ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.
Volume 2, Issue no. 2, DOI 10.18502/espoch.v2i2.11413
Production and Hosting by Knowledge E

Research Article

Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study

Políticas de Ciberseguridad para los Dispositivos de Conmutación de Red en el Centro de Datos Hospitalario: Un Estudio de Caso

Diego Fernando Avila Pesantez[1]*, Richard Chalan Analuisa[2], George Figueras[3], and Miriam Avila[4]

[1]Grupo de Investigación en Innovación Científica y Tecnológica, Escuela Superior Politécnica de Chimborazo, Riobamba (ESPOCH), Riobamba, Ecuador
[2]Escuela de Posgrado, Maestría en Ciberseguridad, Pontifica Universidad Católica del Ecuador sede Ambato, Ambato, Ecuador
[3]Facultad de Ingeniería, Universidad Simón Bolívar, Caracas, Venezuela
[4]Facultad de Mecánica, Escuela Superior Politécnica de Chimborazo (ESPOCH), Riobamba, Ecuador

VIII INTERNATIONAL CONGRESS OF SCIENCE TECHNOLOGY ENTREPRENEURSHIP AND INNOVATION (SECTEI 2021)

Corresponding Author: Diego Fernando Avila Pesantez; email: davila@espoch.edu.ec

Published: 29 June 2022

Production and Hosting by Knowledge E

Abstract

Cybersecurity policies help ensure the operation of network communication devices used in hospital data centers, since administrators can easily implement mechanisms to mitigate attacks and vulnerabilities without affecting the operation of these devices. In this work, the ISO 27032 standard was selected to follow the four-phase guidelines: understanding the organization, risk analysis, action plan, and implementation, which allowed for proposing the necessary cybersecurity policies for the network infrastructure in a Huawei device. First, the vulnerability tests were carried out with the OPENVAS and Yersinia tools, establishing the probability of attacks like MAC-ARP, DHCP Starvation, STP attack, Vlan hopping, etc. Through the respective configurations and enabling functionalities, it was possible to mitigate a significant amount of 98% of the existing vulnerabilities in the initial state of the hospital network infrastructure.

Keywords: *Cybersecurity policies, ISO 27032, hospital network infrastructure, attack mitigation.*

Resumen

Las políticas de ciberseguridad permiten asegurar el funcionamiento de los equipos de comunicación de red en una infraestructura tecnológica hospitalaria, ya que los administradores pueden implementar mecanismos de mitigación a ataques y vulnerabilidades, evitando afectar el funcionamiento de estos dispositivos. En este trabajo se tomó como referencia la norma ISO 27032 para seguir los lineamientos de cuatro fases: entendimiento de la organización, análisis de riegos, plan de acciones e implementación, que permitieron proponer las políticas de ciberseguridad necesarias para la infraestructura de red en equipos de marca Huawei. En la primera etapa se realizó las pruebas de vulnerabilidades con las herramientas OPENVAS y Yersinia, estableciendo la probabilidad de ataques tales como MAC-ARP, DHCP Starvation, ataque STP, Vlan hopping, entre otros. Mediante las respectivas configuraciones y habilitación de funcionalidades, se pudo mitigar una cantidad significativa del 98% de las vulnerabilidades existentes en el estado inicial de la infraestructura de red hospitalaria.

Palabras Clave: *Políticas de ciberseguridad, ISO 27032, Infraestructura de red hospitalaria, Mitigación de ataques.*

How to cite this article: Pesantez DFA, Analuisa RC, Figueras G, Avila M (2022). Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.*, 2(2), 507–518. DOI 10.18502/espoch.v2i2.11413

1. Introducción

La Ciberseguridad en la infraestructura de Red de datos se refiere a la capacidad de protección que se puede aplicar a los activos físicos y digitales, así como a la información que es procesada, almacenada o transportada [1]. Esta se basa en principios y conceptos específicos relacionados con los activos y las protecciones que están destinadas a detectar, reaccionar y recuperarse de ataques, controlar las amenazas de los usuarios internos y brindar una defensa profunda [2]. Los administradores de red implementan seguridades en software y hardware, dando mayor importancia a las capas superiores del modelo OSI [3]. Sin embargo, descuidan las capas inferiores que son infraestructuras más vulnerables. Según el reporte del FBI, el 80% de los ataques a la capa de red provienen del interior de la organización, debido a que el 99% de los puertos de los equipos de conexión están sin restricciones, por factores de gestión del administrador de red, esto permite que cualquier usuario pueda conectarse a ellos [4].

Según el informe de IBM y el Ponemon Institute del 2016, la frecuencia de violaciones a los dispositivos de conmutación en la infraestructura de una red sanitaria ha aumentado desde 2010, y ahora se encuentra entre los sectores más afectados por los ciberataques a nivel mundial [5]. Debido a su inmutabilidad, la información a la que se accede, es de especial interés para los delincuentes, que pueden provocar un daño psico-social cuando están comprometidos [6]. Por tanto, la importancia de la disponibilidad los dispositivos de red capa dos y capas superiores para la conexión hacia el internet se han tornado fundamental en la infraestructura tecnológica. Cabe destacar, que la falta de políticas de ciberseguridad adecuadas facilita el acceso a los atacantes como si fueran usuarios internos, provocando redes zombis o terminales infectados, permitiendo el acceso no autorizado a los recursos y servicios de la infraestructura de red [7].

En el caso de las instituciones públicas, las cuales prestan servicios de salud, los equipos de la infraestructura de red son importantes para mantener la comunicación entre la red integral hospitalaria, que permiten la transmisión, recepción de los datos y mantienen la disponibilidad de la información en línea. Con el pasar del tiempo, los atacantes informáticos han descubierto nuevos métodos para ganar dinero y la industria de la salud se está convirtiendo en un objetivo fácil, debido a la capacidad de vender grandes lotes de datos personales con fines de lucro [8-10].

Los principales ataques a la infraestructura de red a nivel de conmutación son de suplantación de identidad, MAC-ARP (Address Resolution Protocol), ataques a Spanning Tree Protocol (STP), Vlan Hopping y Dynamic Host Configuration Protocol (DHCP) Starvation [11, 12]. Mediante el análisis de tráfico se logra identificar los servicios que

circulan por la red y principalmente se puede concluir que, mediante la aplicación de reglas, y priorización de servicios se logra minimizar estos ataques hacia los dispositivos de comunicación, que ocasionan en ciertos momentos la saturación de la red de datos. Además, con la segmentación se logra dividir y agrupar a los hosts por cada departamento, de este modo, se puede implementar las políticas de ciberseguridad, que ayuden en la administración y gestión de la red [13].

La norma ISO/IEC 27001 detalla los requerimientos generales para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de Información dentro de una organización [14, 15], y específicamente la norma ISO 27032 permiten obtener una visión específica de buenas prácticas de ciberseguridad y brindan la disposición para fortalecer los aspectos técnicos y estratégicos, los cuales están alineados con la protección de activos en redes, internet, información e infraestructuras críticas para la información [16].

En esta normativa se establece cuatro fases para la gestión de riesgos para la infraestructura de red que permitan la implementación de medidas y controles ante vulnerabilidades, respuesta ante posibles incidentes, la reducción de ocurrencia de ataques y la mitigación de elementos adversos [17]. La primera fase es el entendimiento de la organización para conocer sus procesos y funcionamiento, y recopilar los mecanismos técnicos de seguridad, generando un inventario de activos. En la fase dos se lleva a cabo la evaluación de controles y medidas de seguridad, considerando las amenazas, vulnerabilidades y activos críticos, basado en la gestión de riesgos. La siguiente fase define el plan de acción para afrontar con políticas, métodos de protección y estrategias que deberán aplicarse en la organización. Finalmente, la implementación de controles permite la protección ante ataques, validación de datos, procesos de autenticación, configuraciones más confiables, actualización de sistemas operativos y verificaciones de seguridad en la infraestructura de red (ver Figura 1).

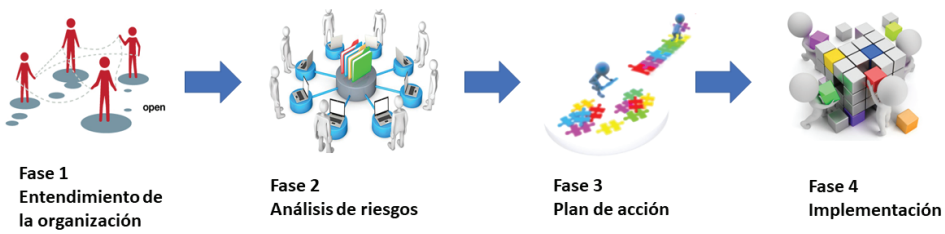

Figure 1

Fases de la norma ISO 27032.. **Fuente:** www.isecauditors.com/consultoria-csf-iso-27032.

En trabajos relacionados al tema de estudio, Ramírez et al. analizaron los ataques en cada capa del modelo OSI que afectan a los procesos de comunicación, estableciendo

los mecanismos teóricos de prevención, detección y mitigación de las principales vulnerabilidades, aplicados la infraestructura de red de una organización [18]. Por otro lado, Ochoa propone un análisis de tráfico para determinar la seguridad en la capa de enlace de datos en una red LAN cableada e inalámbrica, considerando la norma ISO 27000 [19]. En este sentido, Mendizadeha et al. y Yuones establecieron varios mecanismos de mitigación para ataques ARP, DHCP y VLAN que permiten reforzar la seguridad en la infraestructura de red, mediante procesos de autenticación e integridad de los mensajes de ARP y DHCP [20, 21].

En este trabajo se aplicará la norma ISO 27032 orientada a la parte práctica dentro de la infraestructura tecnológica hospitalaria, a fin de preservar la disponibilidad de los servicios mediante mecanismos preventivos, detectivos y reactivos, que permitan mitigar las vulnerabilidades detectadas.

En la primera sección se presentó la información general sobre la ciberseguridad en infraestructura de red basado en las normas ISO y las fases necesarias para su aplicación. La Sección 2 presenta el proceso de implementación de la norma ISO 27032 en un estudio de caso hospitalario. Finalmente, el artículo describe los resultados obtenidos y las conclusiones.

2. Materiales y Métodos

Para el desarrollo del estudio de caso se utilizó las cuatro fases planteadas que permitan evaluar los riesgos de los activos de la infraestructura de red, que se detalla a continuación.

2.1. Fase de Entendimiento de la organización

Para este estudio se seleccionó una casa hospitalaria que proporciona servicios de salud con asistencia especializada de segundo nivel ubicada en la zona central del Ecuador, la cual cumple con la responsabilidad de recuperación y rehabilitación de la salud, docencia e investigación, acorde a las políticas del Ministerio de Salud Pública. Esta institución ofrece los principales servicios de consulta externa, emergencia, medicina interna, cirugía general, laboratorio, gestión administrativa, y área de Tecnologías de la Información, entre otros (ver Figura 2). Estas dependencias generan información, que deben ser compartida por dicho ministerio a la red global de salud ecuatoriana.

En la Figura 3 se muestra la topología y la distribución de los equipos de red, que tiene como parte modular un switch principal multicapa, cinco switches capa 3 y doce switches de acceso, una PBX de telefonía y servidores, que están distribuidos en las

dependencias con una topología en estrella extendida, utilizando enlaces redundantes con fibra óptica y cable par trenzado. Para el sistema de protección se dispone de un firewall, un router de acceso a Internet, y un data storage que respalda de la información. La red está configura con 22 VLANs y los datos que generan el personal de la institución son analizados y digitalizados por equipos biomédicos que se recopilan mediante los sistemas de cómputo. Esta infraestructura no cuenta con mecanismos de ciberseguridad, por lo que se encuentran propenso a ataques.

Figure 2

Diagrama de la estructura institucional hospitalaria.

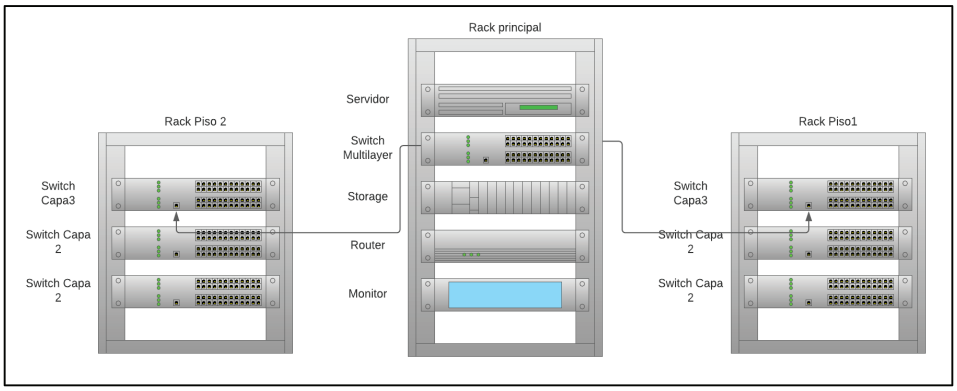

Figure 3

Esquema representativo de la infraestructura de equipos de conmutación del centro hospitalario.

2.2. Fase de análisis de riesgos

En esta etapa se lleva a cabo el análisis de la infraestructura de red utilizando herramientas y técnicas para detectar amenazas y vulnerabilidades de los equipos de conmutación de la institución. Para ello, se empleó la herramienta OPENVAS instalada sobre un sistema operativo Linux (Parrot). Se configuró el identificador (gateway) para obtener el informe estadístico de cada uno de los equipos interconectados (ver Figura 4). Una vez finalizada el escaneo de los dispositivos se generó los huecos de inseguridad y el nivel de vulnerabilidad, que un atacante con privilegios y permisos puede aprovechar para tener acceso a la red, debido a una escasa configuración. La tabla 1 muestra las vulnerabilidades obtenidas, siendo el usuario interno la principal amenaza para ingresar a la infraestructura de red, por la incorrecta asignación de límites y permisos que tienen dentro de la organización.

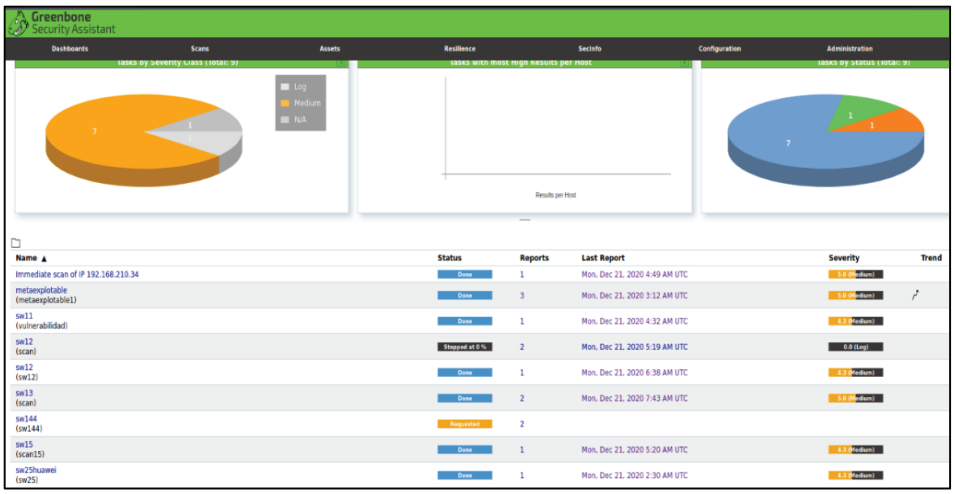

Figure 4

Escaneo de las principales vulnerabilidades encontradas en la infraestructura de red.

2.3. Fase de plan de acciones

Basado en la norma ISO 27032 se implementan buenas prácticas de ciberseguridad, con el objetivo de generar lineamientos para la protección de los dispositivos de la capa de enlace. Con lo expuesto y con el resultado del diagnóstico y análisis realizado en la fase anterior, la organización pudo conocer e identificar las vulnerabilidades y amenazas para efectuar el plan de acciones de control preventivo y correctivo, que se muestra en la Tabla 2.

Table 1

Resumen de los ataques detectados en la infraestructura tecnológica.

ID	Ataque principal	Funcionamiento	Recomendación general
A1	Ataque hombre en la mitad (MITM)	Cuando el atacante ingresar al equipo utilizando telnet, puesto que interceptó información, afectando la identificación de los usuarios y contraseñas. WiFi abierta	Utilizar ssh o stelnet. Restringir acceso y permisos a la red inalámbrica
A2	Ataque CAM table overflow Ataque ARP spoofing	El switch empieza a comportarse como un HUB, debido a que la tabla CAM está saturada, y no se aceptan nuevas entradas. Cuando la tabla CAM no puede almacenar más asociaciones MAC-Puerto, el switch empieza a enviar por todos los puertos (broadcast) las tramas que tengan una dirección MAC destino y no almacenada en la tabla de forwarding	Configuración de ARP anti-attack en los switches
A3	Ataque STP	Un atacante envía mensajes BPDU forzando recálculos STP para convertirse en root, y esto trae como consecuencia que pueda ver tramas que no debería (esto permite ataques MITM, DoS)	Configuración de mecanismo de protección de STP
A4	Ataque DHCP starvation / discovery	Consiste en inundar con peticiones DHCP_REQUEST al servidor DHCP, con direcciones MAC modificadas y con el objetivo de agotar su espacio de direcciones asignables, con el fin de que el servidor DHCP no sea capaz de responder a otros hosts y así realizar otro tipo de ataques (DHCP rogue)	Evitar la denegación de servicio DHCP
A5	Ataque switch spoofing y Ataque a vlans–double tagging	Los switches implementan Vlan, los usuarios se conectan a puertos de acceso que son miembros. Vlan HOPPING es cuando un usuario obtiene el acceso a una Vlan no asignada al puerto del switch, que se conecta	Evitar el doble tagging en las interfaces troncales en los switches

2.4. Fase de implementación

En este apartado se realizó las configuraciones en los dispositivos de conmutación utilizando las herramientas de emulación EVE-NG, Yersinia y DSNIFF, que permitieron analizar el comportamiento de la red en un ambiente simulado, antes de ponerlos en ejecución en los equipos físicos y mitigar las vulnerabilidades establecidas, que se puede visualizar en la tabla 3.

Table 2

Resumen de las Políticas para mitigar los ataques establecidos.

ID	Política de ciberseguridad
A1	Utilizar los protocolos SSHv2/STELNET para ingresar a la configuración de los dispositivos marca Huawei Agregar un ACL para restringir acceso a la VLAN de gestión
A2	Limitar en cada puerto de la cantidad de direcciones MAC que se pueden aprender para que en el momento que se alcance el máximo se descarten las tramas de direcciones no conocidas. Limitar la tasa de paquetes ARP según las direcciones MAC de origen y las direcciones IP de origen Asignar direcciones MAC estática en los puertos, para que solo tramas de ciertas MAC sean procesados. Aprendizaje de direcciones MAC persistentes, al conectar un dispositivo a un puerto, este aprenda su MAC y no acepte la conexión de ningún otro dispositivo Limitar la interfaz para evitar acceso a un gran número de tramas broadcast, unicast o multicast. Interfaces sin uso deben estar modo apagado (shutdown) Interfaces que no estén siendo utilizadas deben estar en *modo Access* y se evidencia que están sin ninguna línea de configuración Habilitar la detección de violaciones de seguridad, y en el caso de ocurrencia se apague el puerto automáticamente
A3	No deshabilitar STP en los switches (introducir un loop físico puede convertirse en una forma de ataque) Habilitar la protección BPDU en un dispositivo de conmutación Habilitar la configuración de protección de cambio de topología Habilitar la protección de root primario en la interfaz de enlace (troncal)
A4	Configurar las interfaces para la detección de paquetes de solicitud DHCP para protegerse contra ataques de agotamiento de DHCP. Configurar interfaces como confiables para protegerse contra ataques falsos al servidor DHCP. Configurar la detección de direcciones MAC para protegerse contra ataques de denegación de servicios (DoS) DHCP.
A5	Desactivar el auto trunking por defecto activando las interfaces en *modo access* Deshabilitar las interfaces que no estén siendo utilizado No utilizar la Vlan nativa.

3. Resultados

En esta sección se presentan los resultados obtenidos de las pruebas realizadas en el escenario de simulación con la herramienta EVE-NG, considerando 1 switch principal y 4 switches de acceso de marca Huawei, configurados con la VLAN 10, 20, 25 y 40. Los puertos que se conectan entre switches están en modo troncal con enlaces redundantes. En cada VLAN se han configurado varias PC, y en el atacante (PC) se instaló Kali Linux para generar los ataques de hombre en la mitad, CAM table overflow, ARP spoofing, STP, DHCP starvation, switching spoofing y VLAN double-tagging (ver Figura 5). Para la experimentación se creó dos escenarios (pre-test y post-test), en el primero se analizó las vulnerabilidades que están expuestas en la infraestructura de red sin políticas de ciberseguridad y en el segundo caso, se implementó las políticas establecidas para medir el porcentaje de mitigación, utilizando la herramienta de OPENVAS. Los resultados obtenidos se contabilizaron en función de 10 escenarios de prueba desarrollados durante una semana, que resume el número de ataques exitosos y fallidos, detallados en la tabla 4.

Table 3

Comandos de configuración aplicados los equipos de red Huawei en función de los ataques registrados.

ID	Configuración implementada
A1	# stelnet server enable SSH authentication-type default password SSH user huawei SSH user huawei authentication-type password SSH user huawei service-type all SSH client first-time enable #
A2	# ARP speed-limit source-ip maximum 50 # interfaz Vlanif4 ARP-limit maximum 20 # port-security enable port-security max-MAC-num 4 port-security protect-action restrict MAC-learning priority 4 ARP anti-attack rate-limit enable ARP anti-attack rate-limit packet 50 blocktimer 60
A3	# STP instance 0 root primary STP bpdu-protection STP tc-protection # interfaz GigabitEthernet0/0/27 description Puerto para PC y Telefono port link-type hybrid voice-vlan 100 enable port hybrid pvid vlan 4 port hybrid tagged vlan 100 port hybrid untagged vlan 4 storm-control broadcast min-rate 5000 max-rate 8000 storm-control action error-down storm-control enable trap STP edged-port enable #
A4	# DHCP server group DHCPgroup1 DHCP snooping enable ipv4 ARP DHCP-snooping-detect enable DHCP snooping check DHCP-rate enable DHCP snooping check DHCP-rate 90 DHCP snooping alarm DHCP-rate enable DHCP snooping alarm DHCP-rate threshold 500 # DHCP snooping enable DHCP snooping check DHCP-giaddr enable DHCP snooping check DHCP-request enable DHCP snooping alarm DHCP-request enable DHCP snooping alarm DHCP-request threshold 120 DHCP snooping max-user-number 20 DHCP snooping check DHCP-chaddr enable DHCP snooping alarm DHCP-chaddr enable DHCP snooping alarm DHCP-chaddr threshold 120 #
A5	# STP instance 0 root primary STP bpdu-protection STP tc-protection # interfaz GigabitEthernet0/0/25 description Puerto para PC y Telefono shutdown port link-type hybrid voice-vlan 100 enable port hybrid pvid vlan 4 port hybrid tagged vlan 100 port hybrid untagged vlan 4 #

La implementación de las políticas propuestas y aplicadas mediante la configuración de comandos en los equipos de conmutación, demuestran los resultados de mitigación a los ataques y vulnerabilidades establecidas con un promedio de efectividad del 98% en el centro de datos hospitalario. Los ataques de overflow a la tabla CAM, ARP spoofing y MITM fueron contrarrestados en su totalidad (100%) y los restantes tienen una media del 96,5% de mitigación efectiva. El siguiente paso fue aplicar las configuraciones en los equipos físicos, concluyendo que en la infraestructura de red del centro hospitalario se aplicó los correctivos necesarios para mejorar su seguridad informática.

4. Conclusiones

Toda organización tanto pública como privada está propensa a ataques informáticos, por lo que es recomendable la implementación de políticas de ciberseguridad. En este trabajo se enfocó el análisis de la infraestructura de red, ya que es una de las áreas más vulnerable de las empresas, debido a que los usuarios internos son quienes tienen mayor privilegio y permisos para poder acceder a información confidencial, sin ninguna restricción. Por lo tanto, es necesario aplicar procesos para mitigar el riesgo de

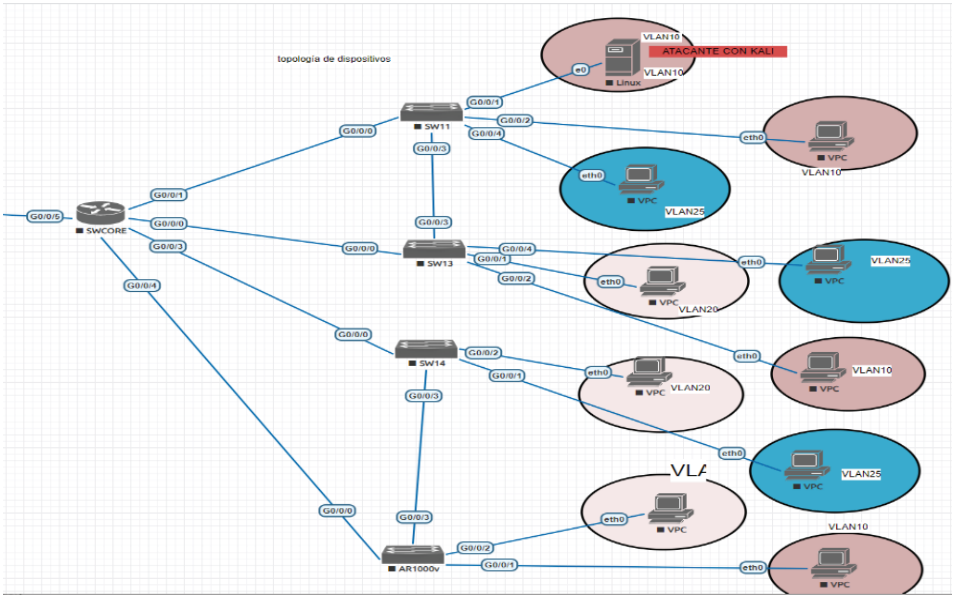

Figure 5

Escenario de pruebas simuladas para mitigar los ataques utilizando EVE-NG.

Table 4

Resultados obtenidos con la experimentación realizada.

Ataque principal	Escenario inicial sin políticas de ciberseguridad (pre-test)	Aplicación de la política de ciberseguridad (post-test)
	% mitigación de ataques	% mitigación de ataques
Ataque hombre en la mitad (MITM)	5%	100%
Ataque CAM table overflow Ataque ARP spoofing	2% 3%	100% 100%
Ataque STP	4%	98%
Ataque DHCP Starvation / Discovery	2%	98%
Ataque switch spoofing Ataque a VLANs–double tagging	3% 3%	95% 95%
Promedio 3.14% 98%		

la indisponibilidad en los dispositivos de conmutación. En el estudio de caso se aplicó la norma ISO 27032, las cuales permitieron reducir el riesgo de los ataques del hombre en la mitad (MITM), DHCP, STP, VLAN Hopping y MAC-ARP, agregando los parámetros y líneas de configuración en los equipos de marca Huawei. Esto mejoró en un promedio del 98% el grado de seguridad en la infraestructura de red, basado en los ataques establecidos en el entorno de simulación con un escenario pre y post test, evidenciando que las organizaciones que no han implementado las políticas de seguridad están

expuestas a amenazas y vulnerabilidades que pueden dejar sin servicio a los usuarios. Por tanto, se debe considerar contratar personal especializado en ciberseguridad que aseguren la protección de la información.

Para trabajo futuro se puede ampliar la mitigación de vulnerabilidades a los servidores y aplicaciones con técnicas de pentesting, que protejan la información que se gestiona en el centro hospitalario.

References

[1] A. Inoguchi Rojas and E. L. Macha Moreno, ”Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016,” Universidad San Ignacio de Loyola, June, 18 2017.

[2] O. M. Gallego, ”Diseño y Manejo de Infraestructuras de Red Cumpliendo con los Estándares de Ciberseguridad,” ETSI Informáticos, January, 6 2021.

[3] R. J. Martelo, J. E. Madera, and A. D. J. I. t. Betín, ”Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI),” Scielo, vol. 26, no. 2, pp. 129-134, May 2015.

[4] Y. Xia, C. Liu, and K. Yu, ”Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on Openvas,” in IOP Conference Series: Earth and Environmental Science, 2020, vol. 440, no. 4, p. 042031: IOP Publishing.

[5] E. Pérez Morera, ”Estudio de soluciones de seguridad para apps móviles en Sanidad,” 2016.

[6] S. T. Argaw et al., ”Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks,” vol. 20, no. 1, pp. 1-10, 2020.

[7] R. Camacho, H. C. C. Romero, M. V. M. Valencia, and M. A. Z. J. C. A. Lozano, ”Diagnóstico de conectividad y dispositivos de telecomunicaciones para el desarrollo de la Telesalud de veinte hospitales en el Departamento del Tolima,” Cuaderno Activa, vol. 11, pp. 105-119, Abril, 10 2019.

[8] J. J. Correa Sánchez, ”Manual de buenas prácticas en seguridad de la información para entornos hospitalarios,” Universidad EIA, Febrero, 18 2020.

[9] R. R. J. B. C. Herrera, ”La seguridad del paciente y la ciberseguridad,” BOLETÍN CONAMED, no. 15, Septiembre, 2 2017.

[10] P. Perea Paños, ”Análisis de ransomware en redes de infraestructuras médicas,” TFG EN ENGINYERIA INFORMATICA, vol. 2, 2020.

[11] C. Bresteau, S. Guigui, P. Berthier, and J. M. Fernandez, "On the security of aeronautical datalink communications: Problems and solutions," in 2018 Integrated Communications, Navigation, Surveillance Conference (ICNS), Herndon, VA, USA, 2018, pp. 1A4-1-1A4-13: IEEE.

[12] V. Umasuthan, "Protecting the Communications Network at Layer 2," in 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Dallas, 2016, pp. 1-5: IEEE.

[13] J. E. Salcedo Castillo, "Diseño y emulación de una red de datos con priorización de servicios en la Unidad Educativa Suizo Ambato," PUCE-Quito, Quito, 2020.

[14] K. G. Bermúdez Molina, "Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa De Servicios Financieros," INGENIERO DE SISTEMAS, Ingeniería de Sistemas, UNIVERSIDAD POLITÉCNICA SALESIANASEDE GUAYAQUIL, 2015.

[15] S. L. Guzmán Solano, "Guía para la implementación de la norma ISO 27032," UNIVERSIDAD CATÓLICA DE COLOMBIA, June, 5 2019.

[16] S. N. Solano, "PROYECTO DE TRABAJO DE GRADO GUÍA PARA LA IMPLEMENTACION DE LA NORMA ISO 27032," UNIVERSIDAD CATÓLICA DE COLOMBIA, Colombia, 2019.

[17] I. Auditors. (2020). Implementación de un Marco de Ciberseguridad ISO 27032. Available: https://www.isecauditors.com/consultoria-csf-iso-27032

[18] N. J. Ramírez Galvis, J. S. Rivera Cardona, and C. A. Mejía Londoño, "Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones," Universidad Tecnológica de Pereira, vol. 2, 2017.

[19] P. Ochoa, "Análisis de tráfico de datos en la capa de enlace de una red LAN, para la detección de posibles ataques o intrusiones sobre tecnologías Ethernet y Wifi 802.11," ESPE, Quito, vol. 4, 2011.

[20] A. Mehdizadeha, K. Suinggia, M. Mohammadpoorb, and H. Haruna, "Virtual Local Area Network (VLAN): Segmentation and Security," in The Third International Conference on Computing Technology and Information Management (ICCTIM2017), Thessaloniki, Greece, 2017, pp. 78-89: The Society of Digital Information.

[21] O. S. J. S. Younes, "Securing ARP and DHCP for mitigating link layer attacks," Sādhanā, vol. 42, no. 12, pp. 2041-2053, 2017.