realiza las siguientes funciones:

- Protege el acceso externo a la red de la UNSCH.
- Controla el tráfico mediante el bloqueo de puertos UDP/TCP.
- Controla las aplicaciones de descarga masiva P2P.

A continuación se muestran algunas configuraciones realizadas en el firewall.

Figura 18

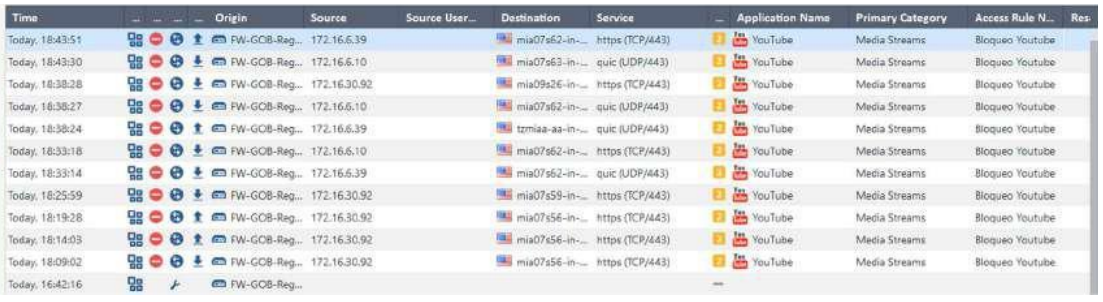
Configuración relacionada a algunas políticas de control de aplicaciones



Nota. Adaptado de *Políticas de Control de Aplicaciones* (p.17), por Cloud IT, 2022.

Figura 19:

Log de bloqueo del firewall



Nota. Adaptado de *Log de bloqueo del firewall* (p.17), por Cloud IT, 2022.

4.1.3. Dispositivos de la red

Los dispositivos que componen la red de la ciudad universitaria son los que se detallan en la Tabla 7.

Tabla 7

Dispositivos de la red del campus universitario de la UNSCH

Tipo de dispositivo	Nombre del dispositivo	Cantidad	Marca	Modelo
Conectividad	Switch core de 48 puertos	1	CISCO	N9K-C93180YC-EX
	Switch de borde de 48 puertos	18	ARUBA	3810M
Acceso inalámbrico	Controlador inalámbrico	1	ARUBA	JW783A
	Access point para exteriores	34	ARUBA	JZ172A
	Access point para interiores	2	ARUBA	JZ356A
Seguridad perimetral	Firewall de nueva generación	1	CHECK POINT	CPAP-6600
Procesamiento y almacenamiento	Servidor HPE ProLiant DL180 Gen10	1	HPE	879515-B21
Dispositivos de protección eléctrica y otros	UPS de 3KVA	1	SALICRU	SLC-3000-TWIN RT2
	Transformador de Aislamiento de 15KVA.	1	A&A	MO-15K-A&A
	Tablero eléctrico, para data Center	1	-	-
	Gabinete de 42 RU, para el Data Center	1	RITTAL	5311126
	Sistema de aire acondicionado autocontenido	1	RITTAL	3313420
	Gabinete de 15 RU	17	DIXON	DXY.6415.BXA

Nota. Adaptado de *Detalle de equipamiento suministrado para la UNSCH* (p.9), por Cloud IT, 2022.

4.2. METODOLOGÌA DE AUDITORÌA CON SECURITY ONION

4.2.1. Especificaciones técnicas para la instalación de Security Onion

De acuerdo a la documentación oficial realizada por Security Onion Solutions, se mencionan que las características de hardware para el despliegue de esta plataforma son las presentadas en la Tabla 8.

Tabla 8

Requisitos mínimos de hardware para el despliegue de Security Onion

Tipo de nodo/despliegue	N° de núcleos	RAM	Almacenamiento	N° de interfaces de red
Import	2	4GB	50GB	1
Eval	4	8GB	200GB	2
Standalone	4	16GB	200GB	2
Manager	4	16GB	200GB	1
Manager Search	8	16GB	200GB	1
Search node	4	16GB	200GB	1
Sensor	4	12GB	200GB	2
Heavy node	4	16GB	200GB	2
IDH node	2	1GB	12GB	1
Fleet node	4	4GB	200GB	1
Receiver node	2	8GB	200GB	1

En el presente trabajo de investigación se hace una instalación de tipo EVAL debido a que está diseñada para instalaciones de laboratorio con un presupuesto limitado. Este tipo de instalación ejecuta los procesos mínimos necesarios para que una sola máquina husmee el tráfico de red en directo desde un puerto TAP o SPAN (puerto que se configura en el switch al que la máquina que ejecuta Security Onion se encuentra conectada) y visualice los resultados.

Para minimizar el uso de RAM, Eval no ejecuta Logstash o Redis en absoluto. Además, Eval utiliza por defecto Suricata para escribir la captura completa de paquetes en el disco (en lugar de Stenographer).

4.2.2. Instalación y configuración de Security Onion

La instalación de Security Onion se divide en dos etapas principales. La primera etapa, que abarca los pasos iniciales de la instalación desde un USB booteable, se describe en el Anexo B. Estos pasos son estándar y no presentan variaciones respecto a la documentación oficial de Security Onion. Una vez completada la primera etapa de la instalación, el sistema solicitará un reinicio. Se procede a retirar el USB booteable antes de realizar el reinicio del equipo para evitar reiniciar el proceso de instalación desde el medio extraíble.

La segunda parte, que también incluye la configuración y se lleva a cabo después del reinicio requerido tras la primera etapa, es abordada en el Anexo C.

4.2.3. Captura de datos de la red

4.2.3.1. Verificación del estado del nodo

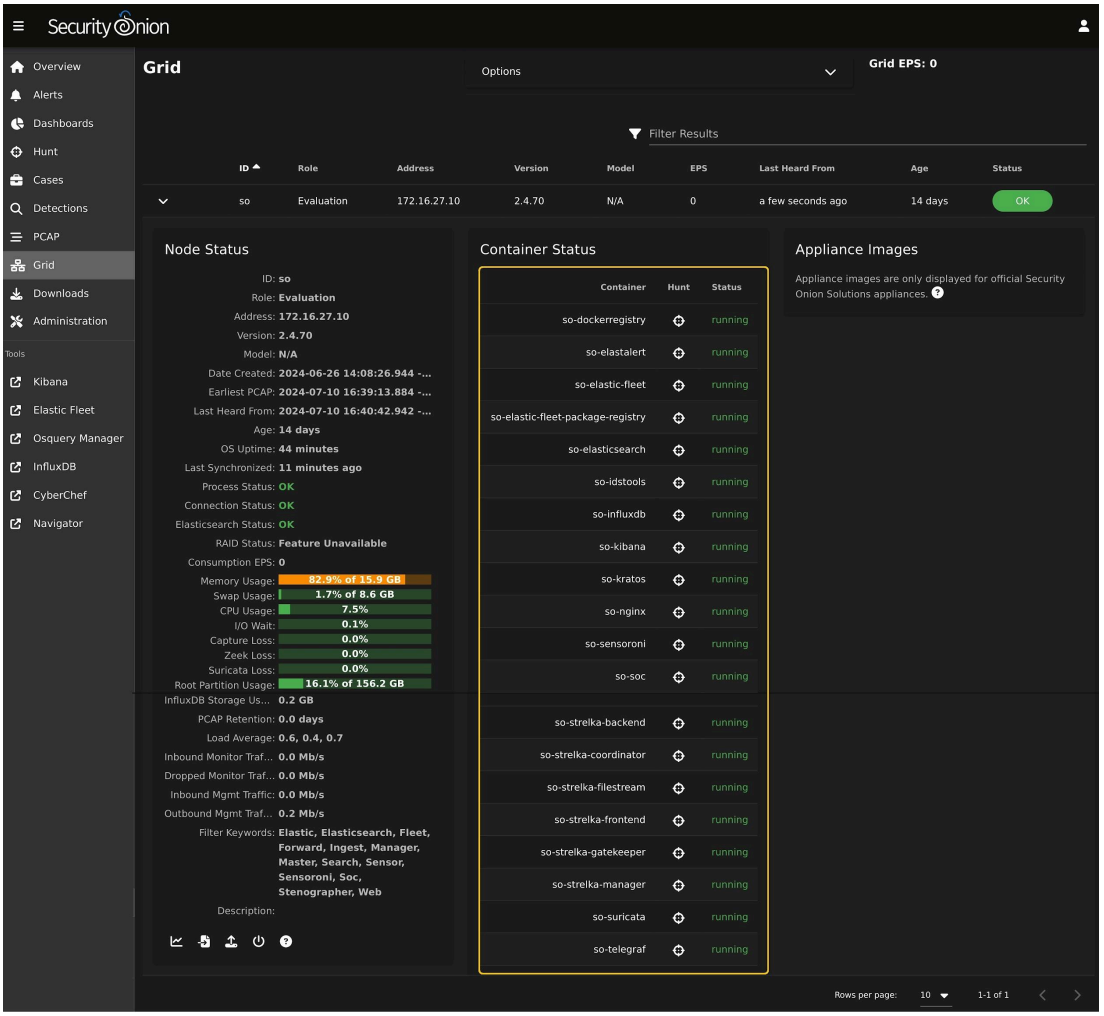
Para verificar el estado del nodo, es necesario acceder a la IP asignada a la máquina que ejecuta Security Onion desde el navegador web de otro dispositivo autorizado en la red, como se muestra en el Anexo D.

Una vez iniciada la sesión, se selecciona la opción "Grid" del menú lateral. En esta sección se muestran los servicios que están ejecutándose en Security Onion y el estado del nodo, permitiendo así comprobar que el despliegue se ha realizado correctamente, como se ilustra en la Figura 20.

En caso se desee ver el rendimiento de todo el nodo se puede ingresar a InfluxDB, herramienta que está incluida en el despliegue de Security Onion, los pasos a seguir se encuentran en el Anexo E.

Figura 20

Estado y servicios que se están ejecutando en Security Onion



4.2.3.2. Detecciones en la red utilizando Security Onion

Para ver las detecciones de Security Onion, se hace clic en la opción “Detections” del menú lateral izquierdo de la consola web. Esto mostrará datos como el nombre, severidad, fecha, tipo, entre otros, de las detecciones realizadas en un cierto periodo de tiempo, como se puede observar en la Figura 21.

Al investigar más a fondo, se observa que Security Onion solo tiene activados algunos tipos de detección. Por lo tanto, es necesario activar los demás tipos o, al menos, aquellos que se consideran relevantes para la red de la ciudad universitaria, para obtener un panorama más completo. Para ello, se deben filtrar todas las detecciones cuyo estado o atributo “Enabled” sea “false” (ver Figura 22). Luego, se busca por palabra clave aquellas que se desean activar y se hace clic en el botón “Go” (ver Figura 23, tomando como ejemplo detecciones SQL).

Después de habilitar las detecciones adicionales, se procede a revisar nuevamente las detecciones realizadas por Security Onion, en las que ahora figuran nuevos registros, tal como se muestra en la Figura 24.

La lista completa de detecciones se encuentra en el Anexo F.

Figura 21

Detecciones realizadas por Security Onion

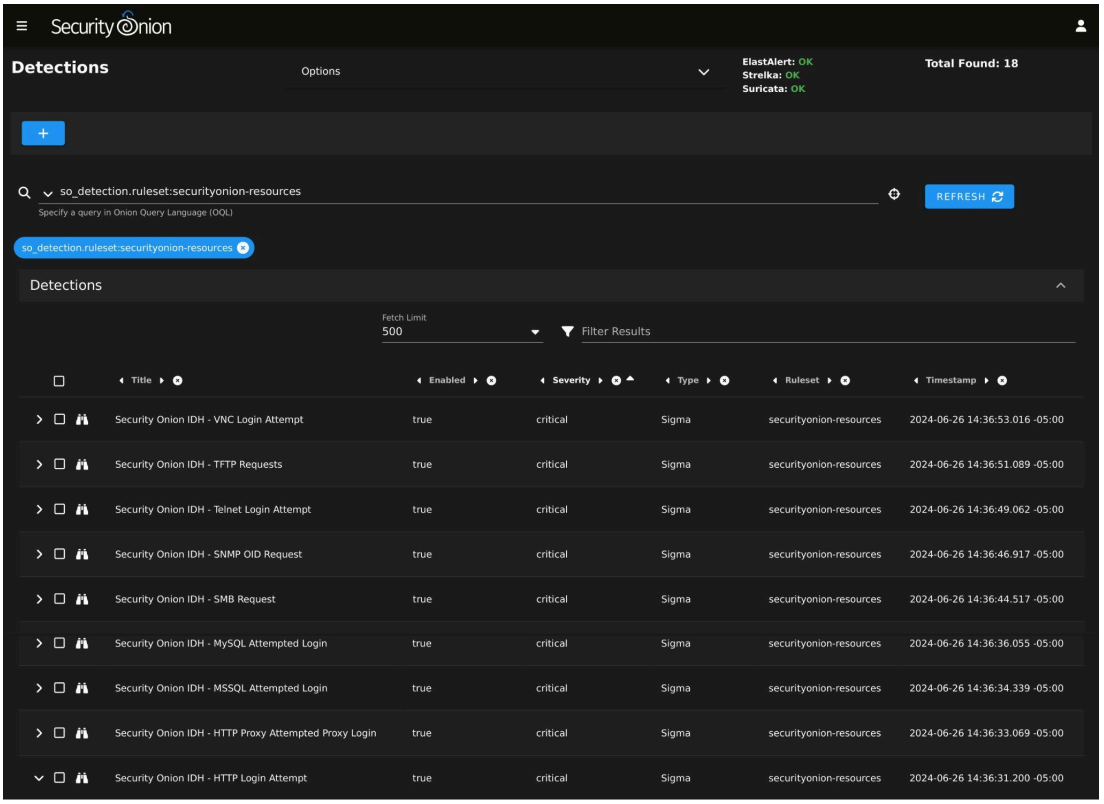


Figura 22

Algunas detecciones deshabilitadas

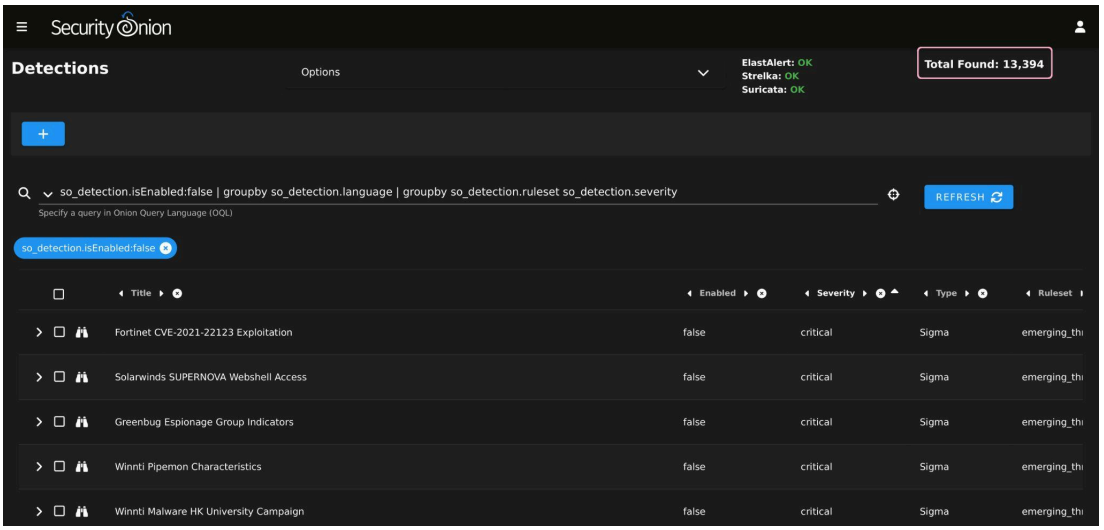


Figura 23

Habilitación de detecciones SQL

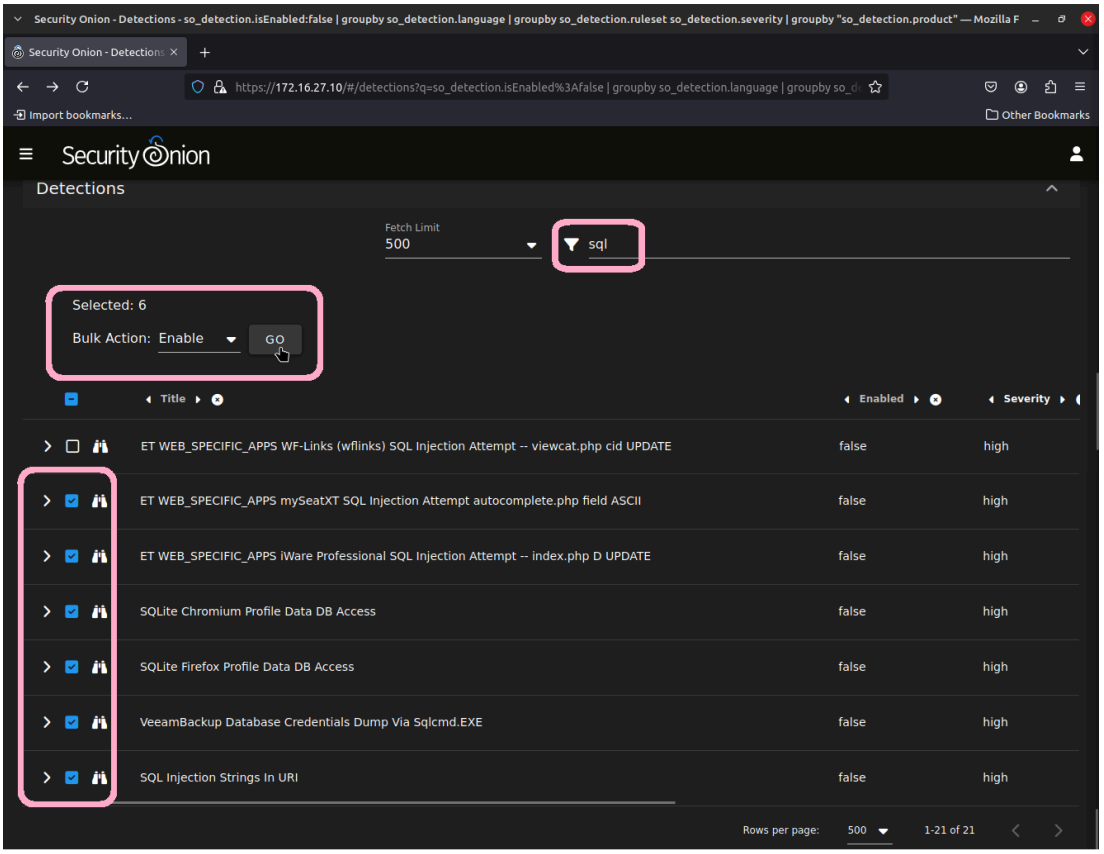
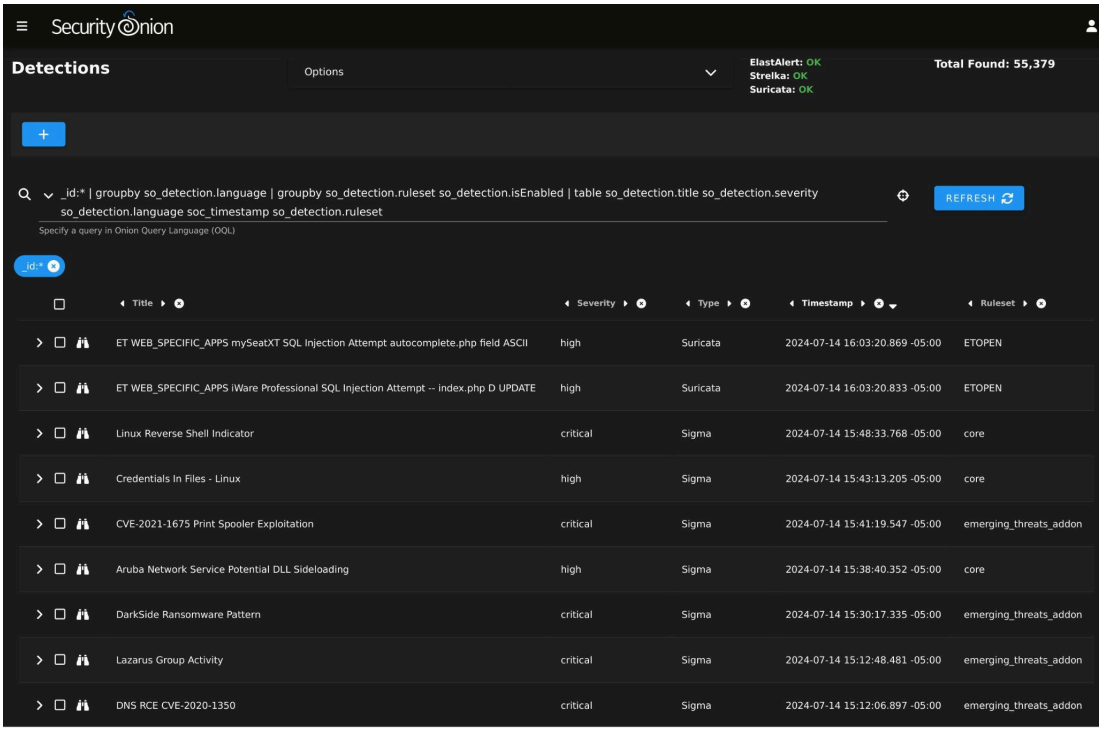


Figura 24

Actualización de detecciones registradas por Security Onion



4.3. INTEGRACIÓN Y DOCUMENTACIÓN DE LOS RESULTADOS

4.3.1. Documentación de hallazgos

Las detecciones realizadas por Security Onion en parte de la red del campus universitario, específicamente en el segmento 172.16.27.x, durante un periodo aproximado de tres semanas, revelan un total de 500 registros. De estos, 485 fueron clasificados como informativos, mientras que los 15 restantes se categorizaron como de severidad crítica y alta. Estas detecciones críticas y de alta severidad abarcaron diversos tipos de amenazas, desde intentos de inyección SQL hasta la detección de ransomware. A continuación, se presenta una tabla con los hallazgos más significativos.

Tabla 9

Reglas que se activaron durante el monitoreo de red

Nombre	Severidad	Regla	Descripción
ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt	Alta	Suricata	Vulnerabilidad web basada en PHP mySeatXT. La vulnerabilidad puede ser explotada mediante la inyección de código SQL codificado en ASCII, que luego es

autocomplete.php field ASCII			ejecutado por la base de datos.
ET WEB_SPECIFIC_APPS iWare Professional SQL Injection Attempt -- index.php D UPDATE	Alta	Suricata	Detecta un posible ataque web de inyección SQL dirigido al archivo index.php de una aplicación iWare Professional. La regla se activa cuando se envía una consulta D UPDATE al servidor, que es un patrón común utilizado en los ataques de inyección SQL.
Linux Reverse Shell Indicator	Crítica	Sigma	Detecta un bash que se conecta a una dirección IP remota (a menudo se encuentra cuando los actores hacen algo como 'bash -i >& /dev/tcp/10.0.0.1/4242 0>&1')
Credentials In Files - Linux	Alta	Sigma	Detección de intentos de extracción de contraseñas con grep.
CVE-2021-1675 Print Spooler Exploitation	Crítica	Sigma	Detecta eventos de carga de controladores del registro operativo del servicio de impresión que son una señal de intentos de explotación con éxito contra la vulnerabilidad del spooler de impresión CVE-2021-1675.
Aruba Network Service Potential DLL Sideloading	Alta	Sigma	Detecta la posible actividad de carga lateral de DLL a través del proceso «arubanetsvc.exe» de Aruba Networks Virtual Intranet Access mediante DLL Search Order Hijacking.
DarkSide Ransomware Pattern	Crítica	Sigma	Detecta el ransomware DarkSide y sus ayudantes.
Lazarus Group Activity	Crítica	Sigma	Detecta diferentes comportamientos de ejecución de procesos descritos en varios informes de amenazas sobre la actividad del grupo Lazarus.
DNS RCE CVE-2020-1350	Crítica	Sigma	Detecta la explotación del fallo DNS RCE reportado en CVE-2020-1350 mediante la detección de subprocesos sospechosos.
HAFNIUM Exchange Exploitation Activity	Crítica	Sigma	Detecta actividad observada por diferentes investigadores como actividad del grupo HAFNIUM (o relacionada) en servidores Exchange.
Security Onion IDH - SSH Accessed	Alta	Sigma	Se activa cuando un nodo IDH (Intrusion Detection Honeypot) detecta un intento de conexión a su servicio SSH simulado. Esta regla forma parte de los registros del honeypot Open Canary, que son procesados por Security Onion para

			generar alertas.
Potential OWASSRF Exploitation Attempt - Proxy	Alta	Sigma	Detecta el intento de explotación de la variante OWASSRF dirigida a servidores Exchange. Utiliza el endpoint OWA (Outlook Web Access) para acceder al endpoint backend powershell.
SQLite Firefox Profile Data DB Access	Alta	Sigma	Detecta el uso del binario «sqlite» para consultar bases de datos en Firefox y otros navegadores basados en Gecko para un posible robo de datos.
VeeamBackup Database Credentials Dump Via Sqlcmd.EXE	Alta	Sigma	Detecta volcado de credenciales en VeeamBackup dbo.
SQL Injection Strings In URI	Alta	Sigma	Detecta posibles intentos de inyección SQL a través de peticiones GET en los registros de acceso.
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 668	Informativo	Suricata	Detecta tráfico de nodos de retransmisión Tor conocidos que no son nodos de salida. La clasificación para este tráfico es misc-attack. Esta clasificación indica que el tráfico no es un ataque tradicional, como un desbordamiento de búfer o una inyección SQL, sino más bien un tipo de actividad de red que no es maliciosa en el sentido clásico.Esta clasificación se debe, probablemente, al hecho de que los nodos de retransmisión Tor están configurados intencionadamente para redirigir el tráfico dentro de la red Tor, en lugar de intentar explotar o comprometer sistemas fuera de la red. La regla está alertando sobre este tráfico Tor legítimo para proporcionar visibilidad y capacidades de monitorización a los administradores de red.

4.3.1.1. Patrones observados e implicaciones de seguridad

Prevalencia de detecciones informativas. La mayoría de las detecciones, 485 de 500, es decir, el 97% son de severidad informacional, lo cual sugiere que Security Onion está configurado para captar una amplia gama de actividades benignas o de bajo riesgo en la red. Este tipo de alertas suele ser menos prioritario, pero es crucial para obtener una visión completa del tráfico de red y las posibles configuraciones indebidas o anomalías menores.

En este trabajo de investigación, la detección «ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184-668» indica tráfico procedente de nodos de retransmisión Tor conocidos, que no son necesariamente maliciosos, pero que pueden ser usados para ocultar otras actividades.

Detecciones críticas y de alta severidad. Aunque solo el 3 % de las detecciones tiene severidad crítica o alta, lo cual es una cantidad pequeña, no deja de ser alarmante debido al potencial daño que pueden causar.
Se ha encontrado que los tipos de amenazas comprendidos son:

- **Inyección SQL:** Varias detecciones (como "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt", “ET WEB_SPECIFIC_APPS iWare Professional SQL Injection Attempt” y "SQL Injection Strings In URI") sugieren intentos de inyección SQL, lo que puede comprometer la integridad de las bases de datos.
- **Ransomware:** La detección "DarkSide Ransomware Pattern" indica la presencia de ransomware conocido por su alta capacidad destructiva. DarkSide es un ransomware como servicio (RaaS), y sus actores han estado atacando a grandes organizaciones, resultando en el cifrado y robo de datos confidenciales. Los atacantes de DarkSide utilizan técnicas como phishing y explotación de servicios accesibles externamente para obtener acceso inicial y emplean TOR para ocultar sus operaciones y comunicaciones de mando y control, lo que en combinación con las numerosas detecciones "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184-668", sugiere un posible vínculo.
- **Ataques Dirigidos y Actividades de Grupos APT:** Detecciones como "Lazarus Group Activity" y "HAFNIUM Exchange Exploitation Activity" revelan posibles intentos de intrusión por parte de grupos avanzados de amenazas persistentes (APT), conocidos por sus sofisticadas tácticas y técnicas utilizadas para acceder y permanecer en una red o sistema informático durante un período prolongado, con el objetivo de obtener información valiosa y confidencial.
- **Actividades relacionadas con vulnerabilidades conocidas:**

    - **Vulnerabilidades específicas:** Varias detecciones están relacionadas con vulnerabilidades específicas, como "CVE-2021-1675 Print Spooler Exploitation" y "DNS RCE CVE-2020-1350". Estas detecciones indican intentos de explotación de vulnerabilidades conocidas que, si no se mitigan, pueden permitir a un atacante remoto ejecutar código arbitrario o comprometer sistemas críticos.
    - **Intentos de explotación:** Las detecciones como "Potential OWASSRF Exploitation Attempt - Proxy" reflejan intentos de explotar puntos débiles en servicios específicos, en este caso, los servidores Exchange. OWASSRF es una técnica que explota vulnerabilidades en los endpoints de Outlook Web Access (OWA) para acceder a servicios backend como PowerShell Remoting. Este ataque permite a los actores maliciosos ejecutar comandos arbitrarios y mantener la persistencia en los sistemas comprometidos.
- **Detecciones de herramientas y técnicas de post-explotación:**
    - **Movimiento lateral y persistencia:** La detección "Aruba Network Service Potential DLL Sideloading" y "Linux Reverse Shell Indicator" sugieren intentos de los atacantes para obtener persistencia (capacidad para mantener su acceso y presencia en la red objetivo durante un período prolongado, sin ser detectados ni eliminados por las defensas de la organización) y moverse lateralmente dentro de la red.
    - **Exfiltración de datos:** Las detección "Credentials In Files - Linux" indica intentos de extraer credenciales de archivos en sistemas Linux, lo cual es una etapa común en el proceso de exfiltración de datos, es decir, de transferencia intencionada, no autorizada y encubierta de datos desde un ordenador u otro dispositivo. En este apartado también se encuentran las detecciones “VeeamBackup Database Credentials Dump Via Sqlcmd.EXE" y "SQLite Firefox Profile Data DB Access".

4.3.2. Relación de hallazgos con los Controles CIS

En esta sección, se detalla cómo las detecciones realizadas por Security Onion se correlacionan con los controles de seguridad establecidos por el Center for Internet Security (CIS). Aunque algunos hallazgos pueden asociarse a múltiples controles, nos enfocaremos en aquellos más relevantes y representativos para cada caso, la Tabla 10 ilustra esta relación.

Además, se presenta una tabla de doble entrada (ver Tabla 11) que resume visualmente estas relaciones, marcando con una "X" la intersección entre cada detección y los controles CIS pertinentes. Esta representación gráfica facilita la identificación rápida de los puntos críticos de seguridad abordados por cada hallazgo.

Tabla 10

Relación entre detecciones y controles CIS

Detecciones	Controles CIS	Relación
➔ ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt ➔ ET WEB_SPECIFIC_APPS iWare Professional SQL Injection Attempt ➔ SQL Injection Strings In URI	Control CIS 02: Inventario y control de activos de software	Estas detecciones están directamente relacionadas con la necesidad de mantener actualizado el software para parchear vulnerabilidades en aplicaciones en las que se pueda realizar la inyección SQL.
	Control CIS 04: Configuración segura de activos y software empresarial	La implementación de configuraciones seguras puede prevenir la explotación de ataques de inyección SQL.
➔ Linux Reverse Shell Indicator ➔ CVE-2021-1675 Print Spooler Exploitation ➔ Lazarus Group Activity ➔ DNS RCE CVE-2020-1350 ➔ HAFNIUM Exchange Exploitation Activity ➔ Potential OWASSRF Exploitation Attempt - Proxy	Control CIS 07: Gestión continua de vulnerabilidades	Identificar y mitigar vulnerabilidades que puedan ser explotadas para crear reverse shells. Detectar y corregir vulnerabilidades específicas como CVE-2021-1675 y CVE-2020-1350. Identificar y mitigar vulnerabilidades que puedan ser explotadas por APTs. Detectar y corregir vulnerabilidades específicas explotadas por HAFNIUM.

		Detectar y mitigar intentos de explotación de vulnerabilidades OWASSRF.
	Control CIS 13: Monitoreo y defensa de la red	Detectar actividad sospechosa de grupos APT como Lazarus y de reverse shell es esencial para el monitoreo continuo y la defensa activa de la red. Monitorear intentos de explotación de vulnerabilidades críticas o actividad maliciosa relacionada con la explotación de servidores Exchange.
➔ Credentials In Files - Linux ➔ SQLite Firefox Profile Data DB Access ➔ VeeamBackup Database Credentials Dump Via Sqlcmd.EXE	Control CIS 03: Protección de los datos	Proteger la información sensible en bases de datos o en los perfiles del navegador, como credenciales, es crucial para evitar su extracción.
	Control CIS 13: Monitoreo y defensa de la red	Monitorear actividades que intenten acceder a credenciales en archivos, accesos no autorizados a bases de datos sensibles y actividades sospechosas que intentan volcar credenciales.
Aruba Network Service Potential DLL Sideloading	Control CIS 04: Configuración segura de activos y software empresarial	Configuraciones seguras para prevenir carga lateral de DLLs.
	Control CIS 13: Monitoreo y defensa de la red	Monitorear actividad sospechosa de carga lateral de DLL.
DarkSide Ransomware Pattern	Control CIS 10: Defensas contra malware	Detectar y prevenir la ejecución de ransomware.
	Control CIS 13: Monitoreo y defensa de la red	Monitorear actividad maliciosa relacionada con ransomware.
Security Onion IDH - SSH Accessed	Control CIS 06: Gestión de control de accesos	Gestionar y monitorear los accesos autorizados y no autorizados a los sistemas.
	Control CIS 13: Monitoreo y defensa de la red	Monitorear accesos sospechosos a servicios SSH.

ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184-668	Control CIS 13: Monitoreo y defensa de la red	Monitorear el tráfico de nodos de retransmisión Tor para identificar posibles actividades sospechosas.

Tabla 11

Resumen de la relación entre las detecciones obtenidas con S.O. y los controles CIS

		Controles CIS																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18
Detecciones	ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field ASCII		X		X														
	ET WEB_SPECIFIC_APPS iWare Professional SQL Injection Attempt -- index.php D UPDATE		X		X														
	Linux Reverse Shell Indicator							X						X					
	Credentials In Files - Linux			X										X					
	CVE-2021-1675 Print Spooler Exploitation							X						X					
	Aruba Network Service Potential DLL Sideloading				X									X					
	DarkSide Ransomware Pattern										X			X					
	Lazarus Group Activity							X						X					

	DNS RCE CVE-2020-1350							X						X					
	HAFNIUM Exchange Exploitation Activity							X						X					
	Security Onion IDH - SSH Accessed						X							X					
	Potential OWASSRF Exploitation Attempt - Proxy							X						X					
	SQLite Firefox Profile Data DB Access			X										X					
	VeeamBackup Database Credentials Dump Via Sqlcmd.EXE			X										X					
	SQL Injection Strings In URI		X		X														
	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184-668													X					

Nota. Se aprecia que 13 detecciones están relacionadas con el Control CIS 13, 6 detecciones con el Control CIS 07, 4 con el control CIS 04, 3 detecciones con los controles CIS 02 y 03, respectivamente, 1 detección con el Control CIS 06 y la detección restante con el Control CIS 10.

4.3.3. Recomendaciones y plan de acción

En esta sección, se proporcionarán recomendaciones y un plan de acción para mejorar la postura de seguridad de la Universidad Nacional de San Cristóbal de Huamanga, basada en los resultados de las detecciones realizadas por Security Onion y su relación con los controles CIS.

4.3.3.1. Grupo de implementación a la que pertenece la UNSCH

Se ha determinado que la UNSCH pertenece al Grupo de Implementación 2 (IG2), es decir, es una organización que maneja información sensible sobre los estudiantes, el personal o información organizacional y es capaz de soportar interrupciones breves de servicios, además de emplear individuos para administrar y proteger la infraestructura de TI.

4.3.3.2. Recomendaciones

A continuación, se describen las recomendaciones específicas basadas en las salvaguardas de los controles CIS con mayor cantidad de detecciones relacionadas. Para mayor detalle se puede ver el Anexo G.

Control CIS 13: Monitoreo y defensa de la red

- Centralización y monitoreo:
  - Centralizar alertas de eventos de seguridad.
  - Recopilar registros de flujo de tráfico de red.
- Detección de intrusiones:
  - Implementar una solución de detección de intrusiones basada en host.
  - Implementar una solución de detección de intrusiones en la red.
- Gestión del tráfico y acceso:
  - Realizar filtrado de tráfico entre segmentos de red.
  - Gestionar el control de acceso para activos remotos.

Control CIS 07: Gestión continua de vulnerabilidades

- Procesos de gestión y remediación:
  - Establecer y mantener un proceso de gestión de vulnerabilidades.
  - Establecer y mantener un proceso de remediación.
- Automatización y análisis de vulnerabilidades:
  - Realizar la gestión automatizada de parches del sistema operativo y de aplicaciones.
  - Realizar análisis automatizados de vulnerabilidades de activos internos de la organización y de activos empresariales expuestos externamente.

- Remediación:
    - Remediar las vulnerabilidades detectadas.

Control CIS 04: Configuración segura de activos y software empresarial

- Procesos de configuración:
    - Establecer y mantener un proceso de configuración seguro para los activos de la empresa, software y dispositivos de red.
- Seguridad de activos y software:
    - Configurar el bloqueo automático de sesiones en activos empresariales.
    - Implementar y administrar un firewall en servidores y dispositivos de usuario.
    - Administrar cuentas predeterminadas en activos y software empresariales.
    - Desinstalar o deshabilitar servicios innecesarios en activos y software empresariales.
- Seguridad de dispositivos:
    - Configurar servidores DNS confiables en activos empresariales.
    - Aplicar el bloqueo automático de dispositivos en portátiles y dispositivos móviles.
    - Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final.

Control CIS 02: Inventario y control de activos de software

- Inventario y gestión de software:
    - Elaborar y mantener actualizado el inventario de software.
    - Asegurarse de que el software autorizado cuente con soporte.
    - Tratamiento del software no autorizado.
- Herramientas y listas:
    - Utilizar herramientas automatizadas de inventario de software.

- Usar lista de permitidos para software autorizados y librerías autorizadas.

Control CIS 03: Protección de los datos

- Procesos de gestión de datos:
  - Establecer y mantener un proceso de gestión de datos, un inventario de datos y un esquema de clasificación de datos.
- Acceso y cifrado:
  - Configurar listas de control de acceso a datos.
  - Cifrar datos en dispositivos de usuarios, medios extraíbles, en tránsito y en reposo.
- Retención y eliminación:
  - Aplicar retención de datos.
  - Eliminar de forma segura los datos.
- Segmentación y documentación:
  - Documentar el flujo de datos.
  - Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad.

Control CIS 06: Gestión de control de accesos

- Procesos de acceso:
  - Establecer un proceso para conceder accesos y otro de revocación de acceso.
- Autenticación y control centralizado:
  - Exigir MFA para aplicaciones expuestas externamente, acceso remoto a la red y acceso administrativo.
  - Establecer y mantener un inventario de sistemas de autenticación y autorización.
  - Control de acceso centralizado.

Control CIS 10: Defensas contra malware

- Implementación y mantenimiento:
  - Implementar y mantener software anti-malware.
  - Configurar actualizaciones automáticas de firmas de antimalwares.

- Medidas preventivas:
    - Deshabilitar la ejecución automática y la reproducción automática para medios extraíbles.
    - Configurar el análisis anti-malware automático de medios extraíbles.
    - Habilitar funciones anti-explotación.
- Gestión centralizada:
    - Administrar de forma centralizada el software antimalware.
    - Utilizar el software anti-malware basado en el comportamiento.

4.3.3.3. Prioridades de implementación

Para garantizar una mejora efectiva en la seguridad de la UNSCH, se recomienda seguir un enfoque escalonado, priorizando la implementación de salvaguardas de acuerdo con su relevancia para los grupos de implementación (ver Anexo G, columnas IG1 e IG2). Este enfoque se detalla a continuación:

- Implementación de salvaguardas para IG1: Las salvaguardas marcadas para IG1 representan las medidas de seguridad fundamentales que deben ser adoptadas de manera prioritaria. Estas medidas aseguran una base sólida de protección y son esenciales para la operación continua de la organización.
- Implementación de salvaguardas para IG2: Una vez implementadas las salvaguardas de IG1, se deben abordar las medidas específicas para IG2. Estas salvaguardas complementan las implementaciones iniciales y están diseñadas para manejar los riesgos adicionales y las complejidades de una organización con perfiles de riesgo variados y mayor sensibilidad de datos.

4.3.3.4. Plan de acción

- Evaluación inicial: Realizar una auditoría completa de la infraestructura actual de TI y seguridad para identificar brechas y conocer lo que se tiene para protegerlo adecuadamente.
- Desarrollo de políticas: Crear o actualizar políticas de seguridad basadas en las mejores prácticas descritas por los controles CIS, adaptándolas a las necesidades específicas de la red de la ciudad universitaria.

- Implementación: Desplegar las soluciones necesarias, comenzando con las salvaguardas de IG1 y luego avanzando a las de IG2. Esto incluye la configuración y puesta en marcha de herramientas como SIEM, HIDS, NIDS, y soluciones de gestión de parches.
- Capacitación y Concienciación: Implementar programas de capacitación para el personal de TI y los usuarios finales, asegurando que comprendan y adopten las nuevas medidas de seguridad.
- Monitoreo y mejora continua: Establecer un proceso continuo de monitoreo y revisión de la efectividad de las medidas implementadas, ajustando las políticas y prácticas según sea necesario para adaptarse a nuevas amenazas y cambios en el entorno de TI.

En la práctica, algunas de estas acciones pueden llevarse a cabo en paralelo para optimizar el tiempo y los recursos:

- Evaluación inicial y Desarrollo de políticas: Mientras se realiza la auditoría completa, se puede comenzar a redactar y actualizar las políticas de seguridad, ya que estas se basan en las mejores prácticas y no dependen completamente de los hallazgos de la auditoría.
- Implementación y Capacitación: Durante la fase de implementación, se puede iniciar la capacitación del personal. Por ejemplo, mientras se implementa un sistema SIEM (Security Information & Event Management), el personal puede recibir capacitación sobre cómo interpretar y responder a las alertas de seguridad.
- Monitoreo y mejora continua: Este proceso debe iniciarse tan pronto como se implementen las primeras salvaguardas, asegurando que cualquier brecha o vulnerabilidad detectada durante la implementación sea abordada de inmediato.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

La implementación de Security Onion en la UNSCH ha demostrado que tal herramienta es eficaz para la auditoría de redes, proporcionando una plataforma robusta y versátil que combina múltiples herramientas de seguridad en una solución integrada para la detección de incidentes de seguridad.

A. Security Onion, como herramienta de auditoría basada en la monitorización de seguridad, ha permitido la detección de actividades sospechosas y anomalías en la red de la ciudad universitaria de la UNSCH lo que, si se tienen en cuenta los salvaguardas de los Controles CIS, da pie al fortalecimiento de la seguridad preventiva y la capacidad de reacción ante incidentes.
B. La gestión de logs de Security Onion ha permitido la recopilación, almacenamiento y análisis de los registros de eventos generados por dispositivos y aplicaciones en la red de la ciudad universitaria. Esto ha proporcionado una visión amplia de las actividades en la red, permitiendo la detección de incidentes de seguridad y la identificación temprana de patrones sospechosos, posibilitando la trazabilidad de eventos críticos.
C. En vista que Security Onion incluye ciertos sistemas de detección de intrusos, se pudo identificar actividades maliciosas en la red.

5.2. RECOMENDACIONES

A. Para obtener mayores detecciones de actividades sospechosas en la red, en el tipo de despliegue EVAL, se recomienda activar las reglas de Suricata, Zeek o Sigma que están deshabilitadas por defecto y que se consideran relevantes.
B. Realizar el tipo de despliegue Standalone en vista que hay opciones o herramientas que no se permite utilizar en el despliegue EVAL.
C. Monitorear y analizar detenidamente el tráfico TOR en la red para identificar posibles amenazas ocultas, esta recomendación puntual se da debido a la correlación entre las detecciones "DarkSide Ransomware

Pattern" y "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184-668".

D. Tener en consideración lo mencionado en la sección *4.3.3. Recomendaciones y plan de acción* para que la Universidad Nacional de San Cristóbal de Huamanga pueda mejorar su postura de seguridad, protegiendo así sus activos digitales y la información sensible de estudiantes y personal.

REFERENCIAS

AO Kaspersky Lab. (s.f.). *¿Qué es una amenaza avanzada persistente (APT)?* Kaspersky. Recuperado el 20 de julio de 2024 de https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Aruba Network Service Potential DLL Sideloading. (2024, February 1). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/windows/image_load/image_load_side_load_aruba_networks_virtual_intranet_access/

Beasley, J. S., & Nilkaev, P. (2022). *NETWORKING ESSENTIALS: SIXTH EDITION A COMPTIA NETWORK+ N10-008 TEXTBOOK* (M. Taber, Ed.; 6 - Instructor Edition ed.). Pearson Education.

Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.

Bernal Torres, C. A. (2016). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales*. Pearson Educación de Colombia S.A.S.

Carrasco Díaz, S. (2015). *Metodología de la investigación científica: pautas metodológicas para diseñar y elaborar el proyecto de investigación*. San Marcos.

Center for Internet Security, Inc. (2021, Mayo). *Controles CIS Versión 8* (8, Español ed.) [Critical Security Controls versión 8]. Center for Internet Security, Inc.

Chakraborty, M., Singh, M., Balas, V. E., & Mukhopadhyay, I. (Eds.). (2020). *The "Essence" of Network Security: An End-to-End Panorama*. Springer Nature Singapore. https://doi.org/10.1007/978-981-15-9317-8

Check Point Software Technologies. (2024). *Check Point 2024 Cyber Security Report*. Check Point Research.

Cibersecurity & Infraestructure Security Agency (CISA). (2021, July 8). *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. CISA. Recuperado el 20 de julio de 2024 de https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

Cloud IT. (2022, Enero). *Informe técnico final* (1) [Contratación del servicio de instalación de equipos y cableado estructurado para el proyecto

"Mejoramiento de las herramientas tecnológicas para las actividades académicas en la ciudad universitaria de la Universidad Nacional de San Cristóbal de Huamanga"].

Cozzupoli, J., Nizamuddin, K., Adeopatoye, R., Kumar, Y., & S., J. (2024, March 15). *How can you choose relevant information security standards?* Linkedin. Recuperado el 26 de mayo de 2024 de https://es.linkedin.com/advice/0/how-can-you-choose-relevant-information-security-eplrc?lang=en

Credentials In Files - Linux. (2023, April 30). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/linux/auditd/lnx_auditd_find_cred_in_files/

Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE.

CVE-2021-1675 Print Spooler Exploitation. (2023, June 20). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/emerging-threats/2021/exploits/cve-2021-1675/win_exploit_cve_2021_1675_printspooler_operational/

DarkSide Ransomware Pattern. (2023, June 20). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/emerging-threats/2021/malware/darkside/proc_creation_win_malware_darkside_ransomware/

Deuble, A., & Shinberg, D. (2012, July 26). *Using and Configuring Security Onion to detect and prevent Web Application Attacks* [Detecting and preventing web applications attacks with Security Onion]. SANS Institute.

Disso, J. P., & Younas, M. (2018). The world of malware: an overview. In *2018 IEEE 6th International Conference on Future Internet of Things and Cloud - FiCloud 2018: 6-8 August 2018, Barcelona, Spain : Proceedings* (pp. 420–427). IEEE. 10.1109/FiCloud.2018.00067

DNS RCE CVE-2020-1350. (2023, June 20). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/emerging-threats/2020/exploits/cve-2020-1350/proc_creation_win_exploit_cve_2020_1350/

Dos Santos de Carvalho Ribeiro, T. C. (2016). *Fundamentos de redes de computadores*. Editora e Distribuidora Educacional S.A.

Elasticsearch B.V. (s.f.). *Kibana: Explora, visualiza y descubre datos*. Elastic. Recuperado el 26 de abril de 2023 de https://www.elastic.co/es/kibana/

Elasticsearch B.V. (s.f.). *¿Qué es Elasticsearch? - Elasticsearch: Motor de búsqueda y analítica distribuido oficial*. Elastic. Recuperado el 26 de abril de 2023 de https://www.elastic.co/es/what-is/elasticsearch

Ertel, J. (s.f.). *ElastAlert 2 - Automated rule-based alerting for Elasticsearch — ElastAlert 2 0.0.1 documentation*. ElastAlert 2. Recuperado el 26 de abril de 2023 de https://elastalert2.readthedocs.io/en/latest/elastalert.html#overview

Forbes Perú. (2024, Marzo 25). El Perú sufrió 5.000 millones de intentos de ciberataques en 2023, reportó Fortinet. *Forbes*. https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet

Fortinet. (s.f.). *Outbreak Alerts Annual Report 2023* [FortiGuard Labs Outbreak Alerts provide a unique analysis of the threat landscape throughout the tech ecosystem.]. FortiGuard Labs.

Gonzáles, R., Watkins, A. B., & Simpson, C. (2015). *Using Security Onion for Hands-On Cybersecurity Labs*. American Society for Engineering Education/Pacific South West Conference.

Google Open Source. (2022, November 4). *Stenographer is a packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets. Discussion/announcements at stenographer@googlegroups.com*. GitHub. Recuperado el 26 de abril de 2023 de https://github.com/google/stenographer

Gupta, S., & Leune, K. (2012, July 4). *Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment*. SANS Institute.

HAFNIUM Exchange Exploitation Activity. (2023, November 28). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/emerging-threats/2021/ta/hafnium/proc_creation_win_apt_hafnium/

Heenan, R., & Moradpoor, N. (2016, May 10). *Introduction to Security Onion.* (The First Post Graduate Cyber Security Symposium - Edinburgh Napier University, Edinburgh, United Kingdom) [Paper presented at The First Post Graduate Cyber Security Symposium]. Introduction to Security

Onion-AbertayUniversity. Recuperado el 23 de abril de 2024 de http://thecyberacademy.org/wp-content/uploads/2016/05/PGCS-symposium_2016_paper_6.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (R. Hernández Sampieri, Ed.). McGraw-Hill Education.

Hickman, A., & Graves, R. (2016, February 1). *Gaining Visibility on the Network with Security Onion: A Cyber Threat Intelligence Based Approach* (GIAC (GSEC) Gold Certification). SANS Institute.

Hjelmvik, E. (2015, June 14). *Hands-on Network Forensics* (Swedish Armed Forces CERT FIRST). Forum of Incident Response and Security Teams. Recuperado el 23 de abril de 2024 de https://www.first.org/resources/papers/conf2015/first_2015_-_hjelmvik-_erik_-_hands-on_network_forensics_20150604.pdf

IBM. (s.f.). *¿Qué es la exfiltración de datos?* IBM. Recuperado el 20 de julio de 2024 de https://www.ibm.com/es-es/topics/data-exfiltration

IBM, Caridi, C., Dwyer, J., Prassinos, G., Metrick, K., Zeizel, A., Chung, J., McMillen, D., Shipley, B., Hammond, C., Mühr, G., Villadsen, O., Fasulo, J., Zaboeva, C., Frydrych-Dean, M., Emerson, R., Singleton, C., Alvarez, M., Piazza, A., … Cassagne, J. (2024, Febrero). *X-Force Threat Intelligence Index 2024 Resumen ejecutivo*. IBM.

Jackson, C. (2010). *Network Security Auditing*. Cisco Press.

Kizza, J. M. (2020). *Guide to Computer Network Security*. Springer International Publishing. https://doi.org/10.1007/978-3-030-38141-7

Laurent, M., & Bouzefrane, S. (2015). *Digital Identity Management* (M. Laurent & S. Bouzefrane, Eds.). Elsevier Science. https://doi.org/10.1016/C2015-0-00282-9

Lazarus Group Activity. (2023, June 20). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/emerging-threats/2020/ta/lazarus/proc_creation_win_apt_lazarus_group_activity/

THE LINUX FOUNDATION PROJECTS. (s.f.). *osquery*. Welcome to osquery. Recuperado el 26 de abril de 2023 de https://osquery.readthedocs.io/en/stable/

Linux Reverse Shell Indicator. (2023, August 28). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/linux/network_connection/net_connection_lnx_back_connect_shell_dev/

Lockheed, M. (2015). *Gaining the advantage: Applying Cyber Kill Chain® Methodology to Network Defense*.

Maier, C., Thatcher, J. B., Grover, V., & Dwivedi, Y. K. (2023, June). Cross-sectional research: A critical perspective, use cases, and recommendations for IS research. *International Journal of Information Management*, *70*(102625). https://doi.org/10.1016/j.ijinfomgt.2023.102625.

Manjunatha, N. (2019). Descriptive Research. *Journal of Emerging Technologies and Innovative Research (JETIR)*, *6*(6), 863-867.

Marotti de Mello, A., & Wood Jr, T. (2019). What is applied research anyway? *Revista de Gestão*, *26*(4), 338-339. 10.1108/REGE-10-2019-128

Meyer, R., & Cid, C. (2008, January 26). *Detecting Attacks on Web Applications from Log Files*. SANS Institute.

Mobeen, N., Mahawish, Bushra, Misbah, P., Soomal, F., & Maham. (2021, March). A Review on Security Onion Tools for Intrusion Detection. *International Journal of Scientific & Engineering Research*, *12*(3), 599-607.

N-able Solutions ULC and N-able Technologies Ltd. (2020, October 1). *How to Perform a Network Audit: A Step-By-Step Guide*. N-able. Recuperado el 29 de abril de 2023 de https://www.n-able.com/blog/how-to-perform-network-audit

NexTReT Ciberseguridad S.L. (s.f.). *Monitorización de Seguridad*. Spidernext. Recuperado el 29 de julio de 2024 de https://spidernext.com/monitorizacion-de-seguridad/

Open Information Security Foundation (OISF). (s.f.). *Suricata User Guide*. Suricata 6.0.11 documentation. Recuperado el 24 de abril de 2023 de https://suricata.readthedocs.io/en/suricata-6.0.11/

Organización para la Cooperación y el Desarrollo Económicos. (2018). *Manual de Frascati 2015: Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental* (OECD Publishing, Paris/FEYCT, Madrid ed.). https://doi.org/10.1787/9789264310681-es.

Perù21. (2023, Agosto 30). Perú fue el objetivo de más de 3.000 millones de intentos de ciberataques en el 2023. *Peru21*. https://peru21.pe/cheka/tecnologia/ciberseguridad-ciberataques-fortinet-peru-fue-el-objetivo-de-mas-de-3000-millones-de-intentos-de-ciberataques-en-el-2023-noticia/

Potential OWASSRF Exploitation Attempt - Proxy. (2024, February 26). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/emerging-threats/2022/exploits/cve-2022-41082/proxy_cve_2022_36804_exchange_owassrf_exploitation/

Quispe, J. (2023, Noviembre 23). Pymes fueron las más afectadas por ciberataques en el 2023: los ataques más comunes. *Gestión*. https://gestion.pe/tecnologia/pymes-fueron-las-mas-afectadas-por-ciberataques-en-el-2023-por-que-empresas-peruanas-emprendimientos-negocios-noticia/

Rodríguez, G. (2023, Agosto 22). Perú es el cuarto país de América Latina con más ciberataques. *América Retail*. https://www.america-retail.com/peru/peru-es-el-cuarto-pais-de-america-latina-con-mas-ciberataques/

Russinovich, M., & Garnier, T. (2023, April 10). *Sysmon - Sysinternals*. Microsoft Learn. Recuperado el 27 de abril de 2023 de https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Saini, S. K., Singh, P., IEEE Staff, & INDIACom. (2016). *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (M. N. Hoda, Ed.). IEEE.

Sanders, C. (2020). *Intrusion Detection Honeypots: Detection Through Deception*. Applied Network Defense.

Schwartau, W. (2021, December 12). It's About Time: The Unappreciated Fundamental Metric for Security. *Cyber Defense Magazine*. https://winnschwartau.com/wp-content/uploads/2021/12/TBS-Overview-Metrics-12Dec2021.pdf

Security Onion Solutions. (s.f.). *Introduction — Security Onion Documentation 2.4 documentation*. Security Onion Documentation. Recuperado el 27 de abril de 2023 de https://docs.securityonion.net/en/2.4/introduction.html

Shin, B. (2021). *A Practical Introduction to Enterprise Network and Security Management*. Auerbach Publishers, Incorporated.

SQL Injection Strings In URI. (2023, September 6). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/web/webserver_generic/web_sql_injection_in_access_logs/

SQLite Firefox Profile Data DB Access. (2023, December 1). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/windows/process_creation/proc_creation_win_sqlite_firefox_gecko_profile_data/

Target. (s.f.). *Strelka: Real-time, container-based file scanning at enterprise scale*. GitHub. Recuperado el 27 de abril de 2023 de https://github.com/target/strelka

VeeamBackup Database Credentials Dump Via Sqlcmd.EXE. (2023, February 13). DETECTION.FYI. Recuperado el 17 de julio de 2024 de https://detection.fyi/sigmahq/sigma/windows/process_creation/proc_creation_win_sqlcmd_veeam_dump/

Vinod, M., Singh, G. D., & Anandh, V. (2018). *CCNA Security 210-260 Certification Guide: Build Your Knowledge of Network Security and Pass Your CCNA Security Exam (210-260)*. Packt Publishing.

Wazuh Inc. (s.f.). *Getting started with Wazuh*. Wazuh documentation. Recuperado el 27 de abril de 2024 de https://documentation.wazuh.com/current/getting-started/index.html

Z3R0th. (2020, February 16). *Setting up Security Onion at home | by Z3R0th | Medium*. Medium. Recuperado el 21 de mayo de 2024 de https://z3r0th.medium.com/setting-up-security-onion-at-home-717340816b4e

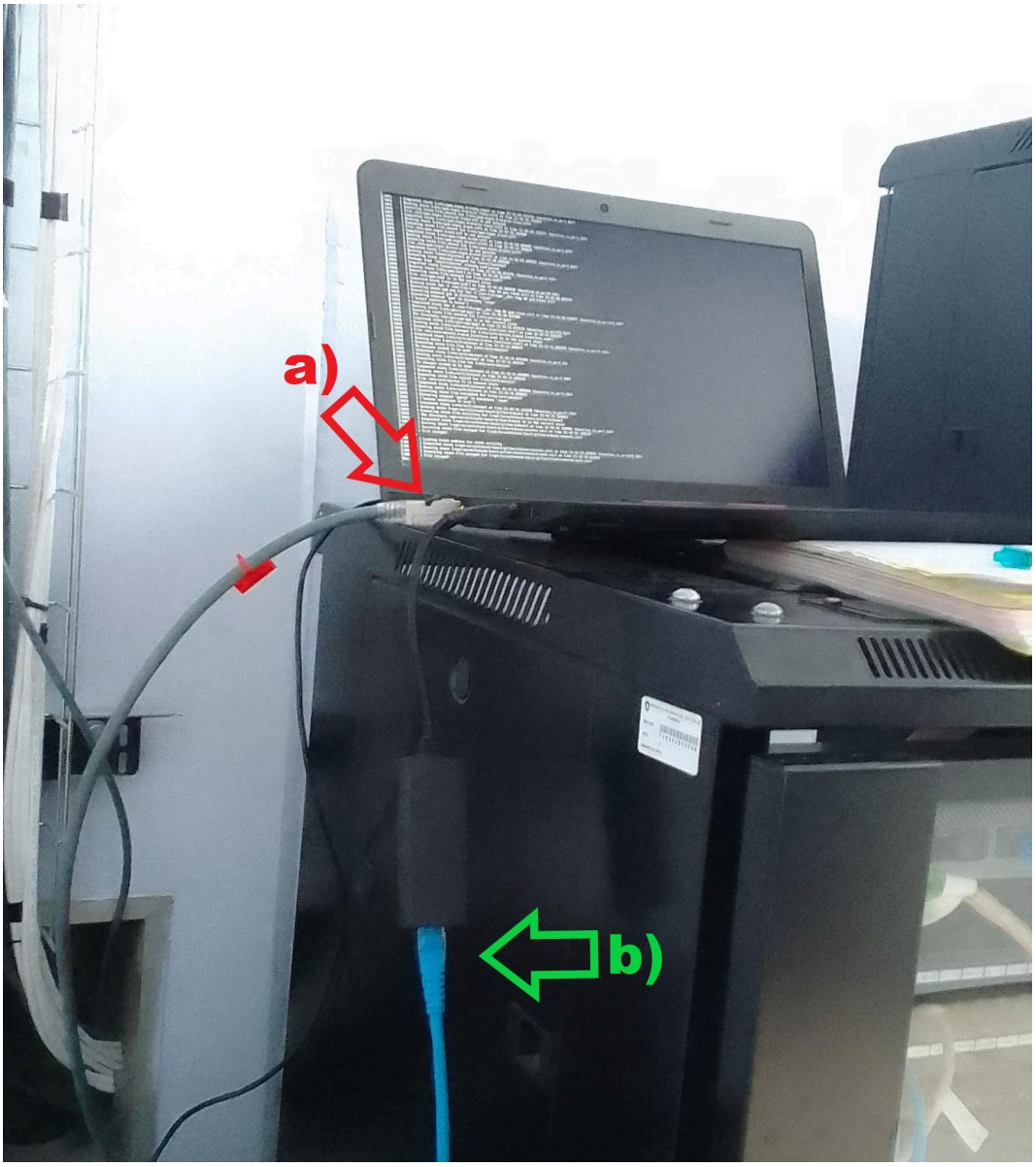
The Zeek Project. (s.f.). *About Zeek — Book of Zeek*. Zeek Documentation. Recuperado el 27 de abril de 2024 de https://docs.zeek.org/en/master/about.html

ANEXOS

ANEXO A: Laptop en la que se instaló Security Onion

Figura 25

Laptop en la que se instaló Security Onion.



Nota. Se observa 2 cables de red conectados a la laptop. a) El cable está conectado al puerto SPAN del switch, es decir, este brinda los datos a analizar por Security Onion. b) Permite obtener una dirección IP para conectarnos a la consola web de Security Onion.

ANEXO B: Capturas de la primera etapa de instalación de Security Onion

Figura 26

Vista inicial al conectar el USB booteado a la laptop, en la que se selecciona la 1era opción para iniciar el proceso de instalación.

Figura 27

Para confirmar la instalación se escribe "yes", se presiona la tecla Enter y se establece un nombre de usuario y una contraseña.

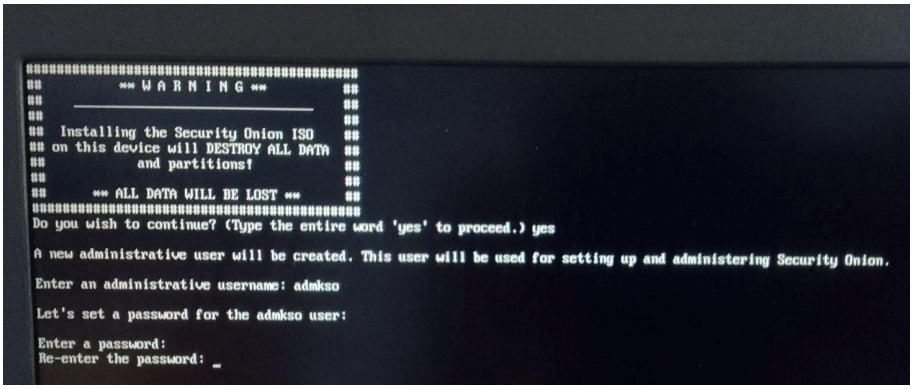
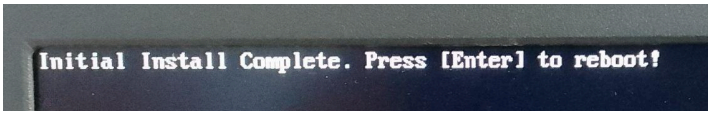


Figura 28

Mensaje que aparece al finalizar la primera parte de la instalación, se presiona la tecla Enter para reiniciar la máquina en la que se está instalando.



ANEXO C: Capturas de la segunda etapa de instalación de Security Onion y configuración

Figura 29

Interfaz que se muestra después del reinicio de la máquina, en la que se debe ingresar las credenciales establecidas anteriormente (ver Figura 28).

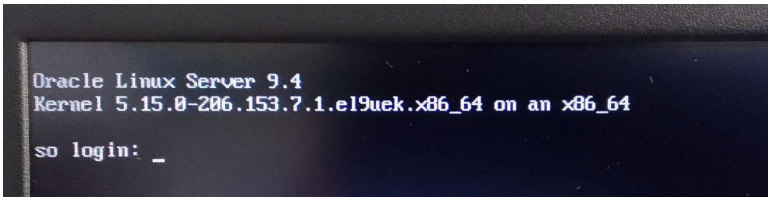


Figura 30

Ventana en la que se presiona "Enter" sobre la opción "Yes" para continuar la instalación y configuración de S. O.

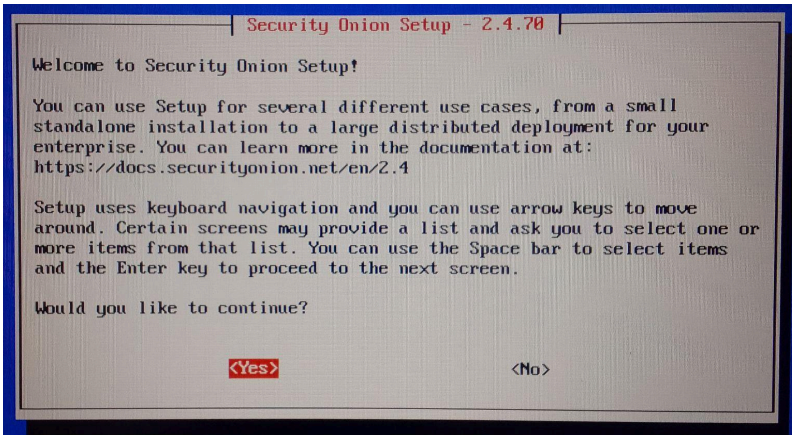


Figura 31

Tipos de despliegue de S.O., la opción a elegir en este caso es EVAL.

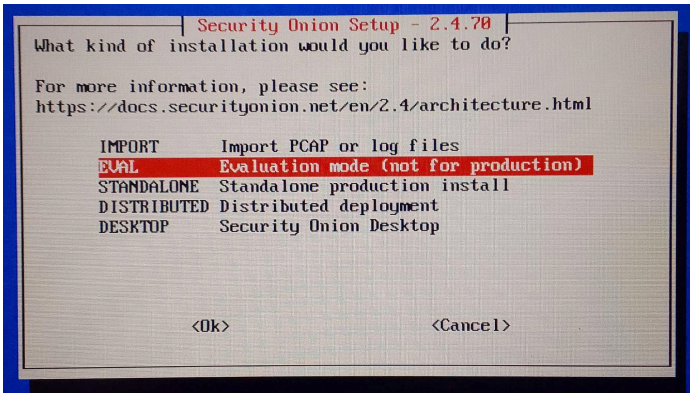


Figura 32

Interfaz en la que debemos escribir “AGREE”, denotando nuestro acuerdo con los términos de Elastic License versión 2, para continuar con la instalación.

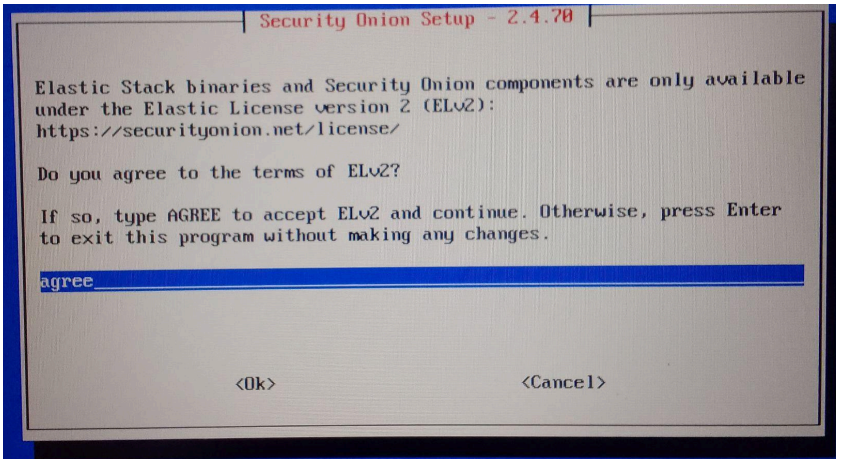


Figura 33

Interfaz en la que se selecciona el tipo de instalación de acuerdo a la existencia o no de conexión a internet, en este caso se selecciona la opción “Standard”.

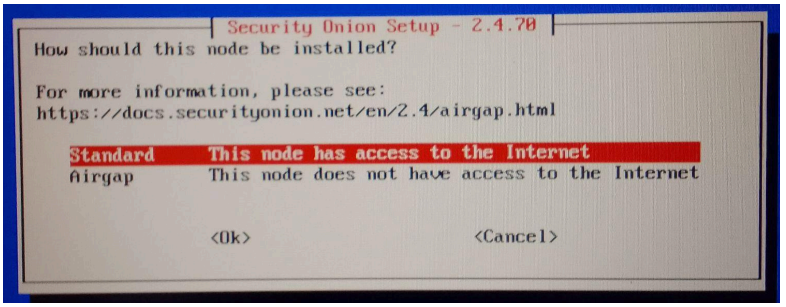


Figura 34

Interfaz en la que ingresamos el nombre del equipo, aquí se le asignó “so”.

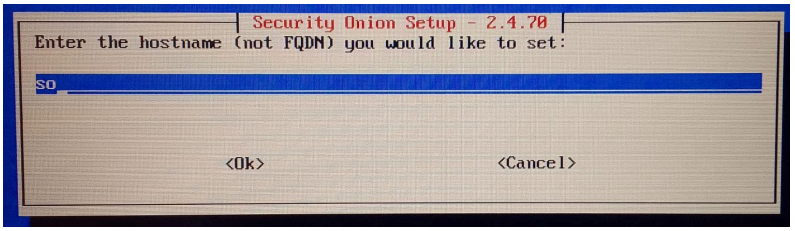


Figura 35

Vista en la que se selecciona la interfaz de red que nos dará una IP.

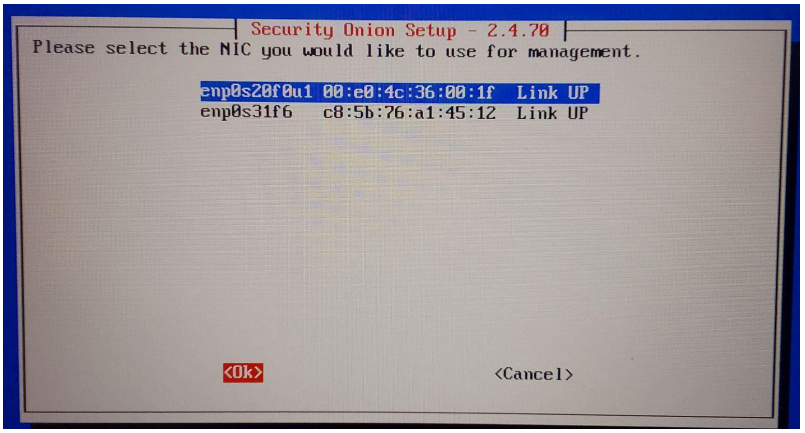


Figura 36

Vista en la que se selecciona el modo en que asignará una IP a la máquina en la que se está instalando S.O, en esta captura se puede observar que la opción seleccionada es DHCP para obtener una IP dinámica.

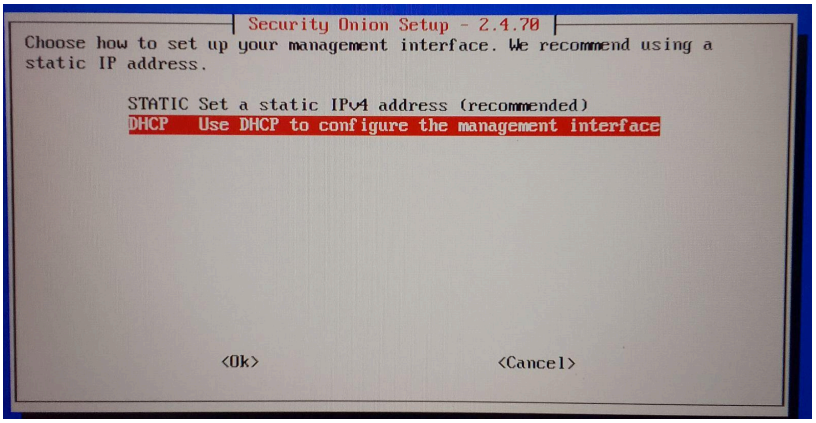


Figura 37

Ventana para aceptar el riesgo de que S.O. falle cuando la IP cambie.

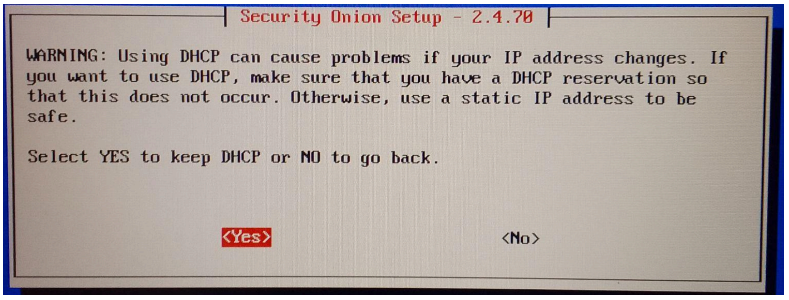


Figura 38

Interfaz en la que se selecciona el tipo de conexión a internet con la que se trabajará.

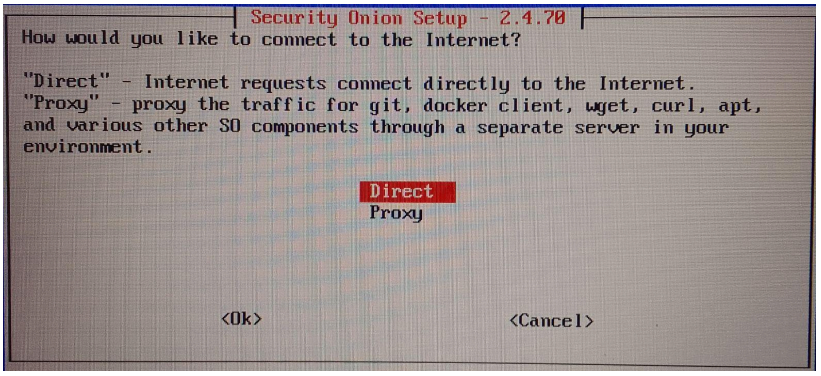


Figura 39

Se selecciona la configuración por defecto de Docker.

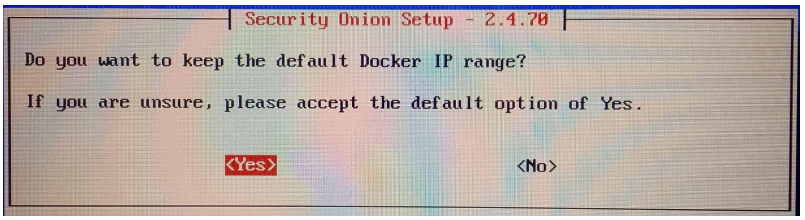


Figura 40

Interfaz en la que se selecciona la interfaz que está conectada al puerto SPAN, es decir, la interfaz que recibirá los datos para su análisis.

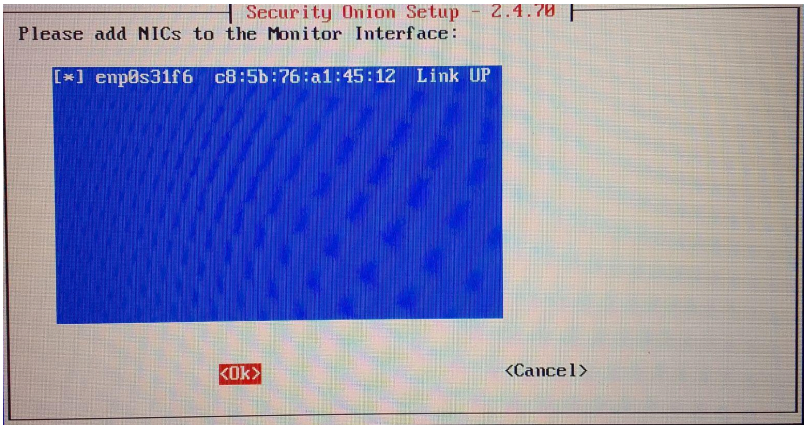


Figura 41

Ventana en la que se ingresa el correo electrónico con el que se iniciará sesión en la consola web de S.O.

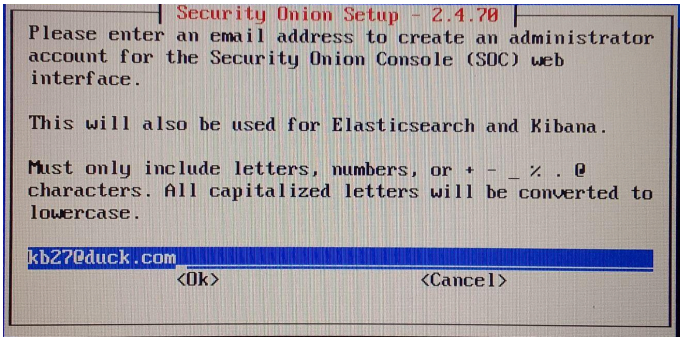


Figura 42

Ventana en la que se ingresa la contraseña para el correo electrónico ingresado en la anterior interfaz.

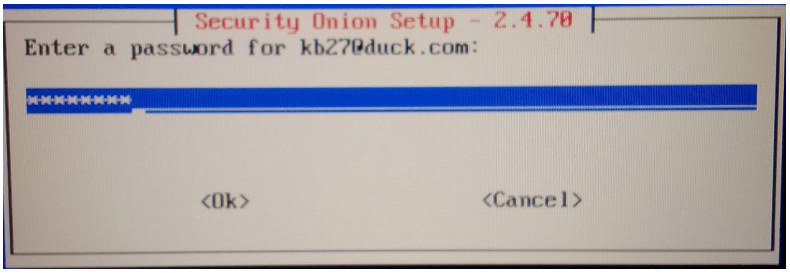


Figura 43

Ventana en la que se re-ingresa la contraseña.

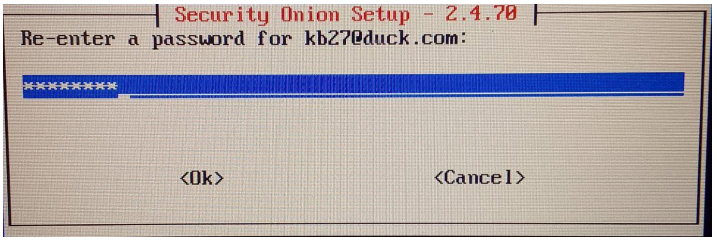


Figura 44

Ventana en la que se selecciona de qué manera se ingresará a la consola web.

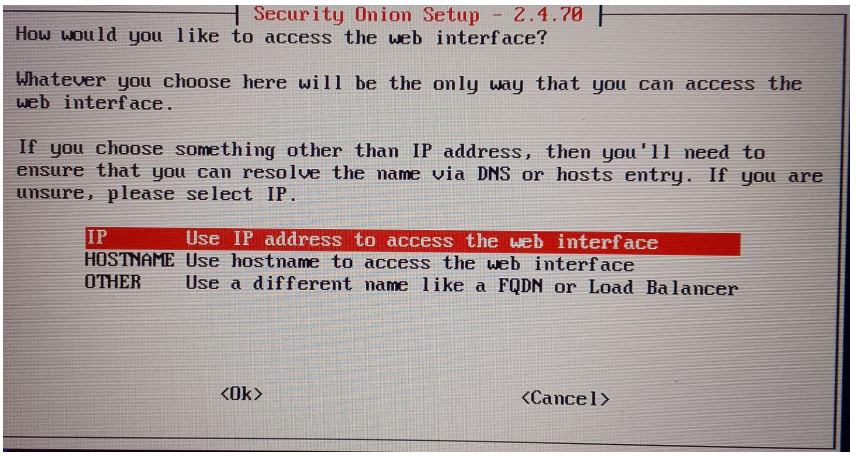


Figura 45

Ventana en la que se reafirma nuestra intención de conectarnos a S.O. desde la web.

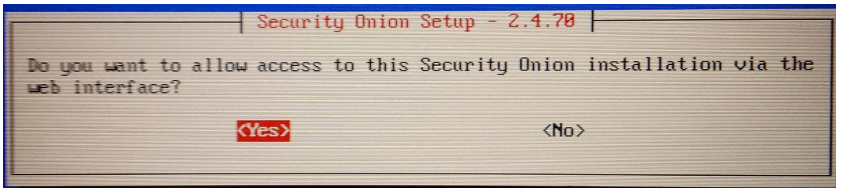


Figura 46

Interfaz en la que se indica la IP o el segmento de red en la que se encuentran los equipos que tendrán acceso a la consola web de S.O.

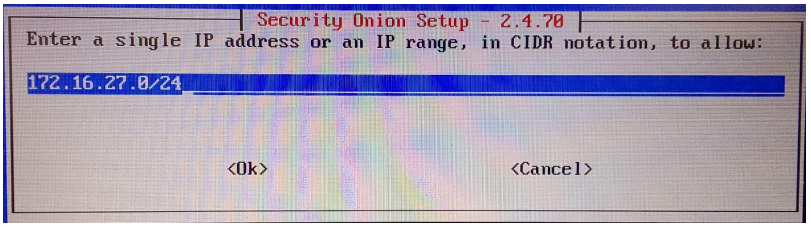


Figura 47

Interfaz en la que se selecciona si se desea colaborar enviando datos de telemetría, en esta ocasión se seleccionó "Yes".

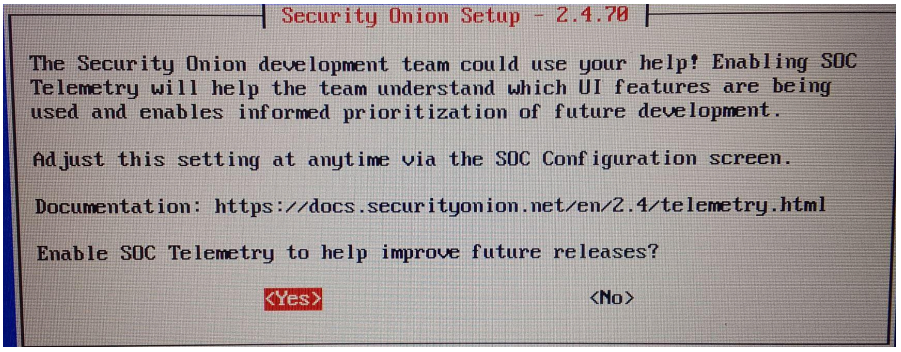
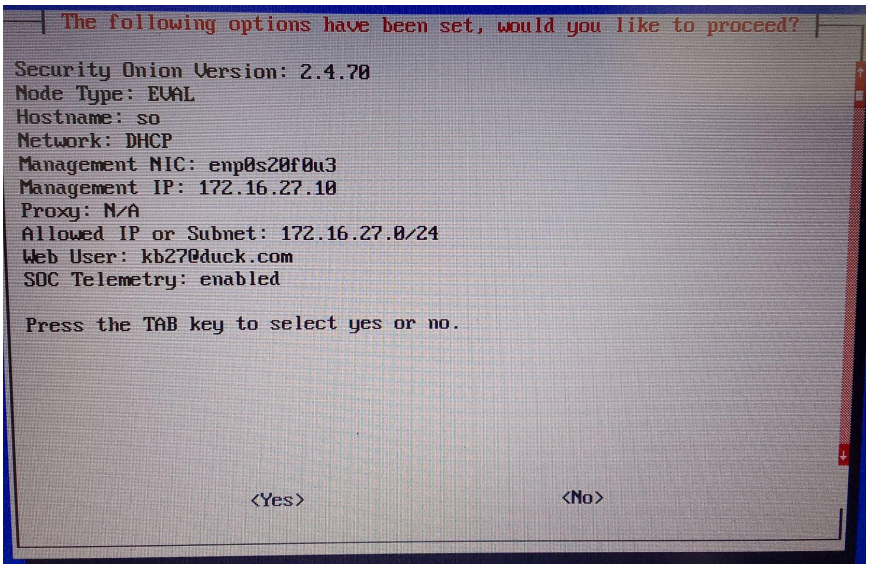


Figura 48

Vista que nos muestra la configuración establecida para S.O.



ANEXO D: Inicio de sesión en Security Onion

Para iniciar sesión en la consola web de Security Onion debemos ingresar a la IP asignada al nodo en la etapa de configuración a través del navegador de un dispositivo autorizado en la red. Al realizarlo, se mostrará una alerta de "riesgo potencial", como se ilustra en la Figura 49. Para continuar, se debe seleccionar las opciones avanzadas y hacer clic en el botón para aceptar el riesgo. A

continuación, aparecerá la interfaz de inicio de sesión de Security Onion, donde se deben ingresar las credenciales establecidas durante la segunda etapa de la instalación (ver Figura 50).

Figura 49

Alerta que muestra el navegador al intentar ingresar a la consola de Security Onion

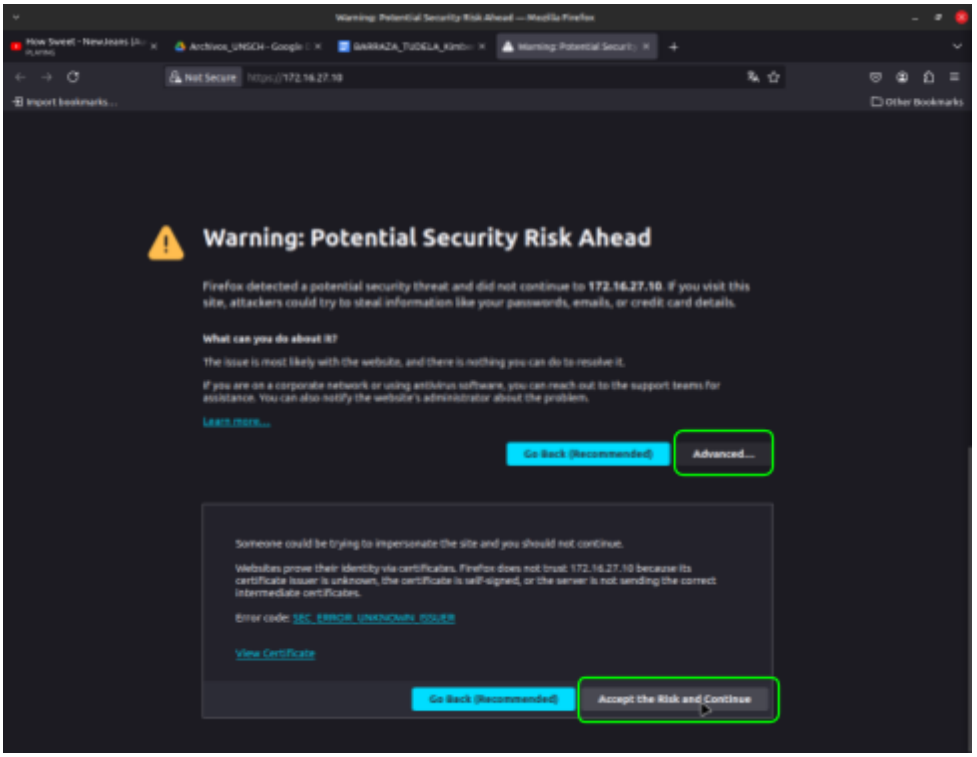
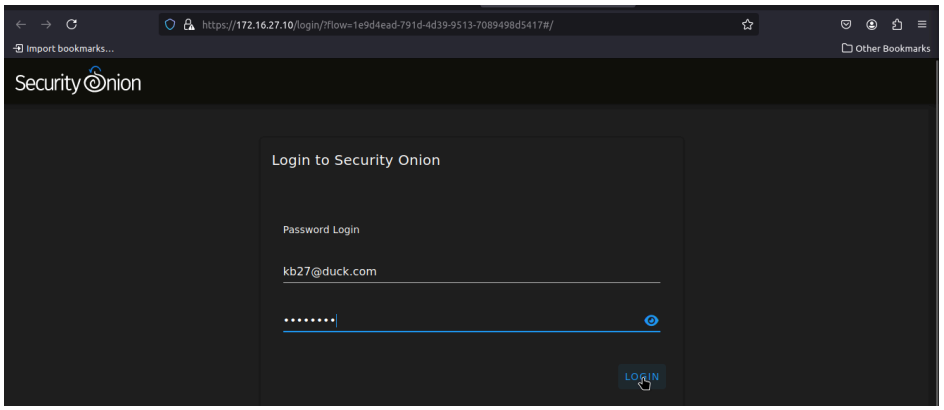


Figura 50

Interfaz de acceso a la consola web de Security Onion



ANEXO E: Rendimiento del nodo de Security Onion

Para ver el rendimiento de todo el nodo de Security Onion se debe ingresar a InfluxDB, el hipervínculo se encuentra en el menú lateral de la consola web de Security Onion.

Figura 51

Selección de la opción InfluxDB

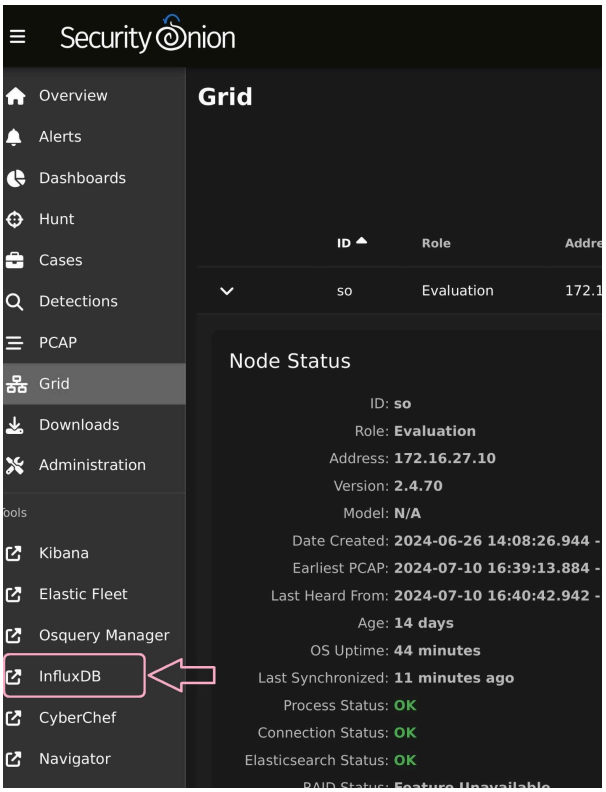


Figura 52

Interfaz de inicio de sesión de InfluxDB

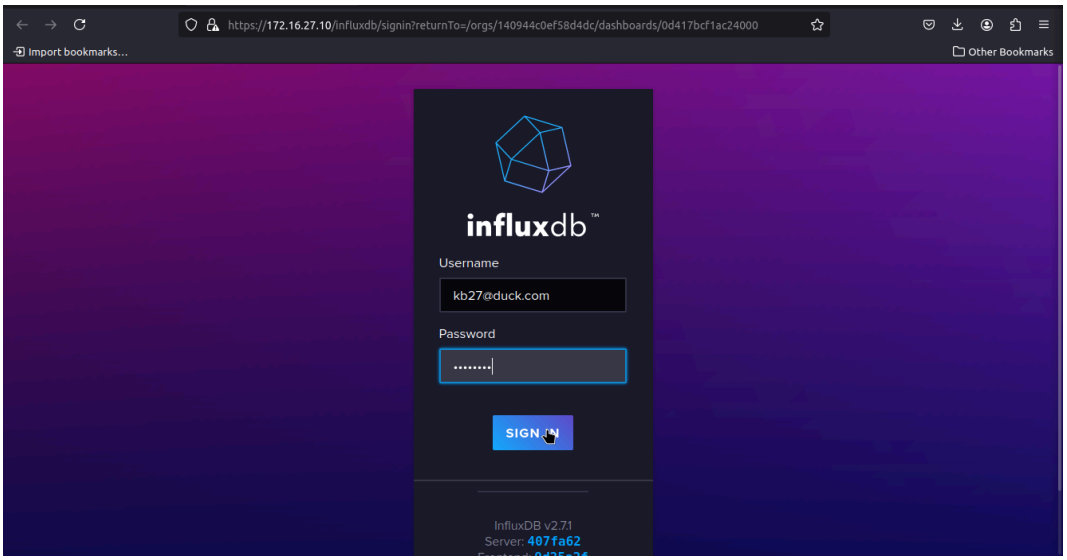


Figura 53

Interfaz de InfluxDB que muestra el rendimiento del nodo de Security Onion (Parte 1).

Nota. En la imagen se observa el tiempo de actividad, la carga media , la EPS estimada (en porcentaje), la cola de Redis, el tráfico entrante, las caídas entrantes, la pérdida de captura, la pérdida de Zeek. la pérdida de Suricata, la pérdida de Stenographer, la retención de captura de paquetes, las alarmas críticas, las alarmas de advertencia, las alarmas informativas, el uso de CPU, el uso de memoria, el uso de Swap y el estado de las alarmas del nodo de Security Onion.

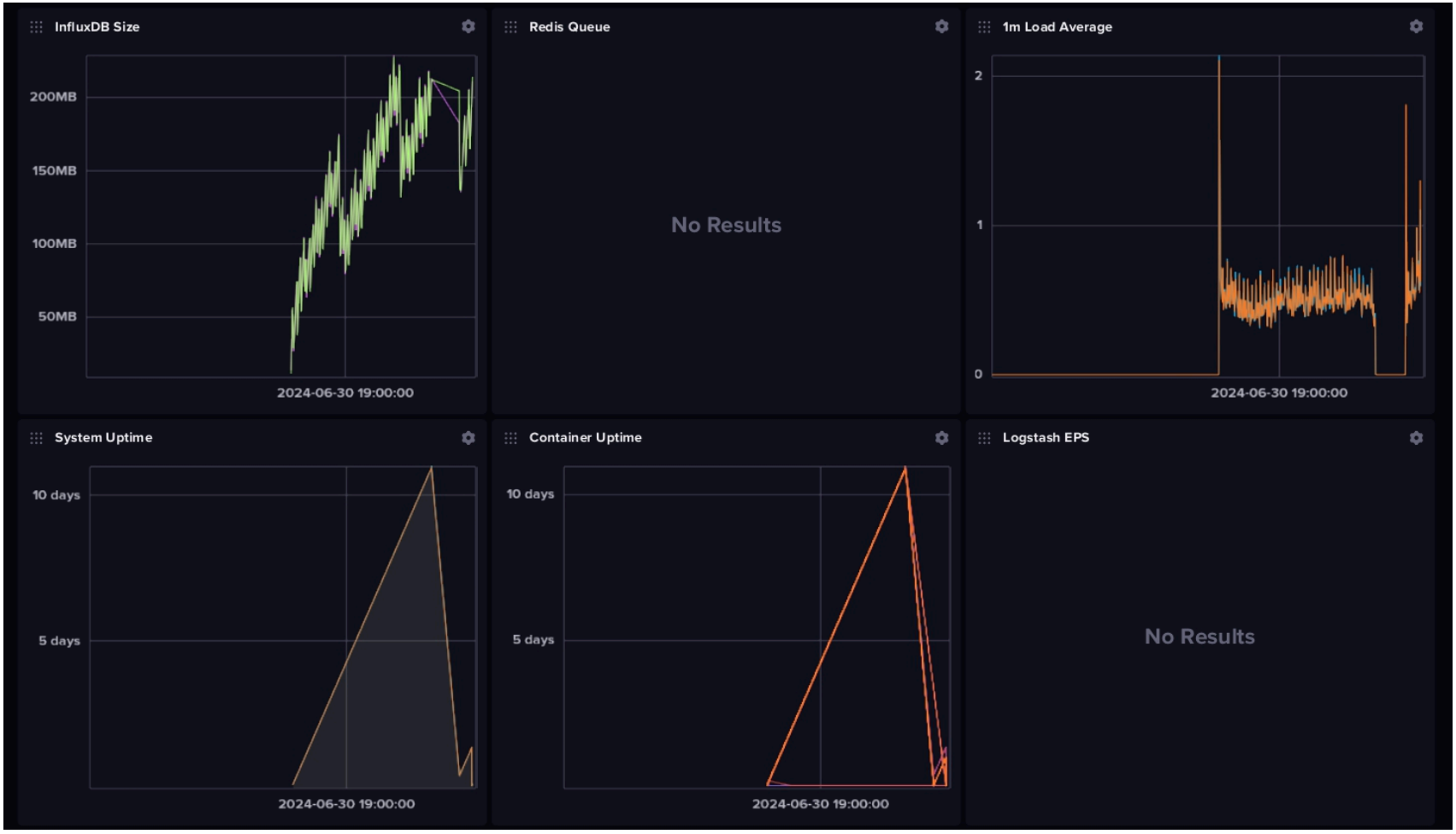
Figura 54

Interfaz de InfluxDB que muestra el rendimiento del nodo de Security Onion (Parte 2).

Nota. En la imagen se observa el uso del disco raíz, el uso del disco NSM, los eventos más recientes del contenedor, el tamaño de almacenamiento de Elasticsearch, el recuento de documentos de Elasticsearch y el tiempo de captura empleado por Elastic del nodo de Security Onion.

Figura 55

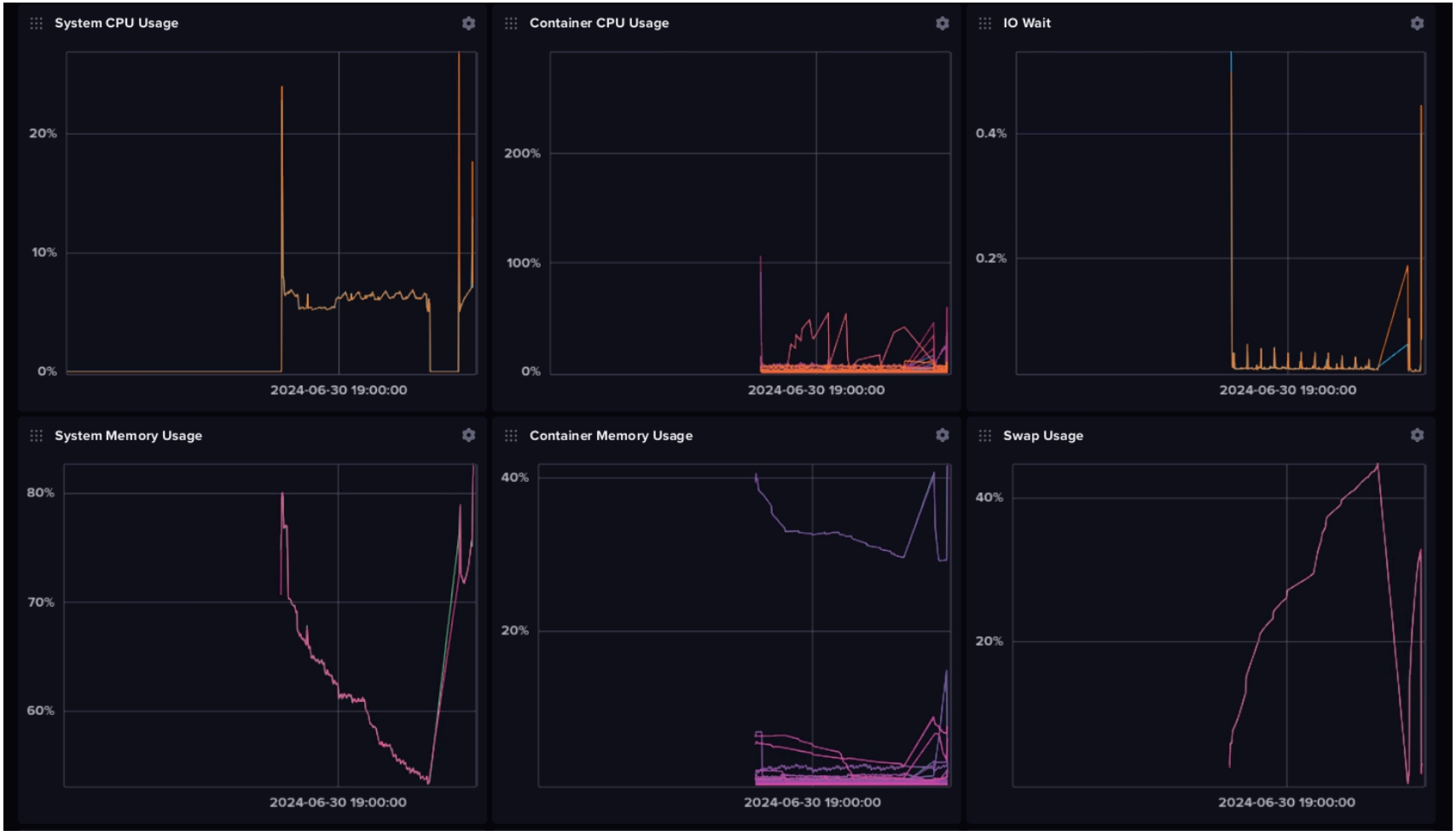
Interfaz de InfluxDB que muestra el rendimiento del nodo de Security Onion (Parte 3).



Nota. En la imagen se muestra el tamaño de InfluxDB, la cola de Redis, la carga media, el tiempo de actividad del sistema, el tiempo de actividad del contenedor y el Logstash EPS del nodo de Security Onion.

Figura 56

Interfaz de InfluxDB que muestra el rendimiento del nodo de Security Onion (Parte 4).



Nota. En la imagen se muestra el uso del CPU del sistema, el uso del CPU del contenedor, la espera de IO, el uso de memoria del sistema, el uso de memoria del contenedor y el uso de Swap del nodo de Security Onion.

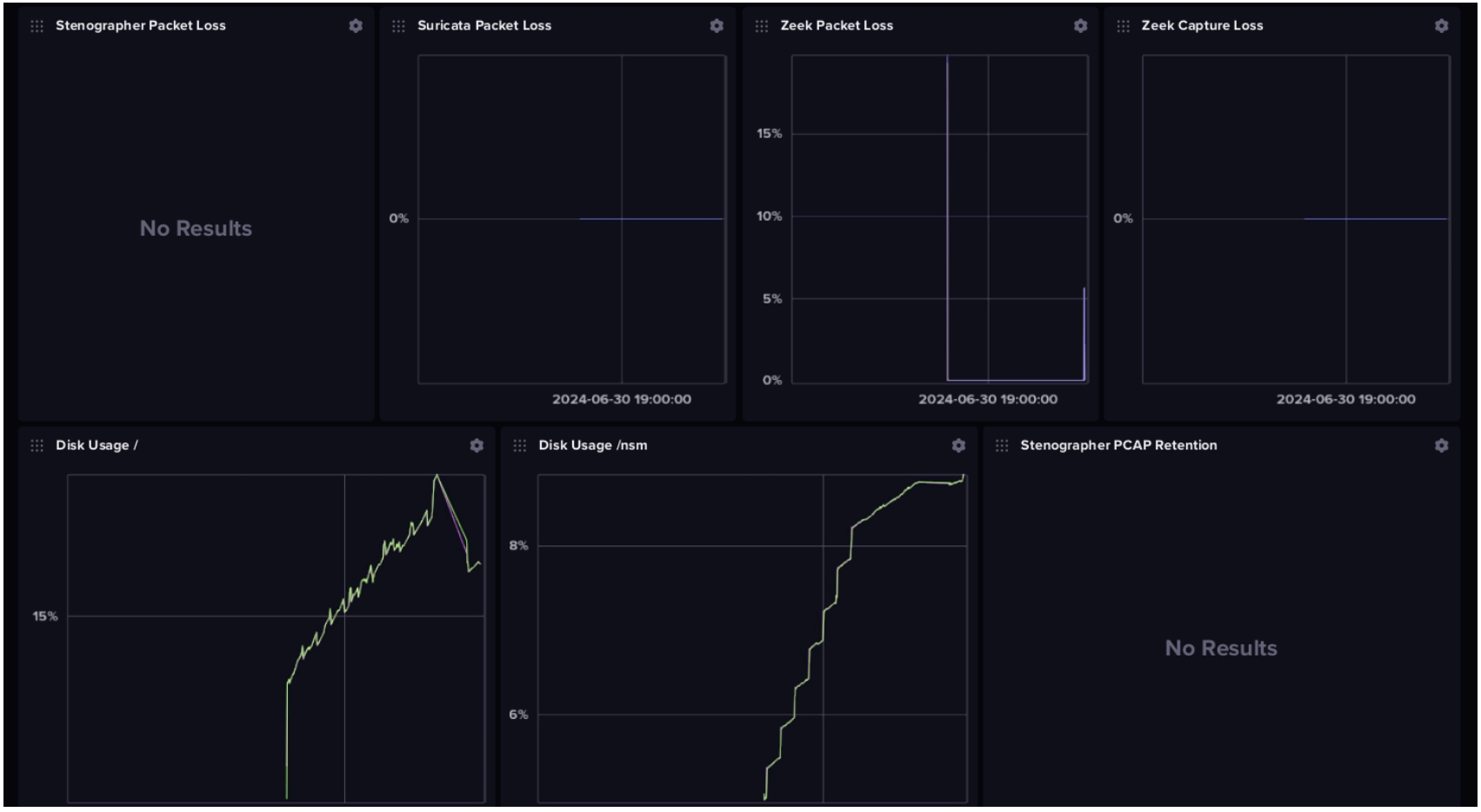
Figura 57

Interfaz de InfluxDB que muestra el rendimiento del nodo de Security Onion (Parte 5).

Nota. En la imagen se muestra el monitoreo de tráfico de interfaz entrante, el tráfico entrante de contenedores, las caídas entrantes de la interfaz, el tráfico entrante de la interfaz de gestión, el tráfico saliente de la interfaz de gestión y el tráfico saliente de la interfaz de gestión del nodo de Security Onion.

Figura 58

Interfaz de InfluxDB que muestra el rendimiento del nodo de Security Onion (Parte 6).

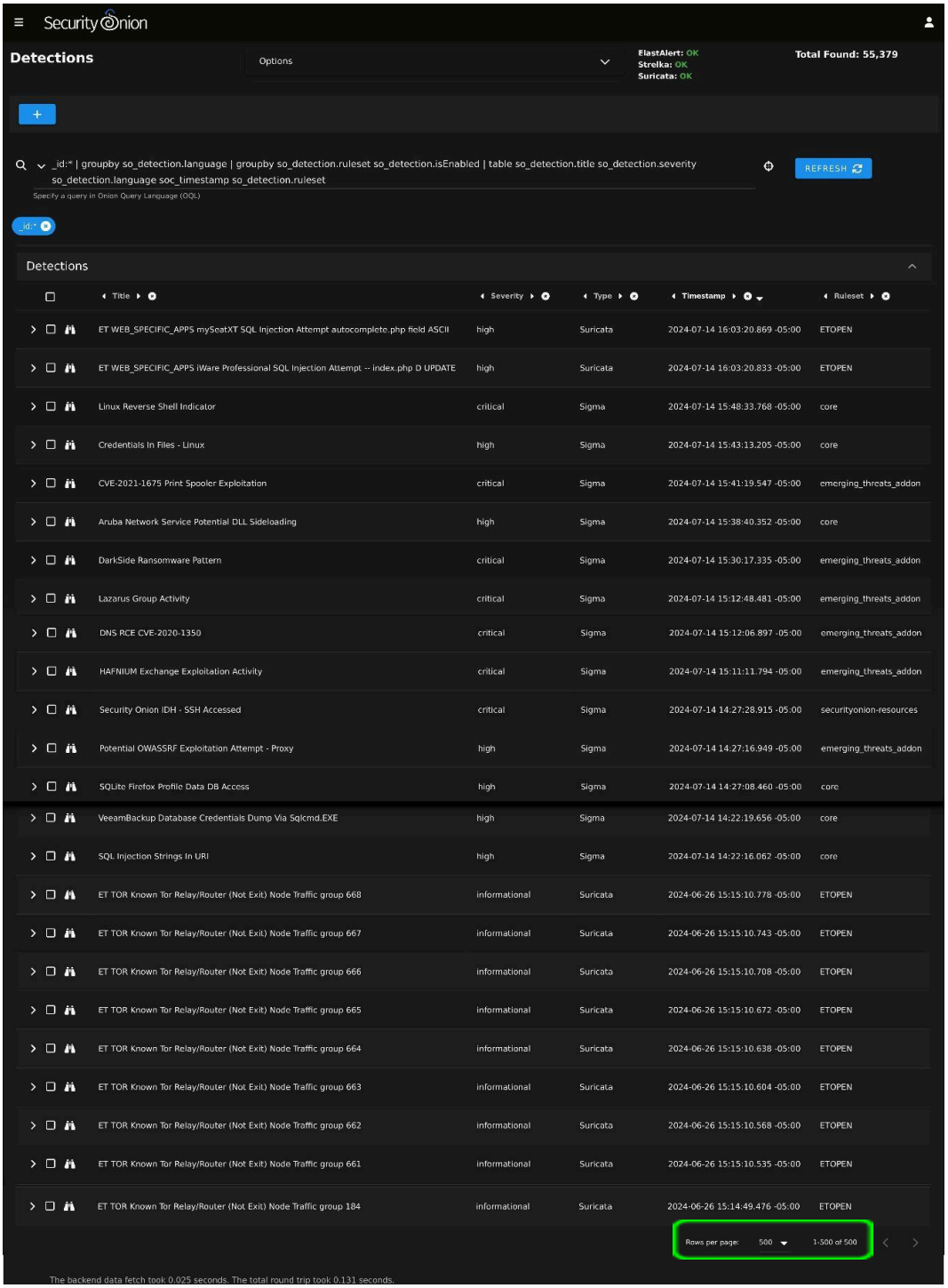


Nota. En la imagen se muestra la pérdida de paquetes detectados por Stenographer, la pérdida de paquetes detectada por Suricata, la pérdida de paquetes detectadas por Zeek, la pérdida de captura de Zeek, los usos de disco y la retención de paquetes por Stenographer del nodo de Security Onion.

ANEXO F: Lista de detecciones registradas por Security Onion

Figura 59

Lista de las detecciones registradas por Security Onion



Nota. En la imagen se omitieron muchas detecciones de tipo informacional debido a que eran, prácticamente, del mismo tipo y conformaban la mayoría de registros.

ANEXO G: Salvaguardas de los controles CIS pertinentes

Tabla 12

Salvaguardas del Control CIS 13: Monitoreo y defensa de la red

13 Monitoreo y Defensa de la red

Operar procesos y herramientas para establecer y mantener la supervisión y defensa integrales de la red contra las amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.

13.1	**Centralizar alertas de eventos de seguridad**	Red	Detectar		●	●
	Centralice las alertas de eventos de seguridad en todos los activos de la empresa para la correlación y el análisis de registros. La implementación de las mejores prácticas requiere el uso de un SIEM, que incluye alertas de correlación de eventos definidas por el proveedor. Una plataforma de análisis de registros configurada con alertas de correlación relevantes para la seguridad también satisface esta protección.					
13.2	**Implemente una solución de detección de intrusiones basada en host**	Dispositivos	Detectar		●	●
	Implementar una solución de detección de intrusiones basada en host en activos empresariales, cuando sea apropiado y/o compatible.					
13.3	**Implementación de una solución de detección de intrusiones en la red**	Red	Detectar		●	●
	Implemente una solución de detección de intrusiones en la red de activos de la empresa, cuando corresponda. Las implementaciones de ejemplo incluyen el uso de un sistema de detección de intrusiones en la red (NIDS) o un servicio equivalente de proveedor de servicios en la nube (CSP).					
13.4	**Realizar filtrado de tráfico entre segmentos de red**	Red	Proteger		●	●
	Realice un filtrado de tráfico entre los segmentos de la red, cuando corresponda.					
13.5	**Gestionar el control de acceso para activos remotos**	Dispositivos	Proteger		●	●
	Administre el control de acceso para los activos que se conectan de forma remota a los recursos de la empresa. Determine la cantidad de acceso a los recursos de la empresa en función de: el software antimalware actualizado instalado, el cumplimiento de la configuración con el proceso de configuración segura de la empresa y la garantía de que el sistema operativo y las aplicaciones estén actualizados.					
13.6	**Recopilar registros de flujo de tráfico de red**	Red	Detectar		●	●
	Recopilar registros de flujo de tráfico de red y/o tráfico de red para revisar y alertar desde dispositivos de red.					
13.7	**Implementar una solución de prevención de intrusiones basada en host**	Dispositivos	Proteger			●
	Implemente una solución de prevención de intrusiones basada en host en los activos de la empresa, cuando corresponda o sea compatible. Las implementaciones de ejemplo incluyen el uso de un cliente de detección y respuesta de extremo (EDR) o un agente IPS basado en host.					
13.8	**Implementar una solución de prevención de intrusiones en la red**	Red	Proteger			●
	Implemente una solución de prevención de intrusiones en la red, en donde corresponda. Entre las implementaciones de ejemplo se incluye el uso de un sistema de prevención de intrusiones en la red (NIPS) o un servicio CSP equivalente.					
13.9	**Implementar el control de acceso a nivel de puerto**	Dispositivos	Proteger			●
	Implementar el control de acceso a nivel de puerto. El control de acceso a nivel de puerto utiliza 802.1x o protocolos de control de acceso a la red similares, como certificados, y puede incorporar autenticación de usuario y/o dispositivo.					
13.10	**Realizar el filtrado en la capa de aplicación**	Red	Proteger			●
	Realizar el filtrado de la capa de aplicación. Entre las implementaciones de ejemplo se incluyen un proxy de filtrado, un firewall de nivel de aplicación o una puerta de enlace.					
13.11	**Ajustar los umbrales de alerta de eventos de seguridad**	Red	Detectar			●
	Ajustar los umbrales de alerta de eventos de seguridad mensualmente o con más frecuencia					

Nota. Adaptado de *Salvaguardas CIS Control 13: Monitoreo y Defensa de la red* (p.35), por Center for Internet Security, 2021.

Tabla 14

Salvaguardas del Control CIS 07: Gestión continua de vulnerabilidades

07 Gestión Continua de Vulnerabilidades

Desarrollar un plan para evaluar y dar seguimiento continuo a las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, con el fin de remediar y reducir la ventana de oportunidad para los atacantes. Monitorear las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades.

7.1	**Establecer y mantener un proceso de gestión de vulnerabilidades**	Aplicaciones	Proteger	●	●	●
	Establezca y mantenga un proceso de gestión de vulnerabilidades documentado para los activos de la empresa. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguardia.					
7.2	**Establecer y mantener un proceso de remediación**	Aplicaciones	Responder	●	●	●
	Establecer y mantener una estrategia de remediación basada en riesgos documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.					
7.3	**Realice una gestión automatizada de parches del sistema operativo**	Aplicaciones	Proteger	●	●	●
	Realice actualizaciones del sistema operativo en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.					
7.4	**Realizar la administración automatizada de parches de aplicaciones**	Aplicaciones	Proteger	●	●	●
	Realice actualizaciones de aplicaciones en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.					
7.5	**Realizar análisis automatizados de vulnerabilidades de activos internos de la empresa**	Aplicaciones	Identificar		●	●
	Realice escaneos automatizados de vulnerabilidades de los activos internos de la empresa de forma trimestral o con mayor frecuencia. Realice escaneos autenticados y no autenticados, utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP.					
7.6	**Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente**	Aplicaciones	Identificar		●	●
	Realice escaneos automatizados de vulnerabilidades de los activos empresariales expuestos externamente utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP. Realice exploraciones mensualmente o con mayor frecuencia.					
7.7	**Remediar las vulnerabilidades detectadas**	Aplicaciones	Responder		●	●
	Repare las vulnerabilidades detectadas en el software a través de procesos y herramientas de forma mensual o más frecuente, según el proceso de corrección.					

Nota. Adaptado de *Salvaguardas CIS Control 07: Gestión Continua de Vulnerabilidades (p.23)*, por Center for Internet Security, 2021.

Tabla 15

Salvaguardas del Control CIS 04: Configuración segura de activos y software empresarial

04 Configuración Segura de Activos y Software Empresarial

Establecer y mantener la configuración segura de los activos empresariales (Dispositivos de usuarios, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (Sistemas operativos y aplicaciones).

4.1	**Establecer y Mantener un Proceso de configuración seguro**	**Aplicaciones**	**Proteger**	●	●	●
	Establecer y mantener un proceso seguro de la configuración para los activos de la empresa (dispositivos de usuarios, incluidos portátiles y móviles; dispositivos no informáticos/IoT; and servers) y software (Sistemas operativos y aplicaciones). Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan causar un impacto a esta salvaguarda.					
4.2	**Establecer y mantener un proceso de configuración seguro para la infraestructura de red**	**Red**	**Proteger**	●	●	●
	Establecer y mantener un proceso de configuración seguro para dispositivos de red. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguardia.					
4.3	**Configurar el bloqueo automático de sesiones en activos empresariales**	**Usuarios**	**Proteger**	●	●	●
	Configurar el bloqueo automático de sesiones en los activos de la empresa después de un período definido de inactividad. Para los sistemas operativos de propósito general, el período no debe exceder los 15 minutos. Para dispositivos móviles de usuario final, el período no debe exceder los 2 minutos.					
4.4	**Implementar y administrar un firewall en servidores**	**Dispositivos**	**Proteger**	●	●	●
	Implemente y administre un firewall en los servidores donde sea compatible. Como ejemplo de implementación se incluyen un firewall virtual, un firewall del sistema operativo o un agente de firewall de terceros.					
4.5	**Implementar y Administrar un Firewall en los dispositivos de usuario**	**Dispositivos**	**Proteger**	●	●	●
	Implementar y administrar un firewall basado en host o una herramienta de filtrado de puertos en los dispositivos del usuario final, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.					
4.6	**Gestione de forma segura los activos y el software de la empresa**	**Red**	**Proteger**	●	●	●
	Gestione de forma segura los activos y el software de la empresa. Por ejemplo las implementaciones incluyen la gestión de la configuración a través de una infraestructura controlada por versiones como código y el acceso a interfaces administrativas a través de protocolos de red seguro, como Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de administración inseguros, como Telnet (Teletype Network) y HTTP, a menos que sea operacionalmente esencial.					
4.7	**Administrar cuentas predeterminadas en activos y software empresariales**	**Usuarios**	**Proteger**	●	●	●
	Administre cuentas predeterminadas en activos y software de la empresa, como root, administrador y otras cuentas de proveedores preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o inutilizarlas.					
4.8	**Desinstalar o deshabilitar servicios innecesarios en activos y software empresariales**	**Dispositivos**	**Proteger**		●	●
	Desinstale o deshabilite los servicios innecesarios en los activos y el software de la empresa, como un servicio de uso compartido de archivos, un módulo de aplicación web o una función de servicio.					
4.9	**Configurar servidores DNS confiables en activos empresariales**	**Dispositivos**	**Proteger**		●	●
	Configurar servidores DNS confiables en activos empresariales. Las implementaciones de ejemplo incluyen: configurar activos para usar servidores DNS controlados por la empresa y/o servidores DNS acreditados externamente.					
4.10	**Aplicar el bloqueo automático de dispositivos en portátiles y dispositivos móviles**	**Dispositivos**	**Responder**		●	●
	Aplicar el bloqueo automático de dispositivos después de un umbral predeterminado de intentos de autenticación fallidos locales en dispositivos portátiles de usuario final, donde sea compatible. En el caso de las computadoras portátiles, no permite más de 20 intentos fallidos de autenticación; para tabletas y teléfonos inteligentes, no más de 10 intentos de autenticación fallidos. Las implementaciones de ejemplo incluyen Microsoft® InTune Device Lock y Apple® Intentos fallidos de mac de perfil de configuración.					
4.11	**Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final**	**Dispositivos**	**Proteger**		●	●
	Borre de forma remota los datos empresariales de los dispositivos portátiles de usuario final de propiedad de la empresa cuando se considere apropiado, como dispositivos perdidos o robados, o cuando una persona deja la empresa.					
4.12	**Espacios de trabajo empresariales independientes en dispositivos móviles de usuario final**	**Dispositivos**	**Proteger**			●
	Asegúrese de que se utilicen espacios de trabajo empresariales independientes en los dispositivos móviles de los usuarios finales, cuando sean compatibles. Las implementaciones de ejemplo incluyen el uso de un perfil de configuración de Apple® o un perfil de trabajo de Android ™ para separar las aplicaciones y los datos empresariales de las aplicaciones y los datos personales.					

Nota. Adaptado de *Salvaguardas CIS Control 04: Configuración Segura de Activos y Software Empresarial (p. 16),* por Center for Internet Security, 2021.

Tabla 16

Salvaguardas del Control CIS 02: Inventario y control de activos de software

02 Inventario y Control de Activos de Software

Gestione activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) dentro de la red. Únicamente el software autorizado debe ser instalado y ejecutado, y aquellos software no autorizados ni gestionados que se encuentren se impida la instalación y/o ejecución.

2.1	**Elaborar y Mantener actualizado el inventario de software**	Aplicaciones	Identificar	●	●	●
	Elabore y mantenga un inventario detallado de todas las licencias de software instalados en los activos de la empresa. El inventario de software debe documentar el título, el fabricante, la fecha de instalación inicial y el propósito para cada activo, cuando corresponda, incluya la dirección URL, las tiendas de aplicaciones, versiones, mecanismo de implementación y fecha de retirada.					
2.2	**Asegurarse de que el software autorizado cuente con soporte**	Aplicaciones	Identificar	●	●	●
	Asegúrese de que únicamente el software con soporte actual del fabricante esté designado como autorizado en el inventario de software de activos empresariales. Si el software ya no se encuentra soportado por el fabricante, pero es necesario para el cumplimiento de la misión de la empresa, documente una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software sin soporte, sin una documentación de excepción, identificarla como no autorizada. Revise la lista de software para comprobar el soporte del software por lo menos una vez al mes o con más frecuencia.					
2.3	**Tratamiento del Software no Autorizado**	Aplicaciones	Responder	●	●	●
	Asegúrese de que el software no autorizado sea removido de los activos de la empresa o ante evidencias de instalaciones no autorizadas el evento cuente con una excepción documentada. Realice este paso mensualmente o con más frecuencia.					
2.4	**Utilice herramientas automatizadas de inventario de software**	Aplicaciones	Detectar		●	●
	Utilizar herramientas de inventario de software, cuando sea posible, en toda la empresa para automatizar la detección y documentación del software instalado.					
2.5	**Use Lista de permitidos Para Software Autorizados**	Aplicaciones	Proteger		●	●
	Utilice controles técnicos, como lista de aplicaciones permitidas, para asegurarse de que solo se pueda ejecutar o acceder al software autorizado. Reevaluar semestralmente o con más frecuencia.					
2.6	**Lista de Librerías Autorizadas**	Aplicaciones	Proteger		●	●
	Utilice controles técnicos para garantizar que solo las bibliotecas de software actual. Bloquee la carga de bibliotecas no autorizadas en los procesos del sistema. Reevalúe semestralmente o con más frecuencia.					
2.7	**Use Lista de permitidos Para secuencias de comandos Autorizados**	Aplicaciones	Proteger			●
	Utilice controles técnicos, como firmas digitales y control de versiones, para asegurarse de que los scripts autorizados, específicos como los .ps1, .py, etc., archivos, estén permitidos para ejecutarse. Bloquear los scripts no autorizados para ejecutarse. Reevalúe semestralmente o con más frecuencia.					

Nota. Adaptado de *Salvaguardas CIS Control 02: Inventario y Control de Activos de Software (p. 10)* por Center for Internet Security, 2021.

Tabla 17

Salvaguardas del Control CIS 03: Protección de los datos

03 Protección de los Datos

Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y eliminar de forma segura los datos.

3.1	**Establecer y mantener un proceso de gestión de datos** Establecer y mantener un proceso de gestión de datos. Durante el proceso, Ubicación de los datos sensibles, propietario de los datos, Tratamiento de los datos, límites de la retención de datos, y requisitos de eliminación, basados en la sensibilidad y estándares de retención para la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que pudieran impactar en esta salvaguardia.	Datos	Identificar	●	●	●
3.2	**Establecer y Mantener un inventario de datos** Establecer y mantener un inventario de datos, basados en el proceso de gestión de datos de la empresa. Inventario de datos sensibles, como mínimo. Revise y actualice el inventario anualmente, como mínimo, con prioridad sobre los datos sensibles.	Datos	Identificar	●	●	●
3.3	**Configure listas de control de acceso a datos** Configurar listas de control de acceso a datos en función de la necesidad de conocimiento de un usuario. Aplicar listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos, bases de datos y aplicaciones locales y remotas.	Datos	Proteger	●	●	●
3.4	**Aplicar retención de datos** Retener los datos de acuerdo con el proceso de gestión de datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.	Datos	Proteger	●	●	●
3.5	**Eliminar de forma segura los datos** Elimine de forma segura como se describe en el proceso de gestión de datos empresariales. Asegúrese de que el proceso y el método de eliminación sean acordes con la confidencialidad de los datos.	Datos	Proteger	●	●	●
3.6	**Cifrar datos en dispositivos de usuarios** Encriptar los datos en los dispositivos de los usuarios que contienen datos sensibles. Un ejemplo de implementación puede incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivos	Proteger	●	●	●
3.7	**Establecer y mantener un esquema de clasificación de datos** Establecer y mantener un esquema general de clasificación de datos para la empresa. En las empresas pueden usar etiquetas, como "sensible," "Confidencial," y "Público," y clasificar sus datos de acuerdo a esas etiquetas. Revise y actualice el esquema de clasificación anualmente, o cuando suceda algún cambio significativo en la empresa que pueda tener impacto sobre esta Salvaguardia.	Datos	Identificar		●	●
3.8	**Documentar el Flujo de datos** Documente el flujo de datos. La documentación del flujo de datos incluye los flujos de datos del proveedor de servicios y debe basarse en el proceso de gestión de datos de la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan impactar esta Salvaguarda.	Datos	Identificar		●	●
3.9	**Cifrar datos en medios extraíbles** Cifre los datos en los dispositivos extraíbles.	Datos	Proteger		●	●
3.10	**Cifre los datos confidenciales en tránsito** Cifre los datos confidenciales en tránsito. Ejemplos de implementación incluyen: Transport Layer Security (TLS) y Open Secure Shell (OpenSSH).	Datos	Proteger		●	●
3.11	**Cifrar los datos confidenciales en reposo** Cifre los datos confidenciales que se encuentran en reposo en servidores, aplicaciones y bases de datos que contengan datos confidenciales. El cifrado de la capa de almacenamiento, también conocido como cifrado del lado del servidor, cumple con el requisito mínimo de esta Salvaguardia. Métodos de cifrado adicionales pueden incluir el cifrado del lado del cliente, también conocido como cifrado del lado del cliente, donde el acceso a los dispositivos de almacenamiento de datos no permite el acceso a los datos de texto sin formato.	Datos	Proteger		●	●
3.12	**Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad** Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad. No procesar datos confidenciales en activos empresariales destinados a datos de menor sensibilidad.	Red	Proteger		●	●
3.13	**Desplegar una solución de Prevención de Pérdida de Datos** Implemente una herramienta automatizada, como una herramienta de prevención de pérdida de datos (DLP) basada en host para identificar todos los datos confidenciales almacenados, procesados, transmitidos a través de los activos de la empresa, incluidos lo que se encuentran en el sitio o en un proveedor de servicios remoto, y actualizar el inventario de datos confidenciales de la empresa.	Datos	Proteger			●
3.14	**Registre de acceso a datos confidenciales** Registre el acceso a los datos, incluidos modificación y eliminación.	Datos	Detectar			●

Nota. Adaptado de *Salvaguardas CIS Control 03: Protección de los Datos (p. 12),* por Center for Internet Security, 2021.

Tabla 18

Salvaguardas del Control CIS 06: Gestión de control de acceso

06 Gestión de Control de Accesos

Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos empresariales y software.

6.1	**Establecer un proceso para conceder accesos** Establecer y seguir un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de un usuario.	Usuarios	Proteger	●	●	●
6.2	**Establecer un proceso de revocación de acceso** Establecer y seguir un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación, revocación de derechos o cambio de rol de un usuario. Es posible que sea necesario deshabilitar cuentas, en lugar de eliminarlas, para conservar las pistas de auditoría.	Usuarios	Proteger	●	●	●
6.3	**Exigir MFA para aplicaciones expuestas externamente** Exija que todas las aplicaciones empresariales o de terceros expuestas externamente apliquen MFA, donde sea compatible. Hacer cumplir MFA a través de un servicio de directorio o un proveedor de SSO es una implementación satisfactoria de esta salvaguarda.	Usuarios	Proteger	●	●	●
6.4	**Exigir MFA para el acceso remoto a la red** Exigir MFA para el acceso remoto a la red.	Usuarios	Proteger	●	●	●
6.5	**Exigir MFA para el acceso administrativo** Requerir MFA para todas las cuentas de acceso administrativo, donde sea compatible, en todos los activos de la empresa, ya sea administrado en el sitio o a través de un proveedor externo.	Usuarios	Proteger	●	●	●
6.6	**Establecer y mantener un inventario de sistemas de autenticación y autorización** Establecer y mantener un inventario de los sistemas de autenticación y autorización de la empresa, incluidos los alojados en el sitio o en un proveedor de servicios remoto. Revisar y actualizar el inventario, como mínimo, anualmente o con mayor frecuencia.	Usuarios	Identificar		●	●
6.7	**Control de Acceso Centralizado** Centralice el control de acceso para todos los activos de la empresa a través de un servicio de directorio o un proveedor de SSO, donde sea compatible.	Usuarios	Proteger		●	●
6.8	**Definir y mantener el control de acceso basado en roles** Definir y mantener el control de acceso basado en roles, a través de la determinación y documentación de los derechos de acceso necesarios para que cada rol dentro de la empresa lleve a cabo con éxito las tareas asignadas. Realice revisiones de control de acceso de los activos de la empresa para validar que todos los privilegios estén autorizados, de forma periódica, como mínimo una vez al año, o con mayor frecuencia.	Datos	Proteger			●

Nota. Adaptado de *Salvaguardas CIS Control 06: Gestión de Control de Accesos (p. 20)* por Center for Internet Security, 2021.

Tabla 19

Salvaguardas del Control CIS 10: Defensas contra malware

10 Defensas contra Malware

Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en activos empresariales.

10.1	**Implementar y mantener software anti-malware** Implementar y mantener software antimalware en todos los activos de la empresa.	Dispositivos	Proteger	●	●	●
10.2	**Configurar actualizaciones automáticas de firmas de Antimalwares** Configurar actualizaciones automáticas para archivos de firma antimalware en todos los activos de la empresa.	Dispositivos	Proteger	●	●	●
10.3	**Deshabilitar la ejecución automática y la reproducción automática para medios extraíbles** Desactive la ejecución automática y la función de ejecución automática de reproducción automática para medios extraíbles.	Dispositivos	Proteger	●	●	●
10.4	**Configurar el análisis anti malware automático de medios extraíbles** Configure el software anti-malware para escanear automáticamente los medios extraíbles.	Dispositivos	Detectar		●	●
10.5	**Habilitar funciones anti-explotación** Habilite funciones anti-explotación en activos y software empresariales, cuando sea posible, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) o Apple® System Integrity Protection (SIP) y Gatekeeper ™.	Dispositivos	Proteger		●	●
10.6	**Administrar de forma centralizada el software antimalware** Gestione de forma centralizada el software antimalware.	Dispositivos	Proteger		●	●
10.7	**Utilice el software anti-malware basado en el comportamiento** Usar software anti malware basado en el comportamiento.	Dispositivos	Detectar		●	●

Nota. Adaptado de *Salvaguardas CIS Control 10: Defensas contra Malware (p. 29)*, por Center for Internet Security, 2021.

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ACTA DE SUSTENTACION DE TESIS N° 085-2024-FIMGC

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE SISTEMAS

En la Universidad Nacional de San Cristóbal de Huamanga de la ciudad de Ayacucho, en cumplimiento a la **Resolución Decanal N° 725-2024-FIMGC-D,** a los dieciocho días del mes de noviembre de 2024, siendo las 05:00 p,m., reunidos en el Auditorio de la Escuela Profesional de Ingeniería de Minas, bajo la presidencia del MSc. Ing. ESTRADA CARDENAS, José Ernesto y los miembros; Mg. Ing. Eloy VILA HUAMAN y Mg. Ing. Hubner JANAMPA PATILLA, actuando como secretario docente el MSc. Ing. Kelvis BERROCAL ARGUMEDO, para proceder a la sustentación de tesis para optar el Título Profesional de Ingeniera de Sistemas, de la bachiller:

Kimberlly Nena BARRAZA TUDELA

Quien presentó la tesis denominada:

Security Onion como herramienta de auditoría de redes en la Universidad Nacional de San Cristóbal de Huamanga, 2023

Los señores miembros del jurado luego de expuesto la tesis y absueltas las preguntas, deliberan y lo declaran:

APROBADO CON NOTA DIECISIETE

Siendo las 06:20 p.m. del día 18 de noviembre de 2024, culmina el acto de sustentación de tesis, y en conformidad a lo actuado los miembros del jurado firmamos al pie del presente.

MSc. Ing. ESTRADA CÁRDENAS, José Ernesto
Presidenta

Mg. Ing. Eloy VILA HUAMAN
Miembro

Mg. Ing. Hubner JANAMPA PATILLA
Miembro - Asesor

MSc. Ing. Kelvis BERROCAL ARGUMEDO
Secretario docente de la FIMGC

cc:
Archivo

FACULTAD DE INGENIERÍA
DE MINAS, GEOLOGÍA Y CIVIL
Av. Independencia S/N
Ciudad Universitaria
Central Tel 066 312510
Anexo 151

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA Nº 013-2024-KPS-FIMGC/UNSCH

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado con el software Turnitin, en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la **Resolución de Consejo Universitario Nº 039-2021-UNSCH-CU**, Reglamento de Originalidad de Trabajos de Investigación de la Universidad Nacional San Cristóbal de Huamanga y **Resolución Decanal Nº 473-2023-FIMGC-D**, deja constancia de originalidad de trabajo de investigación, que el/la Sr./Srta.

Nombres y Apellidos	:	Kimberlly Nena Barraza Tudela
Escuela Profesional	:	INGENIERÍA DE SISTEMAS
Título de la Tesis	:	Security Onion como herramienta de Auditoría de Redes en la Universidad Nacional de San Cristóbal de Huamanga, 2023.
Evaluación de la Originalidad	:	**8%** Índice de Similitud
Identificador de la entrega	:	2549473500

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

En señal de conformidad y verificación se firma la presente constancia

Ayacucho, 11 de diciembre de 2024

FIRMA DIGITAL

Firmado digitalmente por: PERALTA SOTOMAYOR Karel FAU 20143660754 soft
Motivo: Soy el autor del documento
Fecha: 10/04/2025 12:40:04-0500

Con depósito para Sustentación y Tramites
C.c. Archivo

FACULTAD DE INGENIERIA DE MINAS, GEOLOGIA Y CIVIL
Av. Independencia S/N Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

Security Onion como herramienta de Auditoría de Redes en la Universidad Nacional de San Cristóbal de Huamanga, 2023.

por Kimberlly Nena Barraza Tudela

Fecha de entrega: 11-dic-2024 04:43p.m. (UTC-0500)

Identificador de la entrega: 2549473500

Nombre del archivo:
Security_Onion_como_herramienta_de_Auditoría_de_Redes_en_la_Universidad_Nacional_de_San_Cristóbal_de_Huamanga_2023.pdf (20.6M)

Total de palabras: 22798

Total de caracteres: 130472

Security Onion como herramienta de Auditoría de Redes en la Universidad Nacional de San Cristóbal de Huamanga, 2023.

INFORME DE ORIGINALIDAD

8%	8%	1%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	diplomadociberseguridad.com Fuente de Internet	3%
2	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	2%
3	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	1%
4	openaccess.uoc.edu Fuente de Internet	1%
5	Submitted to Grupo IOE Trabajo del estudiante	<1%
6	repositorio.unsch.edu.pe Fuente de Internet	<1%
7	Submitted to Universidad Europea de Madrid Trabajo del estudiante	<1%
8	www.ibm.com Fuente de Internet	<1%

9	readthedocs.org Fuente de Internet	<1 %
10	Submitted to Champlain College Trabajo del estudiante	<1 %
11	www.gandhi.com.mx Fuente de Internet	<1 %
12	repositorio.ucm.edu.co Fuente de Internet	<1 %
13	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		