DOI: https://doi.org/10.46296/yc.v7i12edespjun.0333

SISTEMAS DE MONITOREO ACTIVO PARA EVITAR ATAQUES A SERVICIOS DE RED EN EL HOSPITAL DR. NAPOLEÓN DÁVILA CÓRDOVA

ACTIVE MONITORING SYSTEMS TO PREVENT ATTACKS TO NETWORK SERVICES AT DR. NAPOLEÓN DÁVILA CÓRDOVA HOSPITAL

Cedeño Ignacio [1]; Cedeño-Valarezo Luis [2]

[1] Maestría en Cyberseguridad, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. Calceta, Ecuador. Correo: ignacioka1810@gmail.com. ORCID ID: https://orcid.org/0000-0001-7562-0499

[2] Maestría en Cyberseguridad, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. Calceta, Ecuador. Correo: lcedeno@espam.edu.ec. ORCID ID: https://orcid.org/0000-0002-2403-9781

Resumen

Los Sistemas de monitoreo activo son la nueva tendencia en relación con la ciberseguridad, que están siendo utilizadas por las entidades privadas y públicas con la finalidad de brindar un servicio que bloquea ataques en red y optimiza las labores de registro de información. El objetivo de esta investigación es analizar la aplicación de un sistema de monitoreo activo que permita evitar ataques en el servicio de red en el Hospital Napoleón Dávila Córdova. La metodología consistió en el análisis bibliográfico de varios artículos científicos en los que se plantean las ventajas de contar con este tipo de tecnología, se diseñó el cuestionario para la entrevista al jefe del área de TIC del Hospital, para seguidamente realizar la entrevista en base al cuestionario, luego se realizó el análisis de los resultados de la entrevista. Se buscó y evaluó las posibles herramientas de monitoreo activo que se puedan aplicar. Las herramientas de seguridad aptas para la aplicación en el sistema de red dado que se conocen las características de los equipos activos, han sido Snort y Suricata, las mismas que pueden funcionar en conjunto sin ningún problema para poder detectar intrusos y anomalías en la red.

Palabras claves: Snort, Suricata, ataques en red.

Abstract

Active monitoring systems are the new trend in relation to cybersecurity, which are being used by private and public entities in order to provide a service that blocks network attacks and optimizes the work of recording information. The objective of this research is to analyze the application of an active monitoring system to prevent attacks on the network service at the Napoleón Dávila Córdova Hospital. The methodology consisted of the bibliographic analysis of several scientific articles in which the advantages of having this type of technology are presented, the questionnaire was designed for the interview with the head of the ICT area of the Hospital, and then the interview was conducted based on the questionnaire, then the analysis of the results of the interview was performed. The possible active monitoring tools that could be applied were searched for and evaluated. The security tools suitable for application in the network system, given that the characteristics of the active equipment are known, were Snort and Suricata, which can work together without any problem to detect intrusions and anomalies in the network.

Keywords: Snort, suricata, network attacks.

Información del manuscrito:
Fecha de recepción: 09 de marzo de 2023.
Fecha de aceptación: 30 de mayo de 2023.
Fecha de publicación: 01 de junio de 2023.

1. Introducción

Las tecnologías informáticas, desde su aparición, ha ido incursionando y ganando terreno en las distintas áreas del conocimiento, como la economía, salud, educación, entre otras, llegando a ser muy útiles para los seres humanos debido a la gama de herramientas que ofrecen y que facilitan cada vez más las labores que antes costaba mucho trabajo realizar.

En relación con el área de la Salud, los hospitales contemplan un área específica para el registro de información de distinta índole, entre ellas, llevar un control del personal médico, agentes de enfermería, personal administrativo, y por supuesto, de los pacientes, tratamientos o medicinas. El problema radica en que esta información, archivada por lo general en carpetas, queda expuesta a daños como el tiempo, la humedad, los desastres naturales, entre otros; por lo que se busca poder transformar estos procesos haciendo uso de sistemas más eficientes, innovadores y prácticos.

En ese sentido, a nivel mundial se ha contemplado la optimización de fuentes de registros seguras, pero se ha podido observar que no existe aseguramiento para el manejo reservado de información, aun cuando existen datos importantes de los pacientes como correos electrónicos, datos personales o recetas médicas. Los hackeos informáticos día a día son más comunes, ya que existen organizaciones que no han podido hacer que sus sistemas sean seguros, inclusive instituciones u organizaciones de gran tamaño han sido víctimas de hackeos.

Según (Cristhian, 2021) América Latina sufre constantemente los problemas de ciberseguridad en aplicaciones como el correo electrónico, las redes sociales, entre otros; además, se evidencian en estudios recientes que los ataques informáticos se suelen realizar a empresas que tienen incluso poco tiempo de apertura.

Los sistemas de monitoreo, actualmente se han convertido en una necesidad para las instituciones de salud preocupadas por brindar un servicio de calidad a los usuarios, esto representa un desafío aun mayor para las instituciones hospitalarias del sector público que

funcionan en base a los aportes recibidos por el Estado. Siendo estos sistemas de monitoreo, un recurso innovador utilizado para la optimización de los servicios que brindan las casas de salud, es menester mencionar a Rodríguez (2017) quien en su estudio nos comparte que la aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) en la medicina ha marcado un cambio de paradigma, tal como ocurre en otros campos sociales como educación, agricultura, entre otros.

Rodríguez (2017) para dar una explicación detallada acerca del empleo de las nuevas tecnologías de la información en la atención médica, menciona varias funcionalidades, entre ellas: “la atención a los pacientes, apoyar los diagnósticos, facilitar el control de los procesos administrativos y garantizar la calidad de los servicios de salud”. Sumado a esto, Coventry (2020) nos dice que estos sistemas de monitoreo contribuyen a elevar la eficiencia y la reducción de errores en el tratamiento de enfermedades crónicas en las que no existe necesidad de aplicar procedimientos invasivos. En este ámbito, las redes de datos constituyen medios de comunicación fundamentales para la integración y el intercambio de información entre los diferentes equipos médicos (Ioana, 2017).

Estos sistemas pueden resultar vulnerables al momento de compartir información con otros usuarios, por lo que se debe prever un sistema de monitoreo que ayude a evitar los riesgos de ciberataques, y de esta forma evitar una salida no autorizada de medicamentos, cambios de tratamientos entre pacientes considerados de mayor riesgo, además, el aseguramiento de la confiabilidad de la información compartida entre el médico y el paciente.

Estas situaciones de vulnerabilidad para los sistemas de salud representan un objetivo atractivo para los ciberdelincuentes porque son una fuente de información valiosa deficientemente protegida. Esta información puede ser explotada mediante el robo, la suplantación de identidad y el fraude con el fin de adquirir sustancias médicas controladas. Según Barad (2019), las intrusiones en redes digitales y las afectaciones en el acceso a sistemas e informaciones

de entidades sanitarias constituyen amenazas que producen graves problemas de seguridad e impactan negativamente en el tratamiento de los pacientes.

Los ciberataques en el sector de la salud se han incrementado en un 125% durante los últimos cinco años. Estas transgresiones ocupan la octava posición de los fenómenos con mayor impacto a nivel mundial durante 2020. Su repercusión económica en organizaciones de atención médica es significativamente mayor a las pérdidas que ocasionan en organizaciones de otros sectores (Bhuyan, 2020).

La informatización del Sistema Nacional de Salud se enmarca en el proceso de “informatización de la sociedad cubana”, iniciado en 1996; retomado en la actualidad dado los cambios y transformaciones que se están produciendo en el contexto nacional e internacional. Responde a la política y estrategias definidas como un proceso prioritario del sector, siendo la atención médica a los ciudadanos el eje fundamental y centro de este. (Rodríguez, 2017)

Los Sistemas de Detección de Intrusiones (IDS, por sus siglas en inglés) constituyen una de las herramientas más utilizadas para garantizar la seguridad de las redes de datos porque detectan actividades sospechosas mediante el análisis y monitoreo del tráfico de paquetes de red. Estas herramientas permiten detectar ataques y violaciones de seguridad, implementar diferentes controles de supervisión, prevenir problemas de comportamiento y abusos en los sistemas interconectados a la red. (Perdigón & Orellana, 2021).

Los IDS pueden emplearse para proteger una red o un equipo en particular y en correspondencia al enfoque que utilicen pueden detectar comportamientos anómalos o ataques específicos (Castellanos, 2020). Debido a la complejidad de los IDS y su aplicación en las arquitecturas de seguridad, es necesario realizar una evaluación objetiva de estas herramientas, con el propósito de seleccionar adecuadamente la solución que mejor se ajuste a los requerimientos de las organizaciones (Wang X, 2020). Existe una carencia de investigaciones donde se desarrolle

un análisis crítico de las tendencias actuales de estas herramientas para contribuir a facilitar su selección e implementación (Maniriho, 2020)

El presente artículo denominado sistemas de monitoreo activo para mejorar la eficiencia del registro de la información de hospital Dr. Napoleón Dávila, tuvo como antecedente la ineficiente y obsoleta forma de registrar, organizar y archivar la información referida a los pacientes que allí se atendían, sumado a esto, el terremoto del 2016 afectó fuertemente las instalaciones del hospital ocasionando la pérdida de la información registrada. Una vez reconstruido el hospital, se optó por el manejo sistemático de la información, pero, al momento, este registro no cuenta con programas de seguridad para detectar accesos extraños o inusuales que expidan una alerta para evitar los ataques o accesos de intrusos y puedan obtener información no permitida, al actualizar los programas de registro y anexar un sistema de monitoreo, permite agilitar la atención y brindar un servicio eficaz a la ciudadanía, lo que conlleva a la realización del presente trabajo de investigación que contó con dos etapas primordiales: una dirigida a la comprensión del problema y otra, dirigida a la propuesta de un sistema de monitoreo activo como estrategia de intervención que asegure el buen uso de la información y evite los problemas de suplantación de identidad, acceso a medicinas de alto riesgo, entre otros.

Siendo los sistemas de salud un objetivo atractivo para los ciberdelincuentes, debido a que son una fuente de información valiosa cuando están deficientemente protegidas y que pueden ser explotadas mediante el robo, la suplantación de identidad o el fraude con el fin de adquirir sustancias médicas controladas.

El objetivo de esta investigación es plantear la aplicación de un sistema de monitoreo activo para evitar las intrusiones en redes digitales y las afectaciones en el acceso a sistemas e informaciones en el hospital Dr. Napoleón Dávila Córdova de la ciudad de Chone.

2. Metodología

En esta investigación se siguieron los siguientes pasos:

Revisión bibliográfica

En esta etapa se realizó la búsqueda de investigaciones que se aproximan a los intereses del presente trabajo investigativo, en estas investigaciones se identificaron los conceptos principales relacionados a la temática, como son: Sistemas, Tecnologías de la información y Comunicación (TIC), Monitoreo, entre otras.

Los Modelos de sistemas de protección que han sido utilizados por otras instituciones de salud y que les han permitido brindar a la comunidad un servicio confiable para el manejo de información de los pacientes, diagnósticos y tratamientos, así como también, para llevar el control adecuado de medicinas.

Las fuentes bibliográficas consultadas se obtuvieron de buscadores de información confiables y verídicas para la realización de todo tipo de trabajo de carácter investigativo como Google Scholar, Scielo, IEEE Xplore. Se seleccionaron los temas que incluían sistemas de monitoreo con uso de la tecnología y la relación con las organizaciones.

Además se consideró que los trabajos investigativos hayan sido realizados en los últimos 5 años ya que de allí, se inició la etapa de análisis y tratamiento de la información que sirvió de base para el siguiente trabajo, facilitando verificar el estado de seguridad de la red del hospital y para ello, se aplicó como método científico el analítico-sintético, con los cuales se logró plasmar conclusiones que sustentan la importancia de contar con sistemas de monitoreo y se propuso recomendaciones sobre el tema propuesto. Cabe destacar que el presente trabajo contempla el análisis de artículos investigativos publicados en revistas científicas.

Diseño de cuestionario

Se diseño un cuestionario sobre la seguridad de la red del Hospital Napoleón Dávila Córdova para saber obtener información de las preguntas que se realizara al encargado del área de TIC del hospital Napoleón Dávila Córdova. En cual fueron las siguientes.

- ¿El hospital ha sufrido ataques de redes?
- ¿La red del hospital cuenta con una herramienta de sistema de

monitoreo que permita evitar ataques de red?

- ¿Cómo está diseñada la estructura de red, en su data center como en todos los departamentos?
- ¿Conoce los sistemas de monitoreo que existen actualmente?
- ¿Conoce cuáles son las ventajas de contar con un sistema de monitoreo de red en el Hospital?

Entrevista

Se realizo la entrevista al jefe del área de TIC el día 14 de marzo del 2023 en la oficina de esta la cual se le realizo las preguntas que se diseñó pudiendo conocer como esta diseñada la infraestructura de red del hospital, y nos brindó las marcas de los equipos con sus características y a la vez cuáles son sus funciones que dan al Hospital Napoleón Dávila Córdova, adicional nos informó que no cuentan con un sistema de monitoreo que permita evitar ataques.

Análisis de resultado

Una vez recogida la información de la entrevista, se realizó un análisis para poder tener los resultados de las preguntas que se realizó al jefe del área de TIC del Hospital Napoleón Dávila Córdova.

Evaluación de soluciones

Teniendo en cuenta de los resultados obtenido una vez analizados, se pudo investigar y analizar cuales herramientas de monitoreo activo pueden aplicarse y así poder determinar cuál o cuáles son las más recomendables a la realidad el cual se encuentra el Hospital General Napoleón Dávila Córdova teniendo en cuanta las características de los equipos instalados.

3. Resultados y discusión

En la tabla 1 como resultado de la investigación bibliográfica se pudo encontrar en los artículos seleccionados características muy importante sobre el uso de esta herramienta, como administrar, las vulnerabilidades que existen y las afectaciones que pueden pasar.

Tabla 1. *Características sobre herramientas para un sistema de monitoreo*

N°	Revista	Título	Autor/es	Año	Característica de artículo
1	Scielo	Sistemas para la detección de intrusiones en redes de datos de instituciones de salud	Rudibel Perdigón Llanes, Arturo Orellana García	2021	Sistemas para la detección de intrusiones en redes de datos
2	DSpace	Evaluación de las funcionalidades de los sistemas de detección de intrusos basados en la red de plataformas Open Source utilizando la técnica de detección de anomalías	Arteaga Pucha, José Eduardo	2018	Sistema de detección de intrusos (IDS), suricata (herramienta)
3	Rodin	Despliegue y explotación de herramientas Open Source para la monitorización y gestión de eventos en un entorno virtualizado	Caro Moreno, Raúl	2020	Monitorizar la seguridad del entorno y administrar los datos procedentes de los equipos de la red mediante soluciones de software libre
4	Serie Científica	Análisis y caracterización de conjuntos de datos para detección de intrusiones	Olia Castellanos Leyva, Milton García Borroto	2020	Modelos propuestos para detectar anomalías en el tráfico de red
5	DSpace	Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad	Cristhian Oswaldo Sánchez Guzmán	2021	Las vulnerabilidades, riesgos y amenazas que existen en la red
6	MDPI Journal	A Comparative Experimental Design and Performance Analysis of Snort-Based Intrusion Detection System in Practical Computer Networks	Imdadul Karim, Quoc-Tuan Vien , Tuan Anh Le	2017	network intrusion detection system (NIDS)
7	Infodir	Desarrollo de la Informatización en Hospitales	Lfredo Rodríguez Díaz, María Josefina Vidal Ledo, Armando Cuellar Rojas, Bárbara Daismely Martínez González, Yoan Manuel Cabrera Arribas	2020	Informática en Salud
8	Uvidia	Evaluación De Herramientas De Generación De Tráfico Malicioso Aplicadas A Una Red IP Virtualizada	Luis Alberto Uvidia Armijo	2017	Seguridad informática y herramientas generadoras de tráfico
9	Research Gate Logo	Un nuevo conjunto de datos para la evaluación de IDS de red	Maciá-Fernández, Gabriel Camacho, José Magán-Carrión, Roberto Fuentes-García, Marta García-Teodoro, Pedro Theron, Roberto	2018	Sistemas de detección de intrusiones
10	Research gate	Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System	Syed Ali Raza Shah, Biju Issac	2018	Snort y Suricata, para detectar con precisión el tráfico malicioso en las redes informáticas

En la tabla 2 una vez que se efectuó los análisis de 10 artículos científicos como sus criterios sobre las herramientas de seguridad que existen se obtuvo la siguiente tabla.

Tabla 2. *Análisis de las herramientas de seguridad*

IDS	Autores
Snort	(Arteaga, 2020; Murphy, 2020) (Ashok D, 2020) (Raza, 2020) (Karim I, 2017) (Caro, 2020)
Suricata	(Castellanos O, 2020), (Murphy, 2020), (Arteaga, 2020) (Ashok D, 2020) (Raza, 2020) (Uvidia, 2020) (Caro, 2020)
Zeek (antiguamente Bro)	(Macia-Fernández G, 2017), (Ashok D, 2020), (Uvidia, 2020). (Caro, 2020)
Ourmon	(Zambrano, 2019)
Samhain	(Zambrano, 2019)
Ossec	(Uvidia, 2020) (Caro, 2020)
Tripwire	(Caro, 2020)

Una vez que se diseñó el cuestionario, se aplicó la misma y se hizo el análisis de los datos recopilados. El encargado del área de TIC del Hospital Napoleón Dávila Córdova nos proporcionó el documento donde consta como es el diseño de la red del hospital con las características de los equipos.

De acuerdo con la información presentada se genera el siguiente diagrama de red de la solución implementada para el Hospital General Napoleón Dávila Córdova ubicados en la cuidad de CHONE

En la tabla 3 tenemos el resultado de la encuesta q se aplicó al jefe del área de TIC.

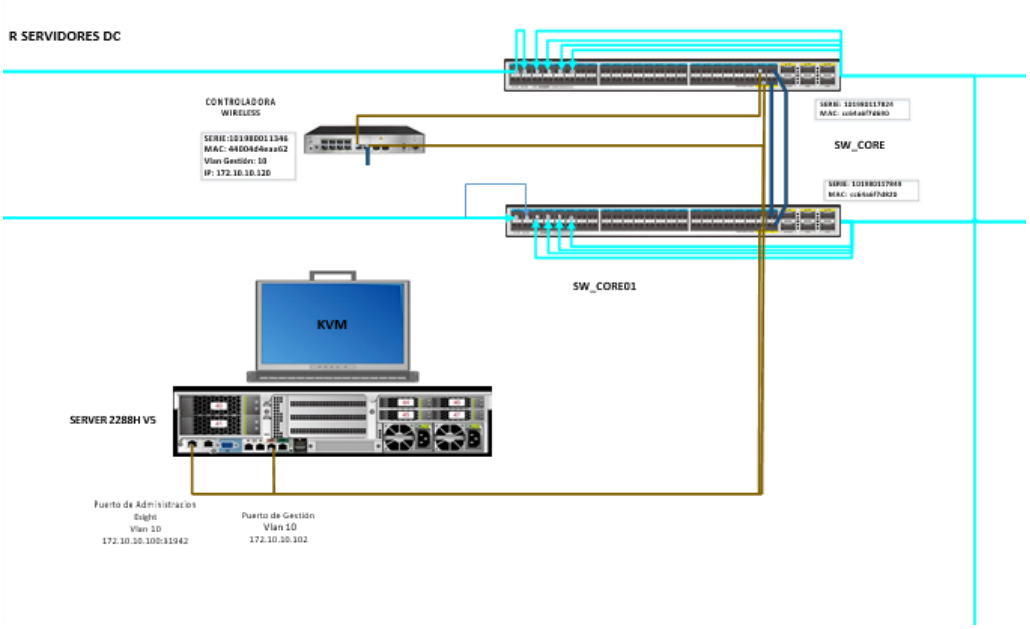
Tabla 3. *Preguntas que se le hizo al jefe del area de TIC*

Preguntas	Respuestas
1. ¿El hospital ha sufrido ataques de redes?	No, el hospital no ha tenido ataques
2. ¿La red del hospital cuenta con una herramienta de sistema de monitoreo que permita evitar ataques de red?	No, el hospital solo cuenta con la herramienta firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red
3. ¿Cómo está diseñada la estructura de red, en su data center como en todos los departamentos?	Se nos proporciono el archivo detallado de la estructura de red
4. ¿Conoce los sistemas de monitoreo que existen actualmente?	Si se conocen en la actualidad
5. ¿Conoce cuáles son las ventajas de contar con un sistema de monitoreo de red en el Hospital?	Si, porque estos nos permitiría tener un monitoreo real de los posibles ataques de red

En las siguientes figuras se presenta la documentación que se nos proporcionó el jefe del area de TIC que contiene el diseño de la infraestructura de red, sus detalles y cómo son sus conexiones como sus características de los equipos que están en funcionamiento.

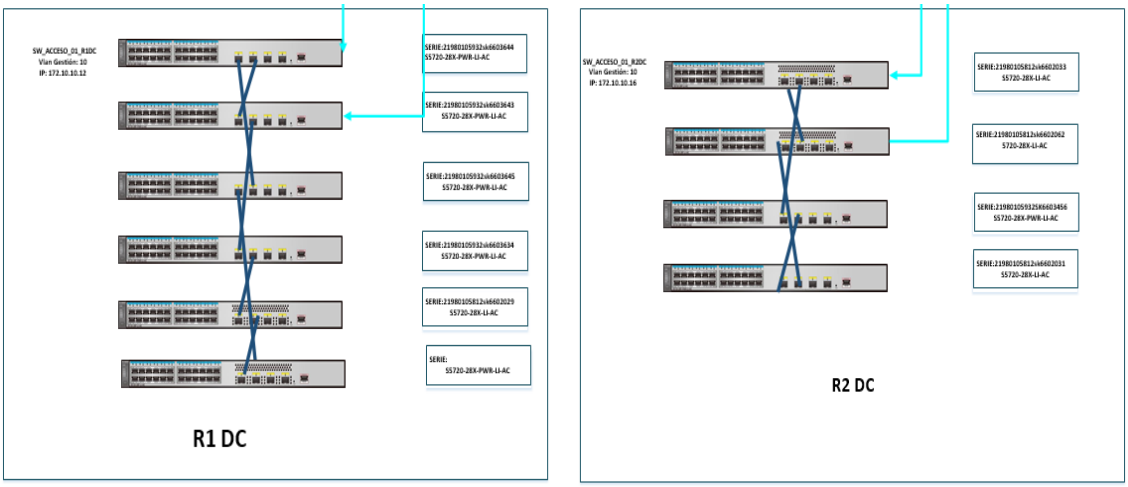
En la figura 1 se muestra el diagrama de topología lógico general para las conexiones de los equipos implementados de acuerdo con el cumpliendo de los requerimientos de HUAWEI-CHINA CAMC en base a las necesidades y requerimientos de la red Interna para el Hospital General Napoleón Dávila Córdova.

Figura 1. *Servidor de red.*



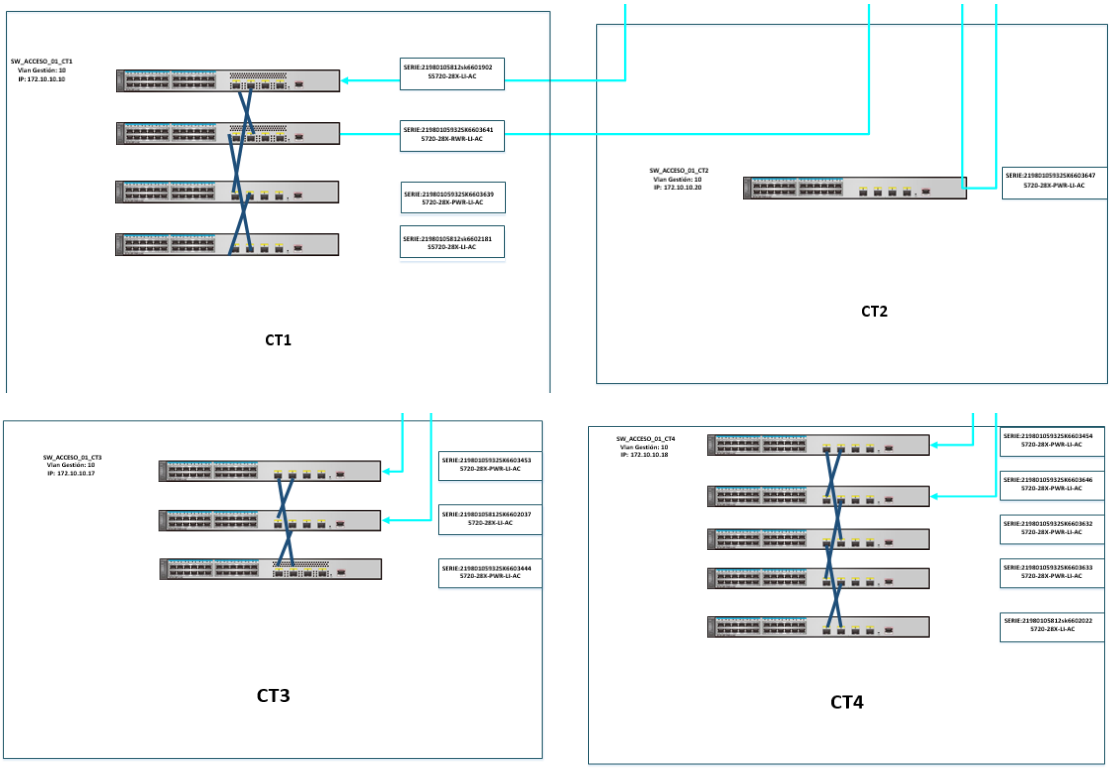
En la figura 2 los racks instalados esta distribuidos en 2 sectores el R1 DC y el R2 DC que distribuyen la información a los equipos que distribuyen a los equipos finales

Figura 2. *Racks instalados.*



En la figura 3 los equipos instalados en los CT1-CT2-CT3-CT4 que se encuentran conectados al respectivamente en los Rack 01de los cuartos de equipos.

Figura 3. *Switches instalados.*



En la tabla 4 se presentan la distribución de los equipos con sus características y sus ubicaciones con una IP fija referentes a la implementación en el Hospital General Napoleón Dávila Córdova.

Tabla 4. *Características de los equipos de Red*

N°	NOMBRE	PARTE No	MODELO	SERIE	MAC	UBICACIÓN	IP
1	SW_CORE	02352qgg	CE6881-48S6CQ-B	S/N:101980117824	cc64a6f7d690	RACK_SERVIDORES	172.10.10.1
2	SW_CORE	02352qgg	CE6881-48S6CQ-B	S/N:101980117849	cc64a6f7d820	RACK_SERVIDORES	172.10.10.1
3	WLC	02351ytv	_ac6508	101980011346	44004d4eaa62	RACK_SERVIDORES	172.10.10.120
4	IBM	02312BSB	MP2M02R22S03	2102312BSB10K9000015	44004d4euo62	RACK_SERVIDORES	172.10.10.100
5	KVM,KVM 17\" LED	6040183	WM1P0CIKVM02	1708A-X11V619BG518	44204d4eaa33	RACK_SERVIDORES	172.10.10.100
6	eSight NMS	05110EUY	NSHBASE390	2105110EUY10K9000045	44004d4iaa57	RACK_SERVIDORES	172.10.10.102

7	SW_ACCESO_01_R1DC-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2sk6603644	f4796012ab80	R1DC	172.10.10.12
8	SW_ACCESO_01_R1DC-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2sk6603643	f4796012ab70	R1DC	172.10.10.12
9	SW_ACCESO_01_R1DC-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2sk6603645	f4796012ab90	R1DC	172.10.10.12
10	SW_ACCESO_01_R1DC-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2sk6603634	f4796012aae0	R1DC	172.10.10.12
11	SW_ACCESO_01_R1DC-PB	98010581	S5720-28X-LI-AC	2198010581 2sk6602029	f47960077300	R1DC	172.10.10.12
12	SW_ACCESO_01_R1DC-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK5600738	f47960077300	R1DC	172.10.10.12
13	SW_ACCESO_01_R2DC-PB	98010581	S5720-28X-LI-AC	2198010581 2sk6602033	f47960077340	R2DC	172.10.10.16
14	SW_ACCESO_01_R2DC-PB	98010581	S5720-28X-LI-AC	2198010581 2sk6602062	f47960077510	R2DC	172.10.10.16
15	SW_ACCESO_01_R2DC-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603456	F47960129FC0	R2DC	172.10.10.16
16	SW_ACCESO_01_R2DC-PB	98010581	S5720-28X-LI-AC	2198010581 2sk6602031	f47960077320	R2DC	172.10.10.16
17	SW_ACCESO_01_CT1-PB	98010581	S5720-28X-LI-AC	2198010581 2sk6601902	f47960076b10	CT1	172.10.10.10
18	SW_ACCESO_01_CT1-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603641	f47960077c80	CT1	172.10.10.10
19	SW_ACCESO_01_CT1-PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603639	F4796012AB30	CT1	172.10.10.10
20	SW_ACCESO_01_CT1-PB	98010581	S5720-28X-LI-AC	2198010581 2sk6602181	F4796012AB50	CT1	172.10.10.10
21	SW_ACCESO_01_CT2_PB	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603647	f47960077290	CT2	172.10.10.20
22	SW_ACCESO_01_CT3-P1	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603453	F47960129F90	CT3	172.10.10.17
23	SW_ACCESO_01_CT3-P1	98010581	S5720-28X-LI-AC	2198010581 2SK6602037	F47960129F00	CT3	172.10.10.17
24	SW_ACCESO_01_CT3-P1	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603444	F47960077380	CT3	172.10.10.17

25	SW_ACCESO_01_CT4-P1	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603454	F47960077330	CT4	172.10.10.18
26	SW_ACCESO_01_CT4-P1	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603646	F47960077367	CT4	172.10.10.18
27	SW_ACCESO_01_CT4-P1	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603632	F47960077378	CT4	172.10.10.18
28	SW_ACCESO_01_CT4-P1	98010593	S5720-28X-PWR-LI-AC	2198010593 2SK6603633	F47960077399	CT4	172.10.10.18
29	SW_ACCESO_01_CT4-P1	98010581	S5720-28X-LI-AC	2198010581 2sk6602022	F47960077350	CT4	172.10.10.18
30	AP_01	02351TYR	AP7060DN	2102351tyr10k5010469	e0cc7a950000	COMEDOR_PB	172.10.10.24
31	AP_02	02351TYR	AP7060DN	2102351tyr10k5010477	e0cc7a950100	SALA DE ESPERA A	172.10.10.25
32	AP_03	02351TYR	AP7060DN	2102351tyr10k5010482	e0cc7a9501a0	SALA DE ESPERA B	172.10.10.26
33	AP_04	02351TYR	AP7060DN	2102351tyr10k5010480	e0cc7a950160	SALA DE ESPERA C	172.10.10.27
34	AP_05	02351TYR	AP7060DN	2102351tyr10k5010479	e0cc7a950140	HOSPITALIZACION	172.10.10.28
35	AP_06	02351TYR	AP7060DN	2102351tyr10k5010481	e0cc7a950180	HOSPITALIZACION	172.10.10.29

En la tabla 5 una vez obtenido los resultados y a la vez analizados se investigó que los IDS, tienen su comportamiento, el soporte técnico y la compatibilidad en las redes y los sistemas operativos en distintos equipos como Windows, MacOS y otros, con esta características se pudo decidir la selección y el análisis de todos estos IDS y se puedo determinar cuáles serían aptos para la implementación y a sí mismo no pueda tener problemas cuando se implemente en la institución, de los cuales el Snort y Suricata son las que han cumplido con lo que se cuenta en la institución ya que permitirán un buen funcionamiento ya que son compatibles.

Tabla 5. *Herramientas que son apropiadas*

IDS	Licencia	Compatibilidad	Estándares de interconexión	Enfoque	Soporte	IPS	Tipo
Snort	Libre	Linux, FreeBSD, Windows, MacOS	IPv4/IPv6	A-IDS, S-IDS	SI	SI	NIDS
Suricata	Libre	Linux, FreeBSD, Windows, MacOS	IPv4/IPv6	A-IDS, S-IDS	SI	SI	NIDS
Zeek	Libre	Linux, FreeBSD, MacOS	IPv4/IPv6	A-IDS	SI	NO	NIDS
MacAfee Network Security Plataform	Propietaria	Linux, Windows	IPv4/IPv6	S-IDS	SI	NO	HIDS
Ossec	Libre	Linux, FreeBSD, Windows, MacOS	IPv4/IPv6	S-IDS	SI	NO	HIDS

Snort y Suricata en la implementación es muy ágil en las aplicaciones en la red, ya que pueden combinarse y poder ejecutarse y poner en funcionamiento la detección de intrusos y anomalías que puedan ser detectadas.

En amparo con las medidas de monitoreo, prevención y mitigación permitirá evitar ataques a la red y el poder adueñarse de información, y así poder tener mayor seguridad en el hospital. Los IDS permiten desempeñar un rol importante porque permite tener un monitoreo constante y así poder implementar medidas de prevención en la red.

Los IDS Snort y Suricata permiten dar soluciones de código abierto permitiendo monitorear y prevenir cualquier ataque que pueda efectuarse en toda la red del hospital. Estas soluciones permiten una mayor seguridad de otras aplicaciones que existen actualmente.

Los IDS como cualquier aplicación que se utilizan en los sistemas informáticos deben estar en constante actualizaciones sistemáticas, ya que permite disminuir ataques y obtener mayor seguridad ante posibles intentos de robo de información o filtración de datos.

Según Llanes (2021) La adopción de medidas de prevención, monitoreo y mitigación constituye una vía efectiva para evitar ataques cibernéticos y elevar la seguridad en instituciones de salud. En este aspecto, los IDS desempeñan un rol fundamental porque son herramientas de monitoreo que

contribuyen a implementar medidas para prevenir intrusiones en las redes de datos.

Al aplicar estas medidas con estas herramientas el cual permitirá monitorear la red y el tráfico permitiendo identificar posibles brechas que permitan tener ataques a los equipos ya que con esto permitirá que la información que está almacenada pueda estar segura, y la institución no pueda sufrir robo de información para después pueda ser extraída y estar en manos de otras.

4. Conclusiones

La herramienta innovadora Snort y Suricata, ha sido una de las más implementadas ganando una posición preponderante que la hace ser percibida por los usuarios como una de las mejores en el mercado, encaminadas a ofrecer seguridad para el registro y uso de los datos, ya que permite prever posibles ataques a estas redes.

Además, permite identificar anomalías que ocurren dentro de ella, detectarlas y dar soluciones inmediatas para evitar el acceso a posibles intrusos, es confiable también porque al aplicar otras herramientas como antivirus o firewall otorga mayor seguridad en los equipos.

Al emplear estas herramientas en la institución permitirá a la institución tener una seguridad alta y permitir que se disminuya los ataques y los posibles intrusos que quieran obtener información de los pacientes o procesos administrativos.

El manejo de la información que los pacientes registran dentro de una casa de salud debe estar garantizada por medio de la utilización de sistemas de monitoreo que garanticen que no exista forma de extraer ninguna especie de datos, a no ser que exista de por medio, la autorización de personal certificado.

Bibliografía

Arteaga, José. (2020). Evaluación de las funcionalidades de los sistemas de detección de intrusos basados en la red de plataformas Open Source utilizando la técnica de detección de anomalías. [Tesis de Maestría, Escuela Superior Politécnica del Chimborazo]. Repositorio Institucional – Escuela Superior Politécnica del Chimborazo.

http://dspace.espoch.edu.ec/handle/123456789/8748

Ashok D, M. V. (2020). Comparative Study and Analysis of Network Intrusion Detection Tools. IEEE Xplore.

Barad, M. (2019), Linking Cyber Security Improvement Actions in Healthcare Systems to Their Strategic Improvement Needs, Procedia Manufacturing, Volume 39, Pages 279-286, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2020.01.335.

Bhuyan SS, K. U. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. SpringerLink.

Caro, R. (2020). Despliegue y explotación de herramientas Open Source para la monitorización y gestión de eventos en un entorno virtualizado.

Castellanos O, G. M. (2020). Análisis y caracterización de conjuntos de datos para detection de intrusiones. Serie Científica de la Universidad de las Ciencias Informáticas.

Coventry L, B. D. (2020). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas.

Iona. (2017), Cyber security in healthcare networks,"E-Health and Bioengineering Conference (EHB), Sinaia, Romania, 2017, pp. 414-417, doi: 10.1109/EHB.2017.7995449.

Karim, Imdadul & Vien, Quoc-Tuan & Le, Tuan & Mapp, Glenford. (2017). A Comparative Experimental Design and Performance Analysis of Snort-Based Intrusion Detection System in Practical Computer Networks. Computers. 6. 15. 10.3390/computers6010006.

Macia-Fernández G, C. J.-C.-G.-T. (2017). Un nuevo conjunto de datos para la evaluación de IDS de red. EDITORIAL UNIVERSITAT POLITÈCNICA DE VALÈNCIA.

Maniriho, Pascal & Mahoro, Leki & Niyigaba, Ephrem & Bizimana, Zephanie & Ahmad, Tohari. (2020). Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches. International Journal of Intelligent Engineering and Systems. 13. 10.22266/ijies2020.0630.39.

Perdigón LR, Orellana GA. 2021. Sistemas para la detección de intrusiones en redes de datos

de instituciones de salud. Revista Cubana de Informática Médica. 2021

Rodríguez Díaz A, Vidal Ledo MJ, Cuellar Rojas A, Martínez González BD, Cabrera Arribas YM. (2017) Desarrollo de la Informatización en Hospitales. https://revinfodir.sld.cu/index.php/infodir/article/view/121

Sánchez. (2021). Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad. https://dspace.ups.edu.ec/bitstream/123456789/20321/1/UPS-GT003222.pdf

Shah, Syed & Issac, Biju. (2018). Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System. Future Generation Computer Systems. 80. 157-170. 10.1016/j.future.2017.10.016.

Syed Ali Raza Shah, Biju Issac. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system, Future Generation Computer Systems, Volume 80, Pages 157-170, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.10.016

Uvidia Armijo, LA. (2017). Evaluación de herramientas de generación de tráfico malicioso aplicadas a una red IP virtualizada. http://hdl.handle.net/10251/91790

Zambrano (2019), Análisis de la eficiencia de los IDS open source Suricata y Snort en las PYMES. Universidad Espíritu Santo.