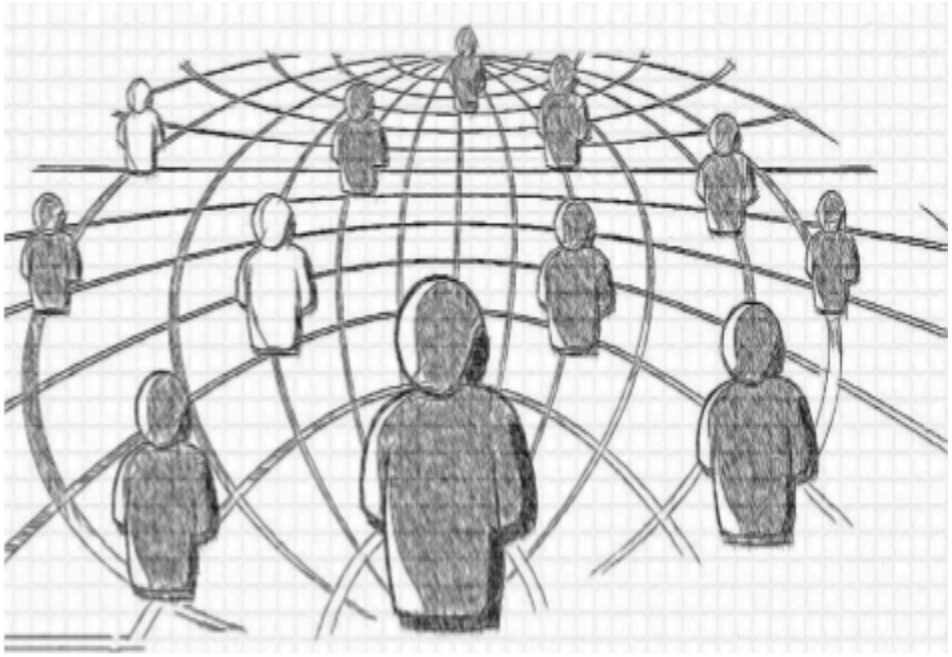
3ducatec
La educación del futuro

VOL. 1 NÚM. 1
ABRIL – MAYO 2024
ISSN EN TRÁMITE

REVISTA DE CIENCIA Y TECNOLOGÍA 3DUCATEC



DERECHOS DE AUTOR Y DERECHOS CONEXOS, AÑO 1, N°1, ABRIL – MAYO 2024.
Es una Publicación mensual editada por el ISC. Arturo Pérez Rendón, Av. Guadalupe Victoria, Col.Centro, C.P. 91700, Tel:(55)2294652980. Revista.3ducatec.com Editor responsable: Arturo Pérez Rendón, Reserva de derechos en proceso, ISSN: en proceso, última modificación, 30 de abril de 2024.
Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación.
Queda prohibida la reproducción total o parcial de los contenidos e imágenes de la publicación sin previa autorización del Instituto Nacional del Derecho de Autor.

ÍNDICE DE PONENCIAS

PRIMER AUTOR	TÍTULO DE PONENCIA	AUTORES	ÁREA TEMÁTICA	PÁGINA
Eudar Escobar Elías	SISTEMA EMBEBIDO COMO AULA VIRTUAL PARA LA POBLACIÓN ESTUDIANTIL VULNERABLE EN LA MATERIA PROGRAMACIÓN WEB	Sergio Alarcón Rodríguez, Dafne Angélica Hernández Vázquez,Omar Meza Vázquez,Dolores Vázquez Trujillo,Arturo Pérez Rendón	Ciencia de la Tecnología	2 a la 9
Eudar Escobar Elías	DHCP SNOOPING: UNA SOLUCIÓN EFICAZ PARA MITIGAR ATAQUES DHCP.	Sergio Alarcón Rodríguez, Luis Mario Correa Lozano, Diego Nava Taguada, Héctor Pérez Ortiz, César Augusto Rogel Gálvez, Arturo Pérez Rendón	Ciencia de la Tecnología	10 a la 13

SISTEMA EMBEBIDO COMO AULA VIRTUAL PARA LA POBLACIÓN ESTUDIANTIL VULNERABLE EN LA MATERIA PROGRAMACIÓN WEB

Eudar Escobar Elías [1],Sergio Alarcón Rodríguez[2], Dafne Angélica Hernández Vázquez[3], Omar Meza Vázquez[4], Dolores Vázquez Trujillo[5], Arturo Pérez Rendón[6]

Resumen. El presente proyecto demuestra cómo reducir el índice de reprobación y deserción escolar de nivel universitario, esta última por carecer de la infraestructura tecnológica en lugares marginados o de difícil acceso a la tecnología, mediante estrategias alternativas de aplicación de las TIC´S y con estas mejorar el desempeño académico de los estudiantes. Se considera como base metodológica el uso de las TIC´S aplicadas a los ámbitos educativos y sociales. El resultado de este proyecto demuestra la versatilidad en la aplicación de un sistema embebido, al ser implementado como apoyo a la estrategia de enseñanza-aprendizaje, auxiliando a los métodos tradicionales existentes y garantizando la equidad de oportunidades para todos los estudiantes universitarios

Palabras clave—Moodle, Maria DB, Raspberry, Linux HTML 5, PHP, LMS, Código Libre, SBC.

Embedded System as a virtual classroom for the vulnerable student population in the subject of Web Programming

Abstract. The present project demonstrates how the school failure and school dropout rates can be reduced, the last one due to lack of technological infrastructure in marginalized places or places with difficult access to technology, through alternative strategies for the application of ICT's and with these improve the academic performance of the students. It is considered as a methodological basis the ICT´S applied to the educational and social fields. In the first area the educational platform Moodle is coupled to a SBC (Single Board Computer) of Raspberry Pi Zero w. On the other hand, the second area seeks candidates in vulnerable populations that do not have Internet and /or computer equipment.

All things considered, with a sample of ten students from the career Computer Systems Engineering from the subject Web Programming studied in the seventh semester, who took their subjects with the Raspberry Pi Zero w, achieved a reduction of up to 40% in the failure rates with respect to previous semesters.

Keywords. Moodle, Maria DB, Raspberry, Linux HTML 5, PHP, LMS, Open Source, SBC.

Introducción

Durante el año 2020, el COVID-19 provocó el cierre de múltiples lugares concurridos, entre ellos los centros educativos, ya que entre las medidas que fueron adoptadas por las naciones, la más importante de ellas fue el confinamiento global para detener la propagación descontrolada. Esto aceleró un proceso de transformación digital que ha pasado de inevitable, a indispensable a fin de evitar una disrupción en las rutinas.

La contingencia sanitaria del SARS-CoV-2 ha puesto un gran reto educacional que trajo cambios significativos en el funcionamiento tradicional de las escuelas, lo que desencadenó la transición del modelo educativo presencial a distancia, el cual, implica diferentes actividades, así como metodologías, para las cuales, la cátedra convencional no se encontraba preparada. Tanto docentes como estudiantes adquirieron actividades adicionales a las regulares, es de notar, por lo tanto, que actualmente es un requisito necesario conocer y dominar herramientas digitales, recursos educativos.

Para aprender el uso de dichas herramientas y plataformas, los docentes tomaron sesiones en línea con expertos en el tema, capacitándose a la par que instruyeron a sus alumnos en el uso de estas. Los alumnos a su vez poseen conocimiento previo de las TIC's de forma intuitiva debido al entorno tecnológico en el que se desenvuelven, pese a ello, este conocimiento no fue, ni es, mensurable. Ahora, el aprendizaje enfrenta como una de sus problemáticas, no ser regularizable.

Sin contar con una base de conocimientos específica, resulta complejo el desarrollo de actividades de forma síncrona como se realizaba de forma presencial.Adicional a esta carencia de punto de partida, se le suma el entorno distinto de cada estudiante porque no se desenvuelven en un ambiente centralizado ni controlado (salón de clases con su figura de autoridad) lo que repercute en un descontrol de actividades y una clara merma en el aprendizaje obtenido por los estudiantes.Resulta imperante regularizar esta situación. Para tener cierto control de la misma, se ha fomentado tener sesiones con actividades asíncronas para los alumnos como también la gamificación de las actividades que integran una asignatura.

[1]Eudar Escobar Elías, Docente del Instituto Tecnológico de Veracruz, eudar@hotmail.com, (autor corresponsal)
[2]Sergio Alarcón Rodriguez, Docente del Instituto Tecnológico de Veracruz, sergioalarxon@gmail.com
[3]Dafne Angélica Hernández Vázquez, Ingeniero de Software en INTEL, dafnehdzvzq@gmail.com
[4]Omar Meza Vázquez, Ingeniero de Control y Monitoreo de Operaciones de TI, omar.mvazquez@outlook.com
[5]Dolores Vázquez Trujillo, Docente de la Universidad Veracruzana, dovazquez@uv.mx
[6]Arturo Pérez Rendón, Docente del Instituto Tecnológico de Veracruz, arturoperezrendon@gmal.com

Resulta imperante regularizar esta situación. Para tener cierto control de la misma, se ha fomentado tener sesiones con actividades asíncronas para los alumnos como también la gamificación de las actividades que integran una asignatura. A diferencia de otras soluciones tecnológicas que tienen como requisito el uso obligatorio de internet en este caso las actividades pueden ser realizadas de forma asíncrona, ya que no se necesita conexión a internet.

Se fomentaron este tipo de sesiones debido a la diversidad de contextos (ambientes) entre individuos que toman sesiones en línea, la problemática es que los que carecen de un buen servicio o del servicio de internet, no pueden realizar las actividades de forma síncrona.

Con lo que esta tecnología provee una gran ventaja, en los lugares donde no existe cobertura o el servicio no es de buena calidad.

Con el uso de plataformas y TIC'S se puede tener un control en la implementación y realización de actividades asíncronas logrando combatir la problemática de estudiantes que por diversos factores como la localidad, situación económica o recursos puedan realizar actividades al mismo tiempo que otros respetando cierto límite de tiempo.

Es importante tener en cuenta las razones para ofrecer a la población estudiantil clases a distancia mediante tecnologías en línea, que van más allá de periodos de confinamiento, esto nos permite una mayor efectividad educativa con refuerzos interactivos como complemento a las clases que permiten al alumno practicar las 24 horas del días los 365 días del año y avanzar a su propio ritmo dentro de una periodicidad, esto conlleva a la flexibilidad en los horarios ya que se puede obtener acceso desde cualquier ubicación e inclusive sin contar con una conexión a internet, asistiendo los estudiantes a sus sesiones cómodamente desde sus dispositivos (celular, tableta y/o computadora), permitiendo lo antes mencionado mayor aprovechamiento del tiempo de los catedráticos y una retroalimentación directa de su profesor por parte del estudiante.

El aprendizaje (asíncrono) puede ser facilitado por las TIC's. A través de Internet, y diferentes Plataformas E-learning, el proceso educativo puede tornarse mucho más versátil y además se puede trabajar en todo tipo de materias y proyectos.

"Las plataformas e-learning, plataformas educativas o entornos virtuales de enseñanza y aprendizaje (VLE), constituyen, actualmente, esta realidad tecnológica creada en Internet y que da soporte a la enseñanza y el aprendizaje universitarios. En estos momentos podemos afirmar que su uso ha transformado una gran parte de los espacios de enseñanza tradicionales en espacios virtuales de enseñanza y aprendizaje2 (EVA)." De acuerdo con Ana Fernández-Pampillón Cesteros (Universidad Complutense de Madrid, 2019).

La tecnología en los sistemas embebidos es cada vez más poderosa y de bajo consumo energético esto gracias a su arquitectura ARM en el procesador, que se enfoca en mantener el número de instrucciones en la menor cantidad posible mientras que también mantiene esas instrucciones tan simples como se pueda. Las instrucciones sencillas tienen algunas ventajas tanto para los ingenieros de hardware como para los ingenieros de software. Como las instrucciones son simples, los circuitos necesarios requieren menos transistores, resultando en más espacio para el chip y menos espacio en la tarjeta embebida. Se encuentra hoy en día en la mayor parte de productos que contienen microprocesadores para dotarlos de cierta inteligencia.

El objetivo del presente proyecto es demostrar el uso de un sistema embebido como estrategia para disminuir los índices de reprobación y evitar la posible deserción estudiantil, aplicado como línea de acción para la eficiencia, eficacia, versatilidad y la facilidad de recolección de datos en las actividades de la materia Programación Web a cursar durante su semestre del estudiante.

La problemática principal está enfocada en los estudiantes de nivel universitario debido a los altos índices de reprobación existentes en este nivel, ocasionados principalmente por la transición forzada de clases presenciales a virtuales durante la pandemia Covid-19. Adicionalmente cabe mencionar que, al estar los estudiantes en diferentes entornos, existen más factores que perjudican su aprendizaje entre ellos los más destacables y frecuentes: carencia de equipo de cómputo y el servicio de internet deficiente o nulo.

Al final se describen los resultados obtenidos en la implementación de la Raspberry Pi Zero w al cursar la materia de Programación Web, así como las ventajas de dicha estrategia destacando la arquitectura ARM, la cual cuenta con distribución Raspbian, con un costo mínimo de mantenimiento y contrasta con el estándar superior de seguridad.

Descripción de Metodología

El internet hoy en día es la fuente más accesible e importante para la asistencia de hardware con distribuciones de software libre, debido a ello, este proyecto en cuestión está fundamentado en gran parte de la información publicada en libros digitales, documentos de asistencia, foros de discusión, blogs, páginas web y revistas digitales.

Para poder implementar las funcionalidades de este proyecto, se llevarán a cabo las siguientes actividades:

Identificación y Análisis del Hardware

La identificación del hardware y su análisis son fundamentales para la ejecución de este proyecto, se requieren equipos de hardware de bajo costo que cumplan con los requisitos necesarios para cubrir las principales necesidades del proyecto.



Figura 1 Raspberry Py Zero w

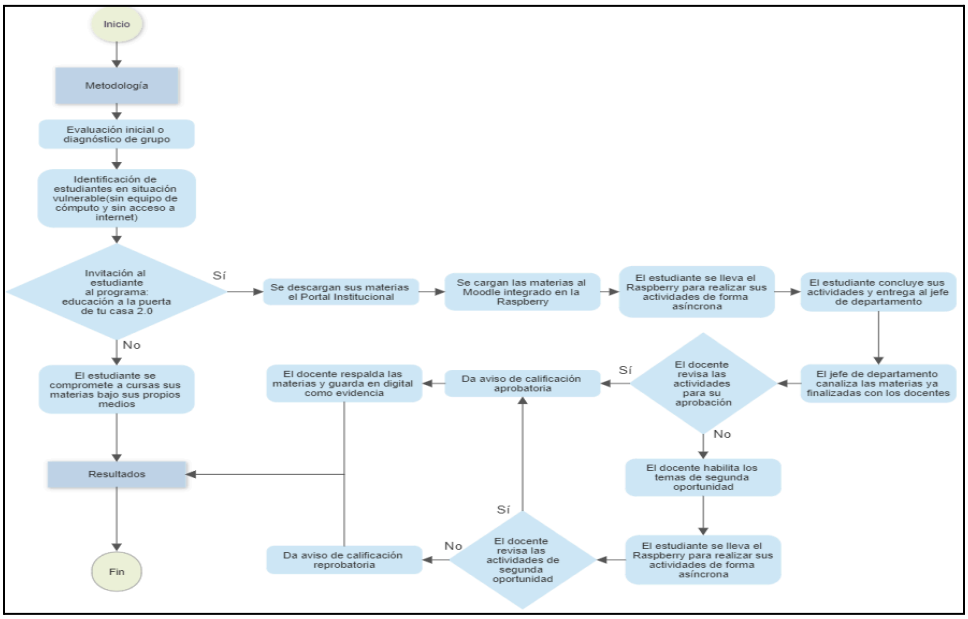
Todas las especificaciones técnicas el modelo de Raspberry Pi Zero w:

- CPU: Mono Core Broadcomm BCM2835 ARM11 a 1GHz el mismo que la Raspberry Pi 1 pero con 300MHz más
- GPU: Video Core IV GPU
- RAM: 512MB
- Almacenamiento: ranura microSD
- Vídeo: salida mini HDMI y vídeo compuesto sin montar el conector
- USB: 1 x micro USB OTG datos
- Wi-Fi y Bluetooth usando el mismo chip que la Raspberry Pi 3, el Cypress CYW43438 con soporte de 802.11n Wireless LAN y
- Bluetooth 4.0.
- GPIO: 40 pin sin montar el conector
- Alimentación: 5V vía micro USB
- Dimensiones: 65mm x 30mm x 5mm

La Raspberry Pi Zero cumple con los requisitos básicos para la implementación de un aula virtual, debido a la utilidad de servidor web que se le otorgará, este ofrece una capacidad de procesamiento ideal y un soporte de software muy amplio en diversos sistemas Open Source (Linux). Se requiere de un Raspberry Pi Zero w.

el estudiante, para ser parte del programa educación a la puerta de tu casa, para ello finalmente ser evaluado a lo largo del periodo escolar de manera eficiente.

En el siguiente diagrama se muestra el proceso por el cual se debe de pasar el estudiante, para ser parte del programa educación a la puerta de tu casa, para ello finalmente ser evaluado a lo largo del periodo escolar de manera eficiente.



Selección y Análisis del Software

En este punto de selección y evaluación del software se utilizó Raspbian, un sistema basado en Debian siendo este una distribución Open Source de GNU/Linux, incluye interfaz gráfica lo cual beneficia el rendimiento y el espacio de memoria; con ello se obtuvo la libertad de configurar cualquier aspecto del sistema operativo por medio de su CLI. En el desarrollo del servidor se procedió a la instalación de Apache2 fungiendo este como el Servidor Web que se utilizó en Raspbian; posteriormente se requirió de un Sistema Gint, configurando nuestro dispositivo como servidor de DHCP permitiendo que otros dispositivos se conecten al Wi-Fi del sistema embebido para darles acceso al Moodle. Una vez realizado lo anterior, se conectó vía Wi-Fi a la red con el nombre MOODestor Base de Datos el cual es MySQL que tiene por derivado para GNU-Linux, a MariaDB. Por cuestiones de practicidad durante la instalación y configuración de los softwares antes mencionados, se utilizó MTPuTTY un software que facilita la opción de gestionar múltiples terminales por conexión SSH.

Como plataforma E-learning Open Source visible en el servidor y para cargar la base de datos, se requirió de Moodle en su versión 3.10.1, el cual durante su instalación se necesitará previamente MySQL (MariaDB) y Módulos específicos de PHP 7.4.3 Se iniciará la instalación por medio de Git, se le otorgó permisos de super usuario -R 755 y -R g+s a la carpeta de Apache2 y al archivo Moodle data.

Posteriormente montamos el servidor de Access PoLE en el navegador que se tenga por defecto desde cualquier dispositivo, se direcciona la IP 10.0.0.1 del servidor seguido de /moodle. Para verificar que el procedimiento hecho previamente fue correcto.

Con todo lo anterior mencionado, Moodle se habrá instalado correctamente, se crea el usuario del estudiante para su acceso a la plataforma y se carga la materia con sus respectivas actividades a cursar por el estudiante de Programación Web de 7° semestre de la carrera de Ingeniería en Sistemas Computacionales.

Durante la etapa de Quality Assurance (QA), una vez que el esquema de todo el sistema quedó implementado, se le realizaron las pruebas pertinentes para corroborar el correcto funcionamiento del proyecto.

Posteriormente se realizó el armado donde se montó en una carcasa prediseñada. Se modeló, diseñó y construyó la carcasa a medida para insertar y sujetar la placa Raspberry Pi y todos los componentes necesarios siguiendo los requerimientos del proyecto. En específico para disminuir el calentamiento, con el fin de facilitar la gestión del hardware y dejarlo en condiciones óptimas para su funcionamiento. Esto último permite, alargar la vida útil del dispositivo.

Etapa de pruebas



Figura 2. Case Raspberry Pi Zero W
Fuente: Elaboración propia



Figura 3. Montaje Raspberry Pi Zero W case
Fuente: Elaboración propia

Una vez armado el dispositivo, se procedió a acceder de forma remota vía wifi, para la visualización del estado actual del Raspberry Pi Zero w, mediante PuTTY, se comprobó que los demonios (servicios) se encontraban correctamente configurados y funcionale**s.**

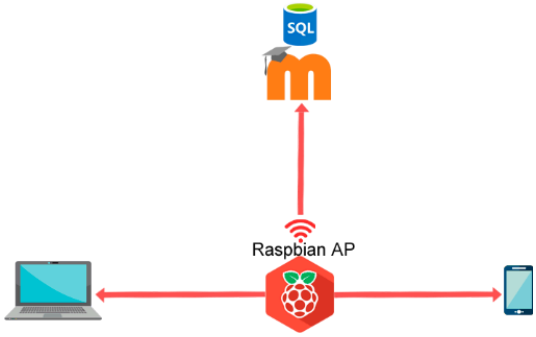


Diagrama SEQ Diagrama_ * ARABIC 2 - Esquema del proyecto



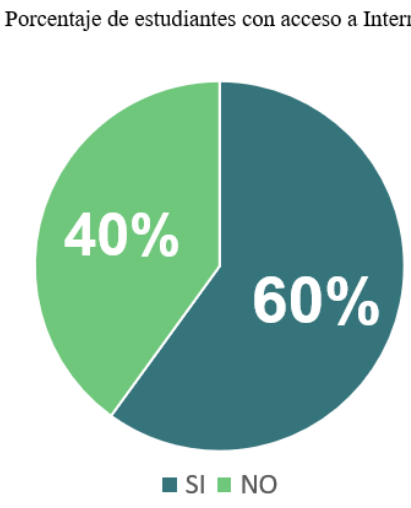
Figura 4 - Interfaz del Moodle implementado

De acuerdo con el diagrama esquemático anterior, se realizaron las pruebas necesarias y pertinentes para el correcto funcionamiento del proyecto.

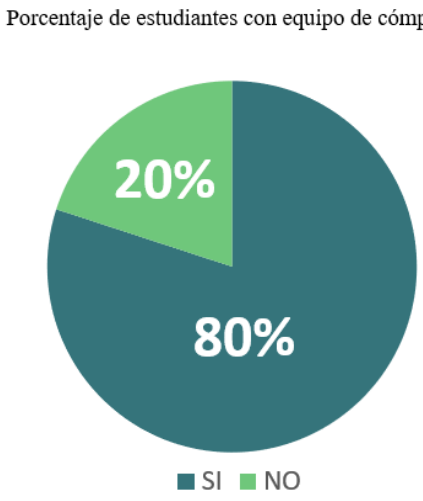
Se procedió a acceder a la plataforma Moodle, de forma remota desde un dispositivo, para visualizar el curso de Programación Web, comprobando con ello que el material del curso era accesible y sin problemas de interoperabilidad ni de accesibilidad. (Figura 4).

La materia de Programación Web consta de 10 estudiantes de los cuales el 40% no cuenta con acceso a internet, y el 20 % no cuenta con equipo de cómputo. Adicionalmente, de lo último mencionado estos estudiantes forman parte del 40 % que no cuentan con internet. (Gráfica 1 y 2).

A continuación, se muestran de manera gráfica los resultados en las calificaciones de los estudiantes de la materia de Programación Web durante el periodo de febrero 2020 - agosto 2020, que abarcó los inicios de la contingencia. Posteriormente, al finalizar el curso del periodo agosto 2020 - enero 2021 se obtuvieron las siguientes calificaciones en la materia impartida mediante la tecnología Raspberry Pi Zero w, obteniendo resultados favorables y con un promedio en la calificación superior que los estudiantes que acceden al Moodle de manera tradicional con internet. (Tabla 1, Gráfica 3, Tabla 2, Gráfica 4 y Gráfica 5).



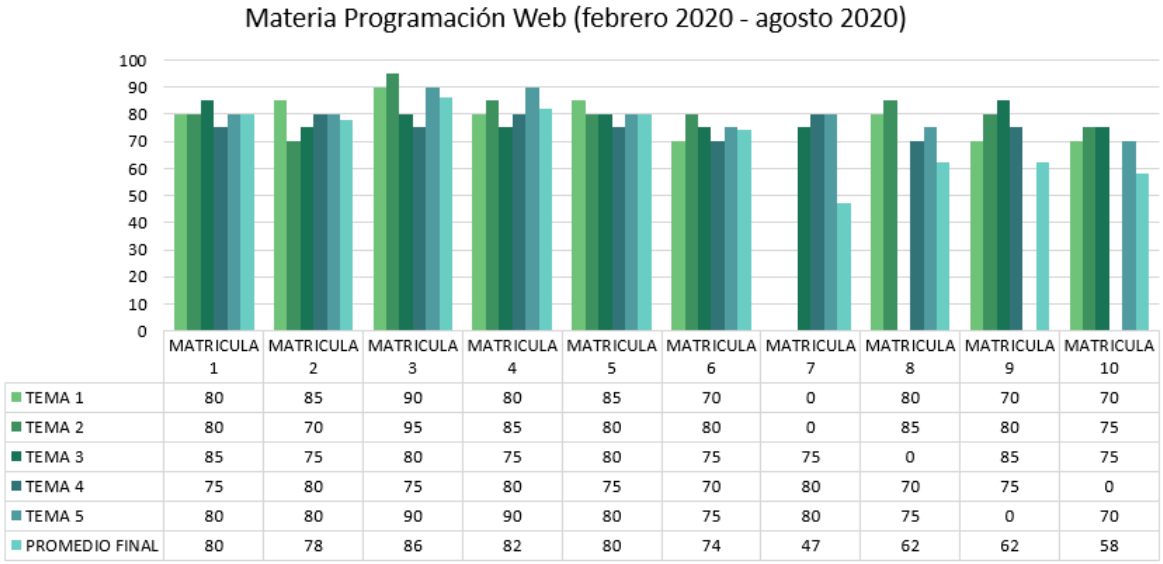
Gráfica 1 - Porcentaje de estudiantes que cuentan con acceso a internet



Gráfica 2 - Porcentaje de estudiantes que cuentan con equipo de computo

N°	MATRICULA	NOMBRE DEL ESTUDIANTE	CARRERA	TEMA 1	TEMA 2	TEMA 3	TEMA 4	TEMA 5	PROMEDIO FINAL
1	MATRICULA 1	ESTUDIANTE 1	ISC-SAB	80	80	85	75	80	80
2	MATRICULA 2	ESTUDIANTE 2	ISC-SAB	85	70	75	80	80	78
3	MATRICULA 3	ESTUDIANTE 3	ISC-SAB	90	95	80	75	90	86
4	MATRICULA 4	ESTUDIANTE 4	ISC-SAB	80	85	75	80	90	82
5	MATRICULA 5	ESTUDIANTE 5	ISC-SAB	85	80	80	75	80	80
6	MATRICULA 6	ESTUDIANTE 6	ISC-SAB	70	80	75	70	75	74
7	MATRICULA 7	ESTUDIANTE 7	ISC-SAB	0	0	75	80	80	47
8	MATRICULA 8	ESTUDIANTE 8	ISC-SAB	80	85	0	70	75	62
9	MATRICULA 9	ESTUDIANTE 9	ISC-SAB	70	80	85	75	0	62
10	MATRICULA 10	ESTUDIANTE 10	ISC-SAB	70	75	75	0	70	58

Tabla 1 Promedios de estudiantes en la materia de Programación Web en el periodo Febrero 2020 – Agosto 2020 (con uso de Raspberry Pi Zero w)

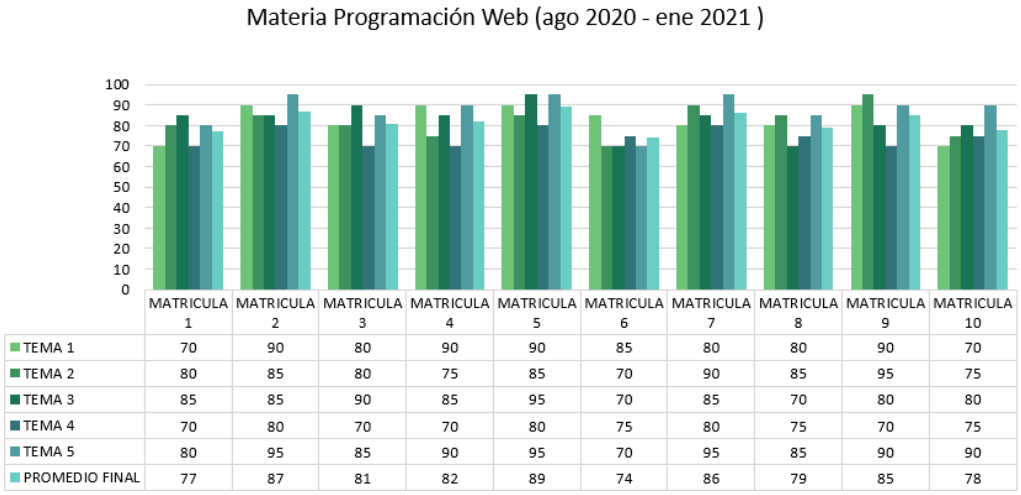


	MATRICULA 1	MATRICULA 2	MATRICULA 3	MATRICULA 4	MATRICULA 5	MATRICULA 6	MATRICULA 7	MATRICULA 8	MATRICULA 9	MATRICULA 10
TEMA 1	80	85	90	80	85	70	0	80	70	70
TEMA 2	80	70	95	85	80	80	0	85	80	75
TEMA 3	85	75	80	75	80	75	75	0	85	75
TEMA 4	75	80	75	80	75	70	80	70	75	0
TEMA 5	80	80	90	90	80	75	80	75	0	70
PROMEDIO FINAL	80	78	86	82	80	74	47	62	62	58

Gráfica 3 – Resultados en la materia de Programación Web durante el periodo Febrero 2020 – Agosto 2020 (con uso de Raspberry Pi Zero w)

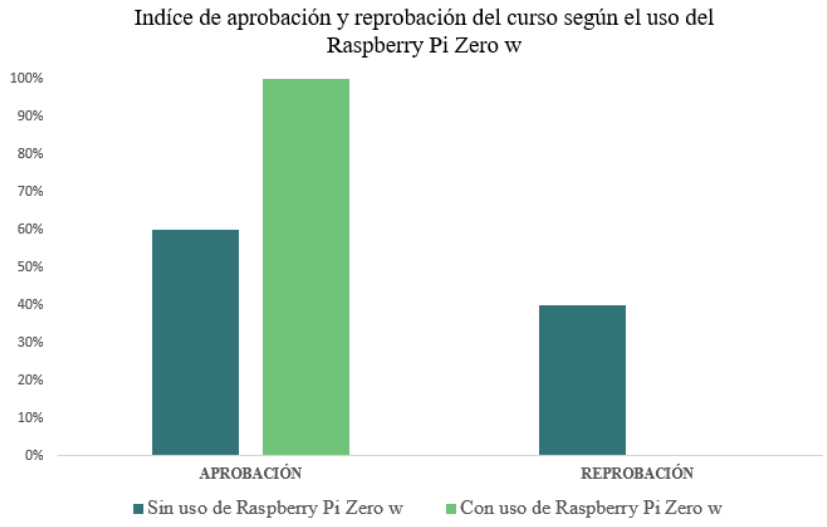
N°	MATRICULA	NOMBRE DEL ESTUDIANTE	CARRERA	TEMA 1	TEMA 2	TEMA 3	TEMA 4	TEMA 5	PROMEDIO FINAL
1	MATRICULA 1	ESTUDIANTE 1	ISC-SAB	70	80	85	70	80	77
2	MATRICULA 2	ESTUDIANTE 2	ISC-SAB	90	85	85	80	95	87
3	MATRICULA 3	ESTUDIANTE 3	ISC-SAB	80	80	90	70	85	81
4	MATRICULA 4	ESTUDIANTE 4	ISC-SAB	90	75	85	70	90	82
5	MATRICULA 5	ESTUDIANTE 5	ISC-SAB	90	85	95	80	95	89
6	MATRICULA 6	ESTUDIANTE 6	ISC-SAB	85	70	70	75	70	74
7	MATRICULA 7	ESTUDIANTE 7	ISC-SAB	80	90	85	80	95	86
8	MATRICULA 8	ESTUDIANTE 8	ISC-SAB	80	85	70	75	85	79
9	MATRICULA 9	ESTUDIANTE 9	ISC-SAB	90	95	80	70	90	85
10	MATRICULA 10	ESTUDIANTE 10	ISC-SAB	70	75	80	75	90	78

Tabla 2 Promedios de estudiantes en la materia de Programación Web en el periodo Agosto 2020 – Febrero 2021 (con uso de Raspberry Pi Zero w)



	MATRICULA 1	MATRICULA 2	MATRICULA 3	MATRICULA 4	MATRICULA 5	MATRICULA 6	MATRICULA 7	MATRICULA 8	MATRICULA 9	MATRICULA 10
TEMA 1	70	90	80	90	90	85	80	80	90	70
TEMA 2	80	85	80	75	85	70	90	85	95	75
TEMA 3	85	85	90	85	95	70	85	70	80	80
TEMA 4	70	80	70	70	80	75	80	75	70	75
TEMA 5	80	95	85	90	95	70	95	85	90	90
PROMEDIO FINAL	77	87	81	82	89	74	86	79	85	78

Gráfica 4 – Resultados en la materia de Programación Web durante el periodo Agosto 2020 – Enerio 2021 (con uso de Raspberry Pi Zero w)



Gráfica 5 – Índice de aprobación y reprobación del curso programación web según el uso de Raspberry Pi Zero w)

Conclusiones

Hoy en día la tecnología ha diversificado las formas de enseñanza educativa a tal grado de facilitar cada vez más la inclusividad para los estudiantes de todos los niveles, especialmente los de nivel universitario de diferentes ambientes. Gracias a que los componentes tecnológicos son cada vez más asequibles y compactos, el uso de ellos es cada vez más frecuente en la aplicación de soluciones innovadoras del ámbito educativo. Con el presente proyecto se obtuvo una reducción de los índices de reprobación hasta en un 40% con respecto a semestres anteriores, como se puede apreciar en las gráficas anteriormente presentadas. Esto demostró la versatilidad y el apoyo a los estudiantes vulnerables haciendo uso de las tecnologías de los sistemas embebidos y su funcionamiento como estrategia para disminuir el índice de reprobación y deserción, demostrando que la solución es factible. Asegurándose la educación inclusiva con calidad, equidad y excelencia. Haciendo efectivos los principios de igualdad y oportunidades, no discriminación y accesibilidad universal. Todos ellos son principios complementarios e inseparables de la educación.

Recomendaciones

Se recomienda la instalación de un botón de encendido y apagado configurado desde terminal, evitando con ello posibles corrupciones en el sistema que pueden afectar las configuraciones establecidas.

Así mismo se sugiere, configurar de forma predeterminada el arranque del SO por CLI (Terminal), para la reducción de carga en el procesamiento, obteniendo mayor rendimiento y eficiencia.

References

1. Ray, R. (2018); Raspberry Pi (2018): Guía Paso a Paso Para Dominar El Hardware Y Software de Raspberry Pi 3, CreateSpace Independent Publishing Platform.
2. Cobo, A., Gómez, P., Pérez, D. and Rocha, R. (2005). PHP y MySQL. Madrid: Ediciones Díaz de Santos.
3. Moodledocs (2019). Instalando Moodle en distribuciones basadas en Debian. Disponible en: Moodledocs.: Recuperado de https://docs.moodle.org/37/en/Main_page
4. Drake, M. (2018). How To Install MySQL on Ubuntu 18.04. Disponible en: DigitalOcean, LLC: Recuperado de: https://www.digitalocean.com/community/tutorials/how-to-install-mysql-on-ubuntu-18-04.
5. Kabir, M. (2003). La biblia de Servidor Apache 2. Madrid: Anaya Multimedia.

DHCP SNOOPING: UNA SOLUCIÓN EFICAZ PARA MITIGAR ATAQUES DHCP.

Eudar Escobar Elías[1], Sergio Alarcón Rodríguez[2], Luis Mario Correa Lozano[3], Diego Nava Taguada[4], Héctor Pérez Ortiz[5] ,César Augusto Rogel Gálvez[6], Arturo Pérez Rendón[7].

Resumen. El protocolo DHCP (Dynamic Host Configuration Protocol) es esencial en la administración de redes locales (LAN), pero su explotación por atacantes puede resultar en amenazas como el secuestro de direcciones IP o la propagación de malware. DHCP Snooping, una función de seguridad, filtra mensajes DHCP de puertos no autorizados, evitando ataques maliciosos. Este artículo explora la implementación de DHCP Snooping en la red LAN del Tecnológico de Veracruz para mitigar riesgos de seguridad y mejorar la gestión de direcciones IP

Palabras clave—DHCP, DHCP Snooping, LAN, redes.33

Introducción

El Tecnológico de Veracruz se destaca como un centro educativo comprometido con la excelencia en la formación de profesionales en diversas disciplinas tecnológicas. La infraestructura de red desempeña un papel fundamental en la facilitación de las actividades diarias, y su seguridad y confiabilidad son prioritarias para garantizar un entorno digital seguro y eficiente. El Protocolo de Configuración Dinámica de Host (DHCP) es un componente crítico en la administración de direcciones IP en una red local (LAN). Sin embargo, la dinámica de DHCP también lo convierte en un vector potencial para amenazas de seguridad, como ataques de suplantación de identidad o la asignación no autorizada de direcciones IP. En este contexto, la implementación de DHCP Snooping emerge como una estrategia esencial para fortalecer la seguridad de la red.Este artículo explora la implementación de DHCP Snooping en la red LAN del Tecnológico de Veracruz como una medida proactiva para mitigar riesgos de seguridad y mejorar la eficiencia en la gestión de direcciones IP.

Este artículo explora la implementación de DHCP Snooping en la red LAN del Tecnológico de Veracruz como una medida proactiva para mitigar riesgos de seguridad y mejorar la eficiencia en la gestión de direcciones IP.

DHCP Snooping es una característica de seguridad diseñada para prevenir ataques maliciosos en la red al supervisar y controlar el proceso de asignación de direcciones IP mediante el Protocolo de Configuración Dinámica de Host (DHCP). Al habilitar DHCP Snooping, se valida la información proveniente de servidores DHCP autorizados y se filtra o bloquea cualquier mensaje DHCP proveniente de fuentes no autorizadas. Esto no solo protege contra posibles ataques de suplantación de identidad, como el DHCP Spoofing, sino que también mejora la eficiencia al garantizar que las direcciones IP se asignen de manera segura y conforme a las políticas establecidas en la red del Tecnológico de Veracruz.

Descripción Del Método

Para poder implementar el DHCP Snooping en la red LAN del Instituto Tecnológico de Veracruz primero se llevó a cabo una prueba pequeña para poder confirmar que el método utilizado será eficiente, la prueba se basó en utilizar 2 servidores DHCP conectados a un switch el cual fue configurado con DHCP Snooping para que este solo pueda recibir un entorno de red seguro y eficiente tráfico DHCP por el puerto configurado como puerto de confianza esto evitó que el servidor malicioso de DHCP no pueda enviar tráfico a través del switch para realizar un ataque a la red LAN. Una vez implementado esta configuración las computadoras clientes solo reciben configuraciones IP dadas por el servidor autorizado por el puerto de confianza. Dada por terminada la prueba se implementó la configuración a todos los switches que pertenecen a la escuela.

[1]Eudar Escobar Elías, Docente del Instituto Tecnológico de Veracruz, eudar@hotmail.com, (autor corresponsal)
[2]Sergio Alarcón Rodriguez, Docente del Instituto Tecnológico de Veracruz,sergioalarxon@gmail.com
[3]Luis Mario Correa Lozano, Estudiante del Instituto Tecnológico de Veracruz,luiiscorrea17@gmail.com
[4]Diego Nava Taguada, Estudiante del Instituto Tecnológico de Veracruz,diego.nava.t2001@gmail.com
[5]Héctor Pérez Ortiz, Docente del Instituto Tecnológico de Veracruz,hector.po@veracruz.tecnm.mx
[6]César Augusto Rogel Gálvez, Docente del Instituto Tecnológico de Veracruz,cesar.rg@veracruz.tecnm.mx
[7]Arturo Perez Rendón, Docente del Instituto Tecnológico de Veracruz, arturoperezrendon@veracruz.tecnm.mx

Materiales Y Recursos

La infraestructura de red del Tecnológico de Veracruz se compone de una red extensa de switches distribuidos estratégicamente por toda la institución. Estos switches están interconectados mediante cables de fibra óptica, lo que facilita una comunicación eficiente entre los distintos edificios y áreas administrativas. Para gestionar la asignación dinámica de direcciones IP a los dispositivos conectados a la red, se ha implementado un servidor DHCP centralizado.Este servidor DHCP desempeña un papel fundamental al proporcionar direcciones IP de manera dinámica a los dispositivos, simplificando así la configuración de red para los usuarios. Sin embargo, también presenta desafíos en términos de seguridad.La asignación dinámica a través del Protocolo de Configuración Dinámica de Host (DHCP) podría ser vulnerable a posibles ataques, como la suplantación de identidad (spoofing) o la asignación maliciosa de direcciones IP. Por lo tanto, es importante implementar medidas de seguridad robustas, como la autenticación de dispositivos y la monitorización activa de la red, para mitigar posibles amenazas y garantizar la integridad y la seguridad de la infraestructura de red del Tecnológico de Veracruz. La utilización de cables de fibra óptica contribuye a una mayor velocidad y confiabilidad en la comunicación, pero se debe poner especial atención en fortalecer las capas de seguridad para mantener



Ilustración 1 Arquitectura DHCP Fuente: Propia

La primera fase de nuestro enfoque metodológico se centró en una evaluación minuciosa de la topología de red que es utilizada actualmente en el instituto. Específicamente, se revisaron las especificaciones técnicas de los switches principales, con un énfasis en su capacidad para admitir y gestionar eficientemente el protocolo DHCP Snooping. La elección de modelos, como los switches de la serie Catalyst de Cisco, se basó en su capacidad probada para integrar funciones avanzadas de seguridad sin sacrificar el rendimiento general de la red.Este análisis no se limitó únicamente a la capacidad de los switches. Se extendió al router que facilitan la comunicación entre las distintas subredes del Tecnológico de Veracruz. Se confirmó que este dispositivo también es compatible con DHCP Snooping y se evaluó su capacidad para gestionar la seguridad de las interconexiones entre las subredes.La configuración precisa de DHCP Snooping en los switches seleccionados fue la fase siguiente de nuestro proceso. Esto involucró la activación de DHCP Snooping a nivel de switch, la designación de interfaces específicas como confiables o no confiables, y la garantía de una sincronización adecuada con la base de datos DHCP Snooping. Cabe destacar que, para salvaguardar la integridad de las asignaciones de direcciones IP, las interfaces configuradas como troncales fueron designadas como confiables, mientras que las interfaces que conectan usuarios y dispositivos finales fueron designadas como no confiables.

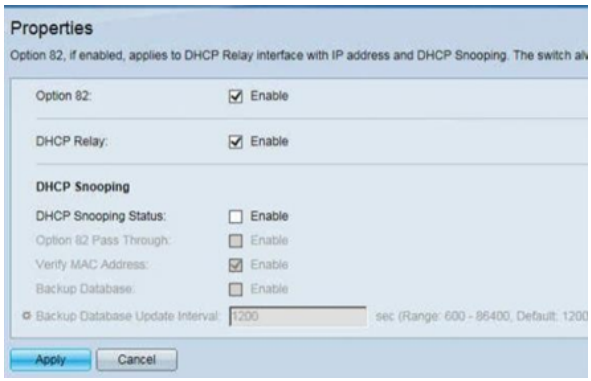


Ilustración 2 Configuración DHCP Fuente: Propia

Esta etapa no solo implicó una configuración estática. Se implementó un mecanismo de actualización dinámica para adaptarse a cambios en la topología de la red, asegurando la persistencia de la seguridad incluso frente a modificaciones en la infraestructura.Con DHCP Snooping plenamente operativo, se sometió a la red a pruebas de estrés simulando cargas de tráfico intensas en diferentes áreas de la institución. Los resultados demostraron un impacto mínimo en el rendimiento general, validando la eficacia de DHCP Snooping en la mitigación de amenazas sin comprometer la velocidad y la eficiencia de la red.

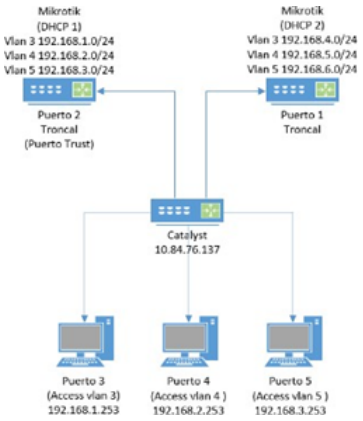


Ilustración 3 Diagrama prueba Fuente: Propia

La fase de post-implementación no se limitó al rendimiento. Se realizaron auditorías de seguridad regulares para evaluar la efectividad de DHCP Snooping en la detección y prevención de posibles ataques. Estas auditorías incluyeron escaneos exhaustivos de la red en busca de anomalías, verificación de logs y análisis forense en caso de eventos sospechosos.Este enfoque integral y detallado en los materiales y métodos garantiza una implementación exitosa de DHCP Snooping en la red LAN del Tecnológico de Veracruz, proporcionando un entorno seguro y eficiente para las actividades académicas y administrativas. La combinación de evaluaciones técnicas, configuraciones precisas y monitoreo continuo se presenta como un modelo robusto para fortalecer la seguridad de la infraestructura de red en entornos educativos de gran envergadura.

Resultados Y Discusión

La implementación de DHCP Snooping en la red LAN del Tecnológico de Veracruz arrojó resultados significativos en términos de seguridad y estabilidad de la red. A continuación, se presentan los hallazgos clave derivados de la ejecución de este protocolo de seguridad:

Detección Efectiva de Actividades Anómalas:
La función de monitoreo constante reveló una detección efectiva de actividades anómalas relacionadas con DHCP. Los registros detallados evidenciaron la identificación oportuna de intentos de suplantación de identidad y la presencia de paquetes DHCP maliciosos.

Reducción de Asignaciones No Autorizadas de Direcciones IP:
La configuración precisa de interfaces confiables y no confiables en los switches condujo a una notable reducción en las asignaciones no autorizadas de direcciones IP. DHCP Snooping demostró ser eficaz al bloquear intentos de asignación de direcciones por dispositivos no autorizados, fortaleciendo así la integridad de la red.

Impacto Mínimo en el Rendimiento:
Las pruebas de estrés realizadas posteriormente a la implementación demostraron un impacto mínimo en el
rendimiento general de la red. La capacidad de los switches seleccionados para gestionar eficientemente DHCP Snooping se tradujo en una mitigación efectiva de riesgos sin sacrificar la velocidad de la red.La implementación exitosa de DHCP Snooping en la red LAN del Tecnológico de Veracruz representa un avance significativo en términos de seguridad y gestión de direcciones IP. Los resultados obtenidos refuerzan la relevancia y eficacia de esta medida de seguridad en un entorno educativo de gran escala. A continuación, se discuten varios aspectos clave:

Adaptabilidad a Cambios en la Red:
La configuración dinámica de DHCP Snooping demostró ser altamente adaptable a cambios en la topología de la red. La capacidad de actualizar automáticamente las configuraciones en respuesta a modificaciones en la infraestructura garantiza una seguridad continua sin intervención manual constante. Integración Transparente con la Operatividad Diaria: La implementación de DHCP Snooping se integró de manera transparente con las operaciones diarias de la red. Los usuarios finales experimentaron una asignación de direcciones IP sin interrupciones, mientras que el protocolo trabajaba silenciosamente en segundo plano para garantizar la integridad y seguridad de las asignaciones.

Necesidad de Educación y Concientización:
A pesar de la eficacia de DHCP Snooping, se destacó la importancia de la educación y concientización del personal y los usuarios finales. La comprensión de las políticas de seguridad y la conciencia sobre las posibles interacciones con DHCP Snooping son cruciales para mantener un ambiente de red seguro y eficiente.

Continuidad en la Monitorización:
La monitorización continua se identificó como un elemento clave en el mantenimiento de la seguridad de
la red. La implementación exitosa no es un punto final, sino el comienzo de un proceso continuo de evaluación y ajuste para hacer frente a las amenazas emergentes.

Conclusiones

La implementación exitosa de DHCP Snooping en la red LAN del Tecnológico de Veracruz representa un hito significativo en la mejora de la seguridad y estabilidad de la infraestructura de red de la institución. A lo largo de este estudio, hemos explorado las razones fundamentales para adoptar DHCP Snooping, desde la dinámica de la asignación de direcciones IP hasta los desafíos específicos que enfrenta una institución educativa de gran escala. Los resultados obtenidos y las lecciones aprendidas durante este proceso subrayan la importancia crítica de esta medida de seguridad en el contexto específico del Tecnológico de Veracruz.
En primer lugar, la implementación de DHCP Snooping ha demostrado su capacidad para detectar de manera efectiva actividades anómalas dentro de la red. La función de monitoreo constante ha permitido una identificación temprana de intentos de suplantación de identidad y la presencia de paquetes DHCP maliciosos. Este nivel de visibilidad proporciona a los administradores de red la capacidad de responder proactivamente a posibles amenazas, mitigando riesgos antes de que se conviertan en problemas significativos.

La reducción substancial en las asignaciones no autorizadas de direcciones IP constituye otro logro clave derivado de la implementación de DHCP Snooping. La configuración precisa de interfaces confiables y no confiables ha actuado como una barrera efectiva contra dispositivos no autorizados, mejorando la integridad de la red y garantizando que las direcciones IP se asignen únicamente a dispositivos legítimos.Es esencial destacar que estos beneficios se han logrado sin comprometer el rendimiento general de la red. Las pruebas de estrés realizadas han confirmado que la implementación de DHCP Snooping no solo es efectiva en términos de seguridad, sino que también se integra sin problemas en el entorno operativo diario. La estabilidad y velocidad de la red se han mantenido a niveles óptimos, validando la elección de switches y la configuración específica implementada.

La adaptabilidad de DHCP Snooping a cambios en la red se presenta como un elemento clave para su éxito continuo. La capacidad de actualizar dinámicamente las configuraciones en respuesta a modificaciones en la topología de la red asegura que la seguridad se mantenga constante, incluso en un entorno dinámico como el del Tecnológico de Veracruz.
No obstante, es crucial reconocer que la implementación de medidas de seguridad como DHCP Snooping no puede operar en un vacío. La educación y concientización del personal y los usuarios finales son elementos esenciales para mantener un entorno de red seguro. La comprensión de las políticas de seguridad y la colaboración continua son fundamentales para optimizar la efectividad de DHCP Snooping y garantizar su éxito a largo plazo.

En conclusión, la implementación de DHCP Snooping en la red LAN del Tecnológico de Veracruz se presenta como un modelo ejemplar para otras instituciones educativas y entidades de gran envergadura. Este estudio no solo subraya la eficacia de DHCP Snooping en la mejora de la seguridad de la red, sino que también destaca la importancia de la planificación meticulosa, la adaptabilidad y la colaboración continua en la gestión de la infraestructura de red en un entorno educativo
dinámico.A medida que avanzamos hacia un futuro digital cada vez más interconectado, la implementación de medidas de seguridad como DHCP Snooping se vuelve no solo una necesidad, sino un imperativo para salvaguardar la integridad de nuestras instituciones educativas y garantizar la continuidad de las operaciones en un entorno cibernético en constante evolución

Referencias Bibliográficas

Tanenbaum, A. S., & Wetherall, D. J. (2011). "Redes de Computadoras". Pearson.
Beasley, D., & Silverman, S. (2007). "Seguridad de Redes para Dummies". For Dummies.
Denning, D. E. (1987). "An Intrusion Detection Model." IEEE Transactions on Software Engineering, 13(2), 222-232.
Bellovin, S. M. (2003). "Using the Domain Name System for System Break-Ins." ACM Transactions on Internet Technology (TOIT), 3(3), 273-296.
Cisco. (2020). "Configuring DHCP Snooping." Cisco IOS IP Configuration Guide.
NIST (National Institute of Standards and Technology). (2018). "Guidelines for Securing Wireless Local Area Networks (WLANs)." NIST Special Publication 800- 153.