Dom. Cien., ISSN: 2477-8818
Vol. 7, núm. 4. Diciembre Especial 2021, pp. 377-398

DOI: http://dx.doi.org/10.23857/dc.v7i4.2426
Ciencias Técnicas y Aplicadas
Artículo de Investigación

Guía de implementación de buenas prácticas de seguridad en redes. Caso de estudio Infocentros MINTEL

Guide for the implementation of good network security practices. Case study Infocentros MINTEL

Guia para a implementação de boas práticas de segurança de rede. Estudo de caso Infocentros MINTEL

Esteban Giovanny García-Herrera [I]
esteban.garcia.92@est.ucacue.edu.ec
https://orcid.org/0000-0002-0463-1665

Juan Pablo Cuenca-Tapia [II]
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Correspondencia: esteban.garcia.92@est.ucacue.edu.ec

*Recibido: 30 de octubre de 2021 *Aceptado: 20 de noviembre de 2021 * Publicado: 07 de diciembre de 2021

I. Ingeniero de Sistemas. CNT-EP, estudiante de la Maestría en Ciberseguridad. Unidad Académica de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniero de Sistemas, docente de la Maestría en Ciberseguridad, Unidad Académica de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El presente artículo, pretende brindar soluciones tecnológicas a la problemática de seguridad de la red que existe en los diferentes Infocentros del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) de la provincia del Azuay mediante la elaboración de una guía de configuraciones enfocada a equipos mikrotik y estaciones de trabajo de 30 Infocentros, basada en una metodología experimental la misma que está dividida en cuatro fases, en la primera se realizó un diagnóstico mediante la aplicación de una ficha de observación que nos permitió tener una evaluación general del estado actual de los equipos mikrotik y estaciones de trabajo, la segunda fase consistió en el análisis exhaustivo de las configuraciones de cada router y estaciones de trabajo con el fin de encontrar las vulnerabilidades más importantes y críticas, la tercera fase fue la fase de implementación en ella se realizó las configuraciones necesarias en los router mikrotik y estaciones de trabajo, que nos permitieron eliminar las vulnerabilidades encontradas en la fase anterior, y finalmente en la fase de documentación se generó la guía de implantación de buenas prácticas de seguridad en redes y de las estaciones de trabajo en donde se detalló las configuraciones requeridas para garantizar una correcta seguridad de los equipos de red y de las estaciones de trabajo, permitiéndonos así reducir los ataques y garantizar una correcta seguridad de la red y de las estaciones de trabajo de dichos espacios tecnológicos, que son utilizados tanto por personas naturales como por instituciones públicas y privadas.

Palabras clave: Mintel; Infocentros; Router Mikrotik; seguridad de la red; protocolos; Linux.

Abstract

This article aims to provide technological solutions to the network security problem that exists in the different Infocentres of the Ministry of Telecommunications and Information Society (MINTEL) of the province of Azuay through the development of a focused configuration guide to mikrotik equipment and workstations of 30 Infocentros, based on an experimental methodology which is divided into four phases, in the first a diagnosis was made by applying an observation sheet that allowed us to have a general evaluation of the current state of the mikrotik equipment and workstations, the second phase consisted of an exhaustive analysis of the configurations of each router and workstations in order to find the most important and critical vulnerabilities, the third phase was the implementation phase in which it made the necessary configurations on the mikrotik routers and workstations, which They allowed us to eliminate the vulnerabilities found in the previous phase, and

finally in the documentation phase, the guide for the implementation of good security practices in networks and workstations was generated, where the configurations required to guarantee a correct security of the workstations were detailed. network equipment and workstations, thus allowing us to reduce attacks and guarantee correct security of the network and workstations of said technological spaces, which are used both by individuals and by public and private institutions

Keywords: Mintel; Infocentros; Mikrotik; network security; configuration.

Resumo

Este artigo visa fornecer soluções tecnológicas para o problema de segurança de rede que existe nos diferentes Infocentros do Ministério das Telecomunicações e da Sociedade da Informação (MINTEL) da província de Azuay, preparando um guia de configuração focado para equipamentos e estações de trabalho mikrotik de 30 Infocentros, com base numa metodologia experimental que se divide em quatro fases, na primeira foi feito um diagnóstico através da aplicação de uma ficha de observação que nos permitiu ter uma avaliação geral do estado atual dos equipamentos e estações de trabalho mikrotik, a segunda fase consistiu num exaustivo análise das configurações de cada roteador e estações de trabalho a fim de encontrar as vulnerabilidades mais importantes e críticas, a terceira fase foi a fase de implementação na qual foram feitas as configurações necessárias nos roteadores e estações de trabalho mikrotik, que Permitiram eliminar as vulnerabilidades encontradas na fase anterior e, finalmente, na fase de documentação, foi gerado o guia de implementação de boas práticas de segurança em redes e estações de trabalho, onde foram detalhadas as configurações necessárias para garantir a correta segurança dos equipamentos de rede e estações de trabalho, permitindo-nos reduzir os ataques e garantir a segurança adequada da rede e das estações de trabalho dos referidos espaços tecnológicos, que são utilizados tanto por particulares como por instituições públicas e privadas.

Palavras-chave: Mintel; Infocentros; Roteador Mikrotik; segurança de rede; protocolos; Linux.

Introducción

Los Infocentros son espacios de participación y encuentro en los que se garantiza el acceso a las Tecnologías de la Información y Comunicación (TIC), contribuyendo a la reducción de la brecha digital, fomentando el desarrollo, la innovación y el emprendimiento, su misión consiste en consolidar la Sociedad de la Información en todos los estratos sociales y productivos de las zonas rurales y

urbanas marginales del Ecuador, buscando el desarrollo económico y productivo, por medio del conocimiento, la innovación y el emprendimiento, sus objetivos estratégicos son: Capacitar en el uso de las TIC y promover emprendimientos productivos, promover el uso de los servicios gubernamentales en línea y promoción y difusión del gobierno en territorio (¿Qué Son Los Infocentros? – Proyecto Infocentros Ecuador, n.d.).

Los infocentros están formados por diferentes actores en su modelo de gestión y son:

- El Ministerio de Telecomunicaciones y de Sociedad de la Información encargado del monitoreo de operación.
- La Corporación Nacional de Telecomunicaciones CNT EP, encargada de proporcionar el mobiliario, la conectividad contratación de personal.
- Los Gobiernos Autónomos Descentralizados, encargados de asignar el espacio físico, mantenimiento de la infraestructura entre otros.
- La Comunidad, que son los beneficiarios.

Este proyecto se compara con otros proyectos similares de otros países como lo son:

Proyecto Infocentro en Venezuela, Redes de Infocentros en España, Infocentros en Chile (¿Qué Son Los Infocentros? – Proyecto Infocentros Ecuador, n.d.).

Podemos citar que en Chile los infocentros son centros de conectividad desde donde se puede acceder a servicios de capacitación, comunicación, información y de educación de manera presencial como a distancia, al igual que en Ecuador están ubicados, especialmente, en zonas rurales o lejanas geográficamente y se han convertido en una opción para quienes no cuentan con línea telefónica o computador, los servicios que ofrece son: acceso a internet, teléfono, fax, scanner, fotocopiado, entre otros. Se puede indicar que 56 infocentros funcionan actualmente con equipos reciclados, de los mil infocentros que componen la red nacional de acceso a Internet. (Infocentros - Subsecretaría de Telecomunicaciones de Chile, n.d.).

En la actualidad, el Proyecto Ampliación de la Red Infocentros realizará la operación de los 900 Infocentros y 25 Megainfocentros, los mismos que se encuentran ubicados en todo el territorio ecuatoriano (De Telecomunicaciones et al., n.d.).

En Ecuador el 43 % de los ciudadanos que tiene acceso a internet, carecen de una educación formal sobre el tema informático, la gran mayoría, desconocen el peligro del uso de internet y no tiene idea de las medidas de protección y prevención que hay que tomar sobre las amenazas, siendo fácilmente

víctimas de los ciberataques; agregando a ello que las políticas de ciber seguridad en las empresas del Ecuador, tampoco se aplican de manera rigurosa. (Alvarado Jorge, 2020).

Los equipos de red que son utilizados en los infocentros son los router de la marca Mikrotik que es una empresa que desde 1996 fabrica equipos de telecomunicaciones basados en hardware y software, siendo uno de los principales proveedores de tecnológica inalámbrica.

Su sistema operativo se llama RouterOS que es un sistema operativo basado en el kernel de Linux 2.6 de gran potencia que permite elaborar cualquier configuración de red, las más conocidas son: Firewall, Routing, Forwarding, MPLS, VPN, Wireless, HotSpot, Calidad de Servicio (QoS), Web Proxy. Para administrar su sistema operativo mediante una interfaz gráfica se puede utilizar la aplicación Winbox y es compatible con Windows, Linux e IOS. (Quinte Sinche & Ushiña Tomalá, 2020).

En su publicación Pauzhi William indica que efectuó la implementación de políticas de seguridad, en un WISP (Wireless Internet Service Provider), en donde propone integrar un mecanismo de seguridad que mitigue los riesgos de sufrir ataques de ciberdelincuentes y la empresa pueda garantizar la confidencialidad, integridad y disponibilidad de su servicio con la utilización de quipos Mikrotik (Pauzhi William, 2016).

Las TICS se han convertido en instrumentos primordiales para el progreso de la sociedad. Por lo que en la actualidad la seguridad en redes se ha convertido en un área de estudio sumamente transcendental, y nos va a permitir identificar y mitigar las vulnerabilidades existentes y asegurar toda la información (Serrano Luis, 2020).

Ya sea las grandes potencias como los países en desarrollo, son susceptibles de recibir ciberataques; existe por lo tanto la necesidad de realizar un estudio obligado para establecer las estrategias de la defensa de los estados; la ciberdefensa y ciberseguridad son las áreas claves de los estudios estratégicos para proteger el ciberespacio. (Enrique et al., 2020)

Ecuador se ha mantenido en la posición 49 dentro de las estadísticas de países con mayores sucesos de software malicioso o malware según la empresa de seguridad Kaspersky. Según el especialista en ciberseguridad Galoget Latorre, Ecuador ocupa el primer lugar en ataques tipo ‘ransomware’, seguido por Bolivia y Venezuela a nivel andino. Los ataques a la seguridad en las empresas se dispararon entre el 2018 y el 2019. En Latinoamérica, en el 2018, Ecuador y Venezuela sufrieron la mayor cantidad de ataques a sus empresas (22%), les siguieron Chile, Costa Rica y Panamá con 21%. En el 2019, en América Latina se mantuvieron los ataques a empresas, ocupando Ecuador el cuarto lugar

en la región en cuanto a estos ataques. (Ecuador, Una de Las Naciones Más Atacadas Por Los 'Hackers' | Datta Business Innovation, n.d.).

En su informe de amenazas en tiempo real Kaspersky Lab, en junio del año 2017, Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes. El 49,05 % de estos fueron producidos por ataques de fuerza bruta. (Enrique et al., 2020).

Los diferentes procedimientos de seguridad que se pueden aplicar para proteger redes inalámbricas dependen del nivel que se requiera. Las redes inalámbricas tienen diferentes protocolos de seguridad, los más utilizados son WEP, WPA, WPA2 e IEEE 802.1x. Uno de los principales inconvenientes es que no existe una herramienta que permita la detección oportuna de anomalías en la red, y pueda detectar y contener lo más pronto posible los diferentes tipos de atacas como por ejemplo denegación de servicios, robo de identidad, propagación de virus, daño de la red, entre otros. Para diseñar una red lo suficientemente segura se necesita principalmente un análisis minucioso y detallado de los diferentes protocolos, herramientas y aplicaciones, también tener un profundo conocimiento de los principales servicios y sus vulnerabilidades (Sánchez Anabel, 2016).

En los últimos años la tecnología inalámbrica no ha parado de evolucionar, su bajo costo y su fácil implementación ha permitido que tenga un importante crecimiento y demanda en relación a las redes cableada, siendo las redes inalámbricas preferidas por parte de los usuarios tanto del sector público como privado, más aún si la mayoría de los equipos terminales laptops, tables, smartphone vienen con una tarjeta integrada Wifi. (Sánchez Anabel, 2016).

Al diseñar un sistema de comunicaciones la seguridad es el punto clave y más delicado que debemos tomar en cuenta más aún si se ofrece un servicio público, por lo que es necesario implementar mecanismos de seguridad que certifiquen la confidencialidad integridad y disponibilidad de la información y que se garantice la estabilidad del servicio que se proporciona por esas redes.

Día tras día aparecen nuevas herramientas de ataque más sofisticadas que pueden atentar el correcto funcionamiento de la red, y más aún si la mayoría de redes wifi no disponen de sistemas de autenticación seguros que garanticen que la información no sea accedida y modificada por usuarios no autorizados utilizando mecanismos de ataque como denegación de servicios, es por ello que se hace necesario disponer de una guía de buenas prácticas a seguir que nos permitan detener las amenazas que intenten ingresar a la red permitiéndonos así proteger la información delicada de nuestros clientes que transita por la red.

La conectividad de los infocentros es mediante una red Wireless utilizando una topología en estrella, es decir el router mikrotik irradia señal inalámbrica a todos los dispositivos electrónicos ubicados en el infocentros los mismos que disponen de antenas wifi, y las estaciones de trabajo funcionan bajo software libre como su sistema operativo.

En este contexto, se ha identificado la necesidad urgente de realizar una guía de implementación de buenas Prácticas de Seguridad en Redes para configuración de equipos mikrotik y estaciones de trabajo de 30 Infocentros del Ministerio de Telecomunicaciones y de la Sociedad de la Información pertenecientes a la provincia del Azuay, que permita garantizar una correcta seguridad de la red y de las estaciones de trabajo que conforman los diferentes infocentros.

Materiales y métodos

Se utilizó una investigación de tipo exploratoria, es decir se utilizó datos recogidos a partir de encuestas realizadas a 30 Infocentros del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) de la provincia del Azuay.

A nivel de la provincia del Azuay existen más de 50 Infocentros, pero con la problemática de que cuentan con diferentes marcas y modelos de equipos para la conectividad y sus estaciones de trabajo se manejan con diferentes sistemas operativos, por lo que básicamente nos centraremos en el estudio de los 30 Infocentros mencionados anteriormente.

El cuestionario realizado de forma presencial y dirigido específicamente a los facilitadores de cada Infocentro quienes son los encargados de ayudar y asesorar a los usuarios para el correcto uso del mismo, el cuestionario está formado por 11 preguntas específicas que se responden mediante una afirmación (SI) o negación (NO).

También es importante indicar que se encuentra documentada la respectiva información de los dispositivos de red y estaciones de trabajo como son las marcas, modelos, versiones de software instalados, versiones de firmware instaladas etc. Además de ellos se cuenta con un registro de los logs de todos los router Mikrotik con el fin de tener una visión general por donde los ciberdelincuentes hackean o intentan hackear dichos equipos.

Esta investigación se basa fundamentalmente en el análisis de los aspectos importantes que se deben tener en cuenta para garantizar una correcta seguridad de la red y de las estaciones de trabajo como son: la tecnología, una correcta configuración de equipos de red y estaciones de trabajo, y así poder documentar una guía de buenas prácticas de seguridad en redes para los infocentros del MINTEL.

En lo que se refiere a la tecnología se analizó todo lo relacionados a la conectividad la misma que la proporciona la Corporación Nacional de Telecomunicaciones CNT, que ofrece su servicio mediante diferentes tipos de tecnologías como son fibra óptica, radio enlace y Servicio Satelital VSAT, para poder cumplir con las necesidades de los usuarios que están ubicadas en diferentes parroquias rurales de la provincia del Azuay.

En base a este estudio realizado se ha optado por la implementación de una guía de buenas prácticas de seguridad de los equipos de red y de las estaciones de trabajo que serán aplicados en los 30 infocentros lo que ha permitido obtener los siguientes beneficios en cuanto a la seguridad de la red y evitar a los ciberdelincuentes:

- Evitar robo de la contraseña wifi.
- Evitar el uso inadecuado del ancho de banda.
- Evitar daños lógicos de equipos por infección de algún malware.
- Garantizar la disponibilidad de la red.
- Tener un control sobre el acceso a diferentes páginas web permitidas y no permitidas.

Modelo propuesto.

El modelo propuesto para la implementación de una guía de Buenas Prácticas de Seguridad en Redes para configuración de equipos mikrotik y estaciones de trabajo para los 30 Infocentros del Ministerio de Telecomunicaciones y de la Sociedad de la Información (Mintel) pertenecientes a la provincia del Azuay, se realizó en base a una investigación experimental que consistió en realizar varias configuraciones en los equipos mikrotik y en las estaciones de trabajo para que al final realizar un análisis comparativo con otros equipos que no fueron aplicados dichas configuraciones y obtener los resultados requeridos y verificar si se pudieron o no obtener los resultados deseados.

Se dividió este modelo en 4 fases las mismas que se detallan en el siguiente grafico:

Figura 1: Modelo de guía de buenas prácticas.
Fuente: Elaboración propia.

Diagnóstico

El primer paso para la implementación de una guía de buenas prácticas de seguridad de seguridad en redes es la fase de diagnóstico que se obtuvo mediante la aplicación de una ficha de observación la cual permitió tener una evaluación general del estado actual de los equipos mikrotik y de las estaciones de trabajo, las mismas se detallan en la siguiente tabla.

CÓDIGO	DESCRIPCIÓN
diaginfo001	No se tiene correctamente identificado el nombre del equipo
diaginfo002	Equipos mikrotik con credenciales de acceso por defecto.
diaginfo003	No está limitado el número de intentos para acceder al router.
diaginfo004	Protocolo MNDP MikroTik Neighbor Discovery protocol habilitado
diaginfo005	Servidor DNS acepta todas las peticiones provenientes de internet a la WAN del mikrotik
diaginfo006	Los diferentes puertos de servicio están habilitados.
diaginfo007	Los diferentes protocolos de acceso como son ssh, telnet, www, www-ssl están habilitados.
diaginfo008	El control de ancho de banda no está deshabilitado
diaginfo009	No poseen listas de control de acceso.
diaginfo010	No se tiene configurado filtrado de contenidos.
diaginfo011	No está instalado la última versión del firmware.
diaginfo012	No están configurados correctamente los tipos de autenticación para la red WLAN.
diaginfo013	Las contraseñas de acceso a la red WLAN son básicas.
diaginfo014	Sistemas operativos Linux desactualizados.
diaginfo015	Navegador Google Chrome desactualizado.
diaginfo016	Navegador Mozilla Firefox desactualizado.
diaginfo017	No se tiene instalado antivirus y antimalware.
diaginfo018	No se tiene instalado complementos antimalware en el navegador Google Chrome.
diaginfo019	No se tiene instalado complementos antimalware en el navegador Mozilla Firefox.
diaginfo020	No se tiene creado los usuarios y sus privilegios

Tabla 1: Diagnostico.
Fuente: Elaboración propia.

Análisis

En este apartado se analizó por separado las vulnerabilidades más importantes y criticas encontradas en cada uno de los 30 infocentros que fueron motivo de estudio.

En la Tabla 2, detallamos la información de los equipos MikroTik como lo son el modelo, la versión del firmware, si posee o no credenciales de acceso, si tiene configurado o no credenciales de acceso, si está configurado el número de intentos de login, si el equipo tiene aplicado listas de control de

acceso, si está configurado algún tipo de filtrado de contenidos, si se está limitando el ancho de banda y si el servidor dns acepta peticiones desde la wan.

En donde: SI= Si tiene configurado, NO=No tiene configurado H=Habilitado, D=Deshabilitado.

EQUIPOS DE RED MIKROTIK															
INFOCENTRO	MARCA	MODELO	VERSION DEL FIRMWARE INSTALADO	CREDENCIALES DE ACCESO		INTENTOS DE LOGIN		LISTA DE CONTROL DE ACCESO		FITRADO DE CONTENIDOS		BTEST SERVER		SERVIDOR DNS ACEPTE PETICIONES A LA WAN DEL ROUTER	
				SI	NO	SI	NO	SI	NO	SI	NO	H	D	H	D
1	MIKROTIK	RB750Gr2	6.48.3	X			X	X		X			X		X
2	MIKROTIK	RB951G-2HnD	6.43.0		X		X		X	X			X	X	
3	MIKROTIK	RB951G-2HnD	6.42.6	X			X		X	X			X		X
4	MIKROTIK	RB951G-2HnD	6.48.2	X			X		X		X	X		X	
5	MIKROTIK	RB951G-2HnD	6.48.3	X			X	X		X			X	X	
6	MIKROTIK	RB951G-2HnD	6.48.1		X		X		X	X		X			X
7	MIKROTIK	RB951G-2HnD	6.48.3	X		X		X		X			X	X	
8	MIKROTIK	RB951Ui-2nD	6.43.0		X		X		X		X	X			X
9	MIKROTIK	RB951G-2HnD	6.43.0	X			X	X			X	X		X	
10	MIKROTIK	RB951G-2HnD	6.43.0	X			X		X	X		X			X
11	MIKROTIK	RB951G-2HnD	6.42.3	X		X		X		X		X		X	
12	MIKROTIK	RB951G-2HnD	6.42.3		X		X		X		X	X		X	
13	MIKROTIK	RB951G-2HnD	6.45.3	X			X	X			X		X		X
14	MIKROTIK	RB951G-2HnD	6.48.4	X		X		X		X			X		X
15	MIKROTIK	RB951G-2HnD	6.48.4	X			X	X		X			X		X
16	MIKROTIK	RB951G-2HnD	6.48.4	X			X	X		X			X		X
17	MIKROTIK	RB951G-2HnD	6.43.7	X			X		X		X	X		X	
18	MIKROTIK	RB951G-2HnD	6.48.3	X		X		X			X		X		X
19	MIKROTIK	RB951G-2HnD	6.45.1		X		X		X		X	X		X	
20	MIKROTIK	RB951G-2HnD	6.48.1	X		X			X	X			X		X
21	MIKROTIK	RB951G-2HnD	6.42.3		X		X	X		X		X		X	

22	MIKROTIK	RB951G-2HnD	6.42.3	X		X			X	X			X		X
23	MIKROTIK	RB951G-2HnD	6.43.4		X		X		X		X	X		X	
24	MIKROTIK	RB951G-2HnD	6.43.4		X		X		X		X	X		X	
25	MIKROTIK	RB951G-2HnD	6.42.3		X		X	X		X			X		X
26	MIKROTIK	RB951G-2HnD	6.43.4		X		X		X	X		X		X	
27	MIKROTIK	RB951G-2HnD	6.42.1		X		X	X		X			X		X
28	MIKROTIK	RB951G-2HnD	6.42.3		X		X		X	X		X		X	
29	MIKROTIK	RB951G-2HnD	6.43.0		X		X		X	X		X			X
30	MIKROTIK	RB951G-2HnD	6.43.4		X		X	X		X		X		X	

Tabla 2: Configuraciones encontradas en los Mikrotik.
Fuente: Elaboración propia.

En la Table 3: se describe si el protocolo MNDP está habilitada o no y que no permite impedir que se pueda encontrar otros dispositivos compatibles con MNDP conectados en un mismo dominio de capa2, también se describe si los puertos de servicio y los protocolos de acceso están habilitados o no, y si se tiene habilitado los tipos de autenticación para la WLAN.

PROTOCOLOS, PUERTOS Y TIPO DE AUTENTICACIÓN PARA LA WLAN																						
INFOCENTRO	PROTOCOLO MNDP		PUERTOS DE SERVICIO (H=Habilitado, D=Deshabilitado)									PROTOCOLOS DE ACCESO (H=Habilitado, D=Deshabilitado)								TIPOS DE AUTENTICACIÓN PARA LA WLAN			
	H	D	DCCP	FTP	H323	IRC	PPTP	SCTP	SIP	TFTP	UDPLITE	API	API-SSL	FTP	SSH	TELNET	WINBOX	WWW	WWW-SSL	WPA PSK	WPA2 PSK	WPA EAP	WPA2 EAP
1		X	H	H	D	D	D	H	D	D	H	D	D	D	D	H	H	D	D	X	X		
2	X		D	D	D	D	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
3		X	D	D	D	D	D	D	D	D	D	D	D	D	H	H	H	H	D	X	X		
4		X	D	H	D	D	H	H	D	D	D	D	D	D	H	H	H	H	D	X	X		
5		X	D	D	D	D	D	D	D	D	D	D	D	D	D	D	H	D	D	X	X		
6	X		D	H	D	D	H	D	D	H	D	D	D	D	H	H	H	H	D	X	X		
7		X	D	D	D	D	D	D	D	D	D	D	D	D	D	D	H	D	D	X	X		
8	X		D	H	H	H	D	D	H	H	D	D	D	D	D	H	H	H	H	X	X		
9		X	D	H	D	D	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
10		X	D	H	H	H	D	D	D	D	D	D	D	D	H	H	H	H	D	X	X		

11	X		D	D	D	D	D	D	D	D	D	D	D	D	H	H	H	H	D	X	X		
12	X		D	H	H	H	H	D	D	H	D	D	D	H	D	H	H	H	D	X	X		
13	X		D	H	D	D	D	D	D	H	D	D	D	H	D	H	H	H	D	X	X		
14		X	D	D	D	D	D	D	D	D	D	D	D	D	D	D	H	D	D	X	X		
15		X	D	D	D	D	D	D	D	D	D	D	D	D	D	D	H	D	D	X	X		
16		X	D	D	D	D	D	D	D	D	D	D	D	D	D	D	H	D	D	X	X		
17	X		D	H	D	D	D	D	D	D	D	D	D	H	H	H	H	H	D	X	X		
18	X		D	H	D	D	D	D	H	D	D	D	D	D	D	D	H	D	D	X	X		
19	X		D	H	D	D	D	D	D	H	D	D	D	D	D	H	H	H	D	X	X		
20		X	D	H	D	D	D	D	D	D	D	D	D	D	H	H	H	H	D	X	X		
21	X		D	H	D	D	D	D	D	D	D	D	D	D	H	H	H	H	D	X	X		
22	X		D	H	D	D	D	D	D	D	D	D	D	D	H	H	H	H	D	X	X		
23	X		D	H	D	D	H	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
24	X		D	D	D	D	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
25		X	D	H	D	D	D	D	H	D	D	D	D	D	D	H	H	H	D	X	X		
26	X		D	H	D	D	D	D	D	D	H	D	D	D	D	H	H	H	D	X	X		
27	X		D	H	D	D	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
28		X	D	H	D	H	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
29	X		D	D	D	D	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		
30	X		D	H	D	D	D	D	D	D	D	D	D	D	D	H	H	H	D	X	X		

Tabla 3: Configuración de Protocolos, Puertos y Autenticación encontrada en los Mikrotik.
Fuente: Elaboración propia.

En la Table 4: identificamos que versión del sistema operativo está instalado en las estaciones de trabajo, si a más del usuario administrador está configurado el usuario cliente con sus respectivos privilegios de acceso, la versión que se encuentra instalada tanto en los navegadores Google Chrome como en el Mozilla Firefox, si está instalado o no algún complemento antimalware en los navegadores y si las estaciones de trabajo tienen instalados algún antivirus.

ESTACIONES DE TRABAJO											
INFOCENTRO	SISTEMA OPERATIVO	USUARIOS		VERSION DE GOOGLE CHROME	VERSIÓN DEL MOZILLA FIREFOX	COMPLEMENTO ANTIMALWARE GOOGLE CHROME		COMPLEMENTO ANTIMALWARE MOZILLA FIREFOX		ANTIVIRUS INSTALADO	
		ADMIN	CLIENTE			SI	NO	SI	NO	SI	NO
1	UBUNTU MATE 20.04	X		94.0.46	93.0	X		X		X	
2	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X

3	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
4	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
5	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
6	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
7	UBUNTU MATE 20.04	X	X	94.0.46	93.0	X		X		X	
8	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
9	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
10	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
11	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
12	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
13	UBUNTU MATE 20.04	X	X	94.0.46	93.0	X		X		X	
14	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
15	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
16	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
17	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
18	UBUNTU MATE 20.04	X	X	94.0.46	93.0	X		X		X	
19	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
20	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
21	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
22	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
23	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
24	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
25	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X
26	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
27	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
28	UBUNTU 18.04	X		84.0.41	91.0		X		X		X
29	UBUNTU MATE 20.04	X	X	94.0.46	93.0	X		X		X	
30	UBUNTU MATE 20.04	X		86.0.42	91.0		X		X		X

Tabla 4: Configuración encontrada en las estaciones de trabajo.
Fuente: Elaboración propia.

Como se puede observar en las tablas anteriormente expuestas, se indican las configuraciones encontradas en los diferentes equipos mikrotik y estaciones de trabajo, en donde se evidencia una falta de uniformidad en las configuraciones, es decir no se sigue ningún patrón o lineamiento, simplemente son configurados para proporcionar el servicio de internet o en el caso de las estaciones de trabajo ser útiles para los usuarios, pero en ningún momento se toma en consideración un correcta configuración de las seguridad algo que hoy en día es primordial en este mundo tan tecnológico.

Entre las principales vulnerabilidades identificadas tenemos firmwares desactualizados, puertos y protocoles habilitados, credenciales de acceso por defecto, no se tiene listas de control de acceso, no existe filtrado de contenidos, etc. Evidenciando principalmente que estos equipos están muy susceptibles a diversos ataques dejando así la puerta abierta para que ciberdelincuentes pueden utilizar estas falencias para materializar su objetivo.

Implementación

En base a los resultados obtenidos en la fase de Análisis, se realizó las configuraciones necesarias en los router mikrotik y estaciones de trabajo, que nos permitieron eliminar las vulnerabilidades encontradas en la fase de análisis y así poder mitigar los diferentes ataques, para luego en base a los resultados obtenido poder generar la guía de buenas prácticas de seguridad en redes y aplicarla a todos los infocentros. En la Tabla 5: se detalle las diferentes configuraciones implementadas en los equipos de red, definiendo cada uno de su propósito.

Código Diagnostico	Código de Implementación	Configuración implementada	Objetivo
diaginfo001	implinfo001	/system identity set name=Nombre_Infocentro_#Servicio	Identificar el nombre del equipo
diaginfo002	implinfo002	/user add name=?????? password=??????? group=full /user remove admin	Crear usuarios y eliminar el usuario por defecto admin
diaginfo003	implinfo003	/system logging action set 1 disk-file-count=1 disk-lines-per-file=500 /system logging set 0 action=disk set 1 action=disk set 2 action=disk set 3 action=disk	Permite acceder al mikrotik con un máximo de tres intentos, el cuarto intento se bloquea la ip que desea ingresar al router

diaginfo004	implinfo004	/ip neighbor discovery-settings set discover-interface-list=!all	Deshabilitamos el protocolo MNDP MikroTik Neighbor Discovery protocol, para impedir que se pueda encontrar otros dispositivos compatibles con MNDP conectados en un mismo dominio de capa2
diaginfo005	implinfo005	/ip dns set allow-remote-requests=no	Impide que el servidor de DNS acepte peticiones provenientes desde Internet hacia la WAN del Mikrotik.
diaginfo006	implinfo006	/ip service disable ftp,telnet,www,www-ssl,api,api-ssl	Deshabilitamos diferentes servicios de acceso como son: ftp, ssh, telnet, www, etc. Solo dejamos habilitado el servicio winbox para poder conectarnos vía remota al router.
diaginfo007	implinfo007	/ip firewall service-port disable dccp,h323,irc,pptp,sctp,sip,tftp,udplite	Deshabilitamos los diferentes puertos para evitar accesos no autorizados.
diaginfo008	implinfo008	/tool bandwidth-server set enabled=no	Deshabilitamos el control de ancho de banda.
diaginfo009	implinfo009	add chain=input comment="Permitir ping limitados" limit=50/5s,2:bit protocol=\ icmp add action=drop chain=input comment="Bloquear ping en exceso" protocol=icmp add action=drop chain=input comment="rechazar ataques telnet" dst-port=23 \ protocol=tcp src-address-list=telnet_blacklist add action=add-src-to-address-list address-list=telnet_blacklist \ address-list-timeout=2d chain=input connection-state=new dst-port=23 \ protocol=tcp src-address-list=telnet_stage2 add action=add-src-to-address-list address-list=telnet_stage2 \ address-list-timeout=1m chain=input connection-state=new dst-port=23 \ protocol=tcp src-address-list=telnet_stage1 add action=add-src-to-address-list address-list=telnet_stage1 \ address-list-timeout=1m chain=input connection-state=new dst-port=23 \protocol=tcp add action=drop chain=input comment="rechazar ataques ssh" dst-port=22 \protocol=tcp src-address-list=ssh_blacklist add action=add-src-to-address-list address-list=ssh_blacklist \ address-list-timeout=2d chain=input connection-state=new dst-port=22 \ protocol=tcp src-address-list=ssh_stage2	Creamos las diferentes reglas como son: • Aceptar conexiones establecidas. • Rechazar conexiones inválidas. • Eliminar ataques ftp de fuerza bruta. • Permitir ping limitados. • Bloquear ping en exceso. • Rechazar ataques telnet. • Rechazar ataques ssh. • Rechazar ataques http. • Rechazar ataques winbox. • Bloqueo de ataques DNS. Por la gran cantidad del script solo describimos las configuraciones de seguridad más importantes.
		/ip firewall address-list add address=192.168.88.0/24 comment="BLOQUEO PORNOGRAFIA" list=\ "BLOQUEO PORNO"	Crear la regla a ser aplicada para el bloque de páginas pornográficas en toda la red LAN.

diaginfo010	implinfo010	/ip firewall nat add action=masquerade chain=srcnat out-interface=WAN_INTERNET add action=dst-nat chain=dstnat dst-port=53 protocol=udp src-address-list=\"BLOQUEO PORNO" to-addresses=199.85.127.30 to-ports=53	Se asigna la regla a toda la interfaz WAN, por el puerto 53, utilizando la ip de un servicio gratuito de Norton ConnectSafe, que es un servicio para bloquear automáticamente los sitios no seguros, en este caso se está utilizando la política 3 de este servicio, que se trata de una política de seguridad + pornografía + otros. Además de bloquear sitios no seguros y sitios de pornografía, esta política también bloquea el acceso a sitios que tengan, aborto, alcohol, crimen, cultos, drogas, juegos de azar, desprecio, orientación sexual, suicidio, tabaco o violencia.
diaginfo011	implinfo011	/System /Package/Check for uptdate/download and install	Descargar la última versión del Firmware
diaginfo012	implinfo012		Configurar los tipos de autenticación para la WLAN
diaginfo013	implinfo013		Establecer contraseñas para la WLAN seguras recomendable más de 10 caracteres utilizar signos de puntuación y caracteres especiales

Tabla 5: Configuraciones de seguridad aplicadas al Mikrotik.
Fuente: Elaboración propia.

En la Tabla 6: se detalle las diferentes configuraciones implementadas en las estaciones de trabajo, definiendo cada uno de su propósito.

Código Diagnostico	Código de Implementación	Configuración implementada	Objetivo
diaginfo014	implinfo014	Sudo apt-get update	Actualizar la lista de paquetes y sus versiones Ubuntu
		Sudo apt-get upgrade	Instalar los paquetes y versiones descargados.
diaginfo015	implinfo015	wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb sudo dpkg -i google-chrome-stable_current_amd64.deb	Actualizar el navegador Google Chrome.
diaginfo016	implinfo016	Sudo apt update Sudo apt install --only-upgrade firefox	Actualizar el navegador Mozilla Firefox
diaginfo017	implinfo017	sudo apt install clamav	Instalar el antivirus clamav para Ubuntu.
		sudo apt install clamtk	Instalar el entorno grafico del clamav.

diaginfo018	implinfo018	Malwarebytes Browser Guard	Instalar la extensión en el navegador Google Chrome, para bloquear paginas maliciosas.
diaginfo019	implinfo019	Malwarebytes Browser Guard	Instalar la extensión en el navegador Mozilla Firefox, para bloquear paginas maliciosas.
diaginfo020	implinfo020	Sudo su - Sudo useradd usuarionuevo	Crear usuarios con el fin de darles ciertos privilegios y evitar que instalen o desinstales software en Ubuntu.

Tabla 6: Configuración de las estaciones de trabajo.
Fuente: Elaboración propia.

Documentación

En esta fase se documentó la guía de implantación de buenas prácticas de seguridad en redes y de las estaciones de trabajo en donde se indicó las configuraciones requeridas para garantizar una correcta seguridad de los equipos de red y de las estaciones de trabajo y así poder mitigar a los ciberatacantes. Se propuso la siguiente guía:

	GUÍA DE IMPLEMETACIÓN DE BUENAS PRACTICAS DE SEGURIDAD EN REDES Y ESTACIONES DE TRABAJO	Versión: 001

Código de guia:
Fecha:
Datos del Infocentro:
Código:
Nombre:
Provincia:
Parroquia:
Datos del equipo de red:
Marca:
Modelo:
Datos de las estaciones de trabajo:
Marca:
Cantidad:

1. Identificación del equipo de red.				
diaginfo001	SI NO	☐ ☐	***Aplicar***	implinfo001
2. Credenciales de acceso.				
diaginfo002	SI NO	☐ ☐	***Aplicar***	implinfo002
3. Intentos de acceso.				
diaginfo003	SI NO	☐ ☐	***Aplicar***	implinfo003
4. Protocolo MNDP deshabilitado.				
diaginfo004	SI NO	☐ ☐	***Aplicar***	implinfo004
5. Desabilitado Allow Remote Requests.				
diaginfo005	SI NO	☐ ☐	***Aplicar***	implinfo005
6. Puertos de servicio deshabilitados.				
diaginfo006	SI NO	☐ ☐	***Aplicar***	implinfo006
7. Protocolos de acceso deshabilitados.				
diaginfo007	SI NO	☐ ☐	***Aplicar***	implinfo007
8. Control de limite de ancho de banda deshabilitados.				
diaginfo008	SI NO	☐ ☐	***Aplicar***	implinfo008

9. Reglas de control de acceso creadas.				
	diaginfo009	SI ☐ NO ☐	***Aplicar***	implinfo009
10. Reglas de filtrado de contenidos creada.				
	diaginfo010	SI ☐ NO ☐	***Aplicar***	implinfo010
11. Ultima version del firmware instalada.				
	diaginfo011	SI ☐ NO ☐	***Aplicar***	implinfo011
12. Tipos de autenticación para la WLAN configurados.				
	diaginfo012	SI ☐ NO ☐	***Aplicar***	implinfo012
13. Contraseña para la WLAN segura.				
	diaginfo013	SI ☐ NO ☐	***Aplicar***	implinfo013
14. Sistema Operativo actualizado.				
	diaginfo014	SI ☐ NO ☐	***Aplicar***	implinfo014
15. Navegador Google Chrome actualizado a la ultima version.				
	diaginfo015	SI ☐ NO ☐	***Aplicar***	implinfo015
16. Navegador Mozilla Firefox actualizado a la ultima version.				
	diaginfo016	SI ☐ NO ☐	***Aplicar***	implinfo016
17. Antivirus instalado.				
	diaginfo017	SI ☐ NO ☐	***Aplicar***	implinfo017
18. Complemento antimalware instalado en el navegador Google Chrome.				
	diaginfo018	SI ☐ NO ☐	***Aplicar***	implinfo018
19. Complemento antimalware instalado en el navegador MozillaFirmware.				
	diaginfo019	SI ☐ NO ☐	***Aplicar***	implinfo019
20. Creado los respectivos usuarios con sus permisos.				
	diaginfo020	SI ☐ NO ☐	***Aplicar***	implinfo020

Figura 2: Guía de buenas prácticas de seguridad en redes y estaciones de trabajo.
Fuente: Elaboración propia.

Resultados y discusión

La implementación de la guía de buenas prácticas de seguridad en redes para la configuración de equipos mikrotik y estaciones de trabajo de los 30 infocentros del Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL de la provincia del Azuay que fueron objeto de estudio permitió que tanto los equipos de red como las estaciones de trabajo incrementen su seguridad en un gran porcentaje permitiendo así que los equipos ya no sean susceptibles a ataques de ciberdelincuentes garantizando con ello la confidencialidad, integridad y disponibilidad de la red y de sus equipos terminales.

Se ha conseguido que en el caso de que los equipos de red o las estaciones de trabajo de algún Infocentro que no cuenten con las seguridades necesarias y se evidencia que están siendo víctimas de ciberataques, inmediatamente se pueda implementar la guía antes descrita permitiendo así mitigar los ataques de una manera más rápida y oportuna.

La figura 3 muestra el acceso fallido al router con las credenciales por defecto, la figura 4 muestra el firmware actualizado a la última versión, la figura 5 muestra los logs de un equipo mikrotik que fue aplicado la guía de buenas prácticas de seguridad en redes, mientras que la figura 6 muestra los logs de un equipo que no fue implementado esta guía.

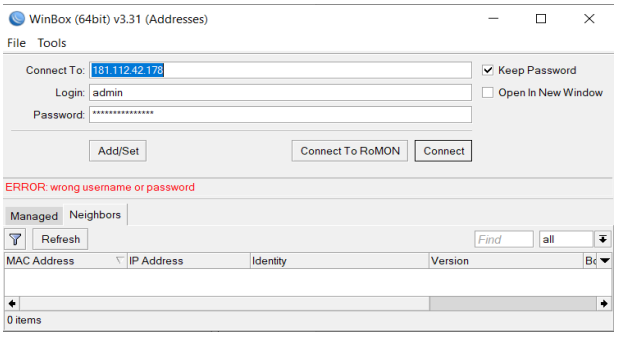

Figura 3: Acceso al router con las credenciales por defecto.
Fuente: Elaboración propia.

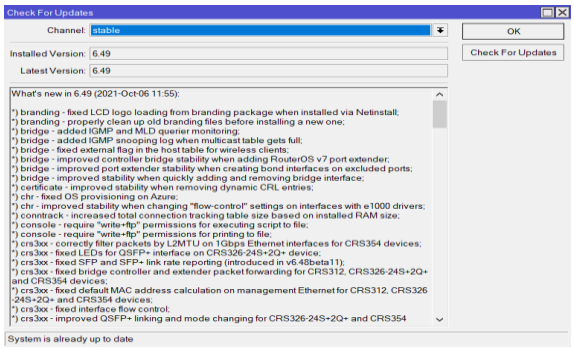

Figura 4: Firmware actualizado.
Fuente: Elaboración propia.

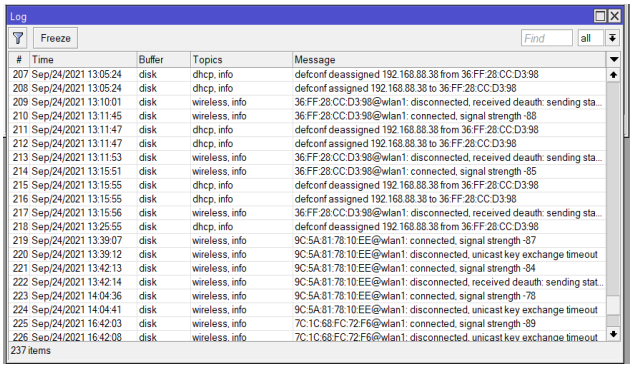

Figura 5: Mikrotik aplicado seguridades.
Fuente: Elaboración propia.

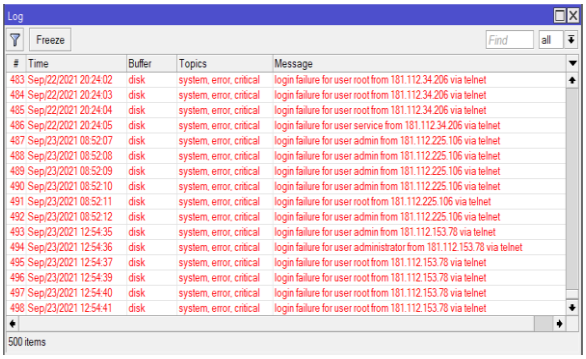

Figura 6: Mikrotik sin seguridades.
Fuente: Elaboración propia.

Conclusiones

- En la actualidad con el continuo desarrollo de nuevas tecnologías y un sinnúmero de aplicaciones que permitan aprovechar las vulnerabilidades de los equipos de red ingresar a ellos y utilizar sus recursos para potenciar sus ataques, es primordial contar con mecanismos de defensas que permitan mitigar dichos ataques y poder contar con equipos de red y estaciones de trabajo que garanticen una correcta seguridad, lógicamente no será suficiente y no se conseguirá nunca un 100% de seguridad de los equipos, ya que como se indicó anteriormente día tras día los avances tecnológicos hacen que aparezcan nuevas aplicaciones que puedan dejar sin efecto estas seguridades, pero en base a esta guía que se propone poder garantizar en gran medida que los equipos de red y estaciones de trabajo sean lo más seguras ante algún ataque.
- Con el presente trabajo de investigación se determinó que Ecuador es uno de los países más atacados por hackers en Latinoamérica, es por ello que es muy importante contar con métodos y procedimientos adecuados con el fin de mitigar estos ataques y hacer de los equipos de red y estaciones de trabajo equipos más seguros impidiendo que se produzca un eventual ataque.
- Esta guía de implementación de buenas prácticas de seguridad en redes de equipos mikrotik y estaciones de trabajo se presenta como una alternativa moderna y adecuada que brinde una y correcta configuración de equipos de red permitiendo así mitigar en gran medida ataques de hackers y ciberdelincuentes.

Referencias

1. ¿Qué son los Infocentros? – Proyecto Infocentros Ecuador. (n.d.). Retrieved August 2, 2021, from https://infocentros.mintel.gob.ec/que-son-infocentros/
2. Alvarado Jorge. (2020, May 21). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. Revista Científica Aristas. https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf
3. De Telecomunicaciones, M., De, Y., & De, L. S. (n.d.). PROYECTO AMPLIACIÓN DE LA RED INFOCENTROS.
4. Ecuador, una de las naciones más atacadas por los 'hackers' | Datta Business Innovation. (n.d.). Retrieved September 26, 2021, from https://datta.com.ec/articulo/ecuador-una-de-las-naciones-mas-atacadas-por-los-hackers
5. Enrique, J., Chang, A., Juan, T., & Aguirre, B. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. Revista Científica Aristas, 2(1).
6. Infocentros - Subsecretaría de Telecomunicaciones de Chile. (n.d.). Retrieved October 2, 2021, from https://www.subtel.gob.cl/infocentros/
7. Pauzhi William. (2016). ANÁLISIS E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA WISP MEDIANTE EQUIPOS MIKROTIK Y ELEMENTOS DE RED. https://dspace.ups.edu.ec/bitstream/123456789/12127/1/UPS-CT006042.pdf
8. Quinte Sinche, P. I., & Ushiña Tomalá, I. L. (2020). Implementación de topologías de red utilizando equipos Mikrotik. http://bibdigital.epn.edu.ec/handle/15000/20647
9. Sánchez Anabel. (2016). Propuesta de Configuración de Seguridad en la Red WiFi del Proveedor de Servicios ETECSA en Villa Clara. https://dspace.uclv.edu.cu/bitstream/handle/123456789/6693/Anabel_Sanchez_.pdf?sequence=1&isAllowed=y
10. Serrano Luis. (2020). "Guía de Buenas Prácticas de Seguridad en Redes para la Configuración de Dispositivos de Capa 2 y 3 del Modelo OSI y Validación en una Red de Pruebas. http://dspace.uazuay.edu.ec/bitstream/datos/9779/1/15410.pdf