SEGURIDAD INFORMÁTICA DE REDES DOMÉSTICAS DE LA CIUDAD DE EL CARMEN

COMPUTER SECURITY OF DOMESTIC NETWORKS OF THE CITY OF EL CARMEN

Clara Guadalupe Pozo Hernández [1*]

[1] Carrera de Ingeniería en Tecnologías de la Información. Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen. Ecuador. ORCID: https://orcid.org/0000-0001-6186-1099. Correo: clara.pozo@uleam.edu.ec

Raúl Saed Reascos Pinchao [2]

[2] Carrera de Ingeniería en Tecnologías de la Información. Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen. Ecuador. ORCID: https://orcid.org/0000-0002-7903-4312. Correo: raul.reascos@uleam.edu.ec

Renelmo Wladimir Minaya Macías [3]

[3] Carrera de Ingeniería en Tecnologías de la Información. Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen. Ecuador. ORCID: https://orcid.org/0000-0002-0418-6864. Correo: renelmo.minaya@uleam.edu.ec

*** Autor para correspondencia: clara.pozo@uleam.edu.ec**

Resumen

Actualmente contar con acceso a internet es esencial en el ámbito empresarial, educativo y en los hogares; a partir de la pandemia han tenido la necesidad de comunicarse y mantenerse conectados a través de diferentes plataformas virtuales que facilitan sus actividades diarias, junto a los beneficios que ofrece utilizar internet está la exposición a peligros y riesgos de seguridad informática que pueden afectar la información de los usuarios en caso de no estar protegidos; por esta razón el objetivo de este trabajo de investigación fue determinar los principales riesgos de seguridad informática a las que están expuestas las redes de internet en los hogares de la ciudad de El Carmen; se realizó la selección de 100 hogares de la ciudad con acceso a internet obteniendo su autorización para el estudio, se aplicó un checklist de 90 preguntas para evaluar el cumplimiento de controles de seguridad y se realizó un escaneo de vulnerabilidades en la red con la herramienta de distribución libre OpeVAS; los datos recolectados fueron procesados utilizando una hoja

electrónica que permitió agrupar los datos considerando diferentes criterios, para su análisis posterior tales como: proveedor de internet, tipo de plan, características del router entre otros; obteniendo como resultados que el nivel de riesgo general es del 55% considerado como nivel MEDIO ALTO, en cuanto a los factores de análisis se concluyó que ningún influye de forma significativa en el nivel de seguridad puesto que los resultados se mantuvieron en el rango de seguridad MEDIO ALTA, entre las principales causas se encontró el desconocimiento sobre seguridad de información por parte de los usuarios.

Palabras clave: Riesgo; seguridad informática; vulnerabilidad.

Abstract

Currently having internet access is essential in the business, educational and home spheres; Since the pandemic, they have had the need to communicate and stay connected through different virtual platforms that facilitate their daily activities. Along with the benefits offered by using the Internet, there is the exposure to dangers and computer security risks that can affect the information of the users in case of not being protected; For this reason, the objective of this research work was to determine the main computer security risks to which Internet networks are exposed in homes in the city of El Carmen; The selection of 100 households in the city with Internet access was carried out, obtaining their authorization for the study, a checklist of 90 questions was applied to evaluate compliance with security controls and a vulnerability scan was carried out in the network with the free distribution OpeVAS; The collected data was processed using an electronic sheet that allowed grouping the data considering different criteria, for its subsequent analysis such as: Internet provider, type of plan, router characteristics, among others; obtaining as results that the general risk level is 55% considered as a MEDIUM HIGH level, in terms of the analysis factors it was concluded that none significantly influences the security level since the results remained in the security range MEDIUM HIGH, among the main causes was the lack of knowledge about information security on the part of the users.

Keywords: *Risk; computer security; vulnerability.*

Fecha de recibido: 29/10/2022
Fecha de aceptado: 19/12/2022
Fecha de publicado: 19/12/2022

Introducción

La tecnología informática fue desarrollada con la finalidad de ofrecer a las personas herramientas de procesamiento para grandes cantidades de información en forma precisa y rápida; desde el primer ordenar creado a finales de los años 40 y principios de los 50 su evolución y aplicación se ha diversificado existiendo en la actualidad equipos y programas para dar solución a necesidades de tratamiento de información variados. Al utilizar las personas, empresas e instituciones equipos y dispositivos informáticos para almacenar,

procesar, transmitir su información surge la incertidumbre por la seguridad de este activo valioso porque si llegase a caer en manos equivocadas las consecuencias se podrían tornar catastróficas (Curi, 2018).

Los avances tecnológicos no paran y las empresas deben adaptarse a los cambios que conllevan, y tener presente que los beneficios que traen los sistemas de información también están expuestos a riesgos de seguridad que son esencialmente posibilidad de ocurrencia de un evento no deseado, de consecuencias negativas. En nuestro contexto sobre la seguridad de los recursos de información, es importante por lo tanto que los usuarios tengan la tranquilidad que sus datos e información estén libres de peligro, sean utilizados solo por personas autorizadas y estén disponibles en el momento requerido.

En los hogares de la ciudad de El Carmen provincia de Manabí que disponen de acceso a internet existe desconocimiento sobre el nivel de exposición a riesgos de seguridad informática es por ello que se plantea la presente investigación con el objetivo de determinar el nivel de seguridad informática de las redes en los hogares de la ciudad de El Carmen, y establecer si existe relación con criterios como: proveedor servicio de internet, marca de dispositivo de conexión, plan de internet contratado.

Seguridad Informática

Según Larrocha (2017) la seguridad informática también denominada ciberseguridad o inclusive como seguridad de TI. Es una serie de técnicas, metodologías y procesos aplicados con la finalidad de que los sistemas informáticos estén protegidos de forma física y digital, con el fin de disminuir los riesgos que pueden sobrellevar los sistemas informáticos, en vista, que suelen existir hechos amenazantes de manera lógica que afectan a la información y disponibilidad del equipo (Murillo, et al., 2018). Por su parte Baca Urbina (2016) manifiesta que: es la custodia de cualquier tipo de mal e inclusive pérdida total, tiene un precio, el cual es de manera directa proporcional al tipo de defensa que se otorgue al activo. Los activos de seguridad informática son los recursos tecnológicos del entorno de toda la información comunicativa que pertenece a las organizaciones y su objetivo es la mayor difusión de información

Principios de Seguridad de la Información

Los principios de seguridad de la información según ISO 27001 son:

- **Confidencialidad:** es la propiedad que garantiza que la información sea utilizada por personas o máquinas debidamente autorizadas, utilizando para ello mecanismos como: autenticación, cifrado y autorización. (Buendía, 2013, p15)
- **Integridad:** se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, que la información que se recibe sea precia y completa, de acuerdo con los valores y expectativas del negocio. (Urbina, 2016, p13)
- **Disponibilidad:** En el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto (ISO 27001)

Riesgo

El riesgo informático se define como una dificultad que interviene en el cumplimiento de una meta o así mismo una amenaza a la pérdida de documentos. Este riesgo puede estar clasificado en ganancia o pérdida. De acuerdo con los riesgos, se hace referencia a la combinación de la frecuencia, la probabilidad y las consecuencias que podrían derivarse de la materialización de un peligro, mismo que se define como una medida del tamaño de los perjuicios ante una situación peligrosa, este se mide aceptando una cierta vulnerabilidad ante cada tipo de riesgo (Pérez Sánchez, 2017).

Vulnerabilidad

En informática una vulnerabilidad es cualquier debilidad de un activo que pueda influir negativamente el normal funcionamiento del sistema, pueden estar relacionadas a diferentes factores, errores de programación, configuración, manipulación, descuido en la utilización o escasos controles de protección frente a posibles riesgos (Gascó, 2013)

Amenaza

La amenaza informática tiende a producir daños a los sistemas tecnológicos por medio de las redes, tales como, redes domésticas (privadas), públicas o corporativas, es decir, es un acontecimiento que es ejecutado por usuarios y técnicas maliciosas que provocan un impacto negativo en recursos que presenten insuficiencias de software o físicas. (CEP, 2019).

Análisis de riesgos

Según Hernández y Baquero (2020) el análisis de riesgos es un procedimiento que es realizado con el afán, de poder determinar qué tan elevado es el riesgo e impacto sobre una amenaza al concretarse en redes o equipos tecnológicos. Permite identificar y prevenir con medidas de seguridad ante peligros y reducir consecuencias sobre pérdidas de recursos económicos, tecnológicos e incluso la información operativa en una empresa; es el uso sistemático de la información disponible para determinar la frecuencia con la que es probable que ocurran ciertos eventos y la magnitud de sus consecuencias, agregando que consiste en examinar la magnitud y la índole de los posibles efectos negativos de la introducción propuesta (Robles Torrente, 2015)

Seguridad en redes

Cuando se habla de seguridad se hace referencia a la protección a algo o alguien frente a los intrusos, es decir que la seguridad en las redes debe otorgar una garantía óptima de la mantención y protección de la información dentro de una empresa u organización, conservándola de manera: confidencial, controlada, autentificada y disponible en todo momento, por lo que para llevar a cabo una buena seguridad en las redes es necesario implementar las políticas de seguridad sujetas a la empresa. Actualmente es difícil garantizar la seguridad puesto que los atacantes denominados hackers están al asecho y no dudarán en atacar y robar la información, siendo necesario buscar la fiabilidad para que la información que viaja en la red actúe de manera normalizada. (Forero, 2017)

Las amenazas pueden ser de diferente origen y tipo:

- **Intercepción:** es cuando existen acceso a través de redes por usuarios que no son oficiales. Son capaces de acceder a los datos afectando únicamente a la confidencialidad o privacidad de la información. La ejecución de este tipo de amenaza puede resultar difícil de revelar, puesto que se basa en los documentos o usuarios que logran copiar información sin ser autorizados al observar correos y escuchar diálogos mediante llamadas. (Briceño, 2021). Es temporal o en ciertos casos se mantienen permanente porque prácticamente son hechos naturales que afectan a la disponibilidad de los activos de información y a los recursos económicos.
- **Interrupción:** es el más fácil la detección, a diferencia de la amenaza interceptación, pero tiene un alto nivel dificultad para poder solucionar el problema. En vista que son circunstancias de incendios, fallas de operación a los sistemas operativos, o fallas de electricidad etc. (Larrocha E. R., 2017)
- **Modificación:** Briceño (2021) indica que este ataque o habilidad involucra cambios de datos en el contenido de un archivo almacenado en los activos de información. Estos se relacionan directamente con la integridad y en algunos casos también con la disponibilidad de la información. Por lo regular las modificaciones se realizan en una base de datos y aplicaciones web.
- **Ingeniería Social:** esta técnica se dirige a personas de manera física o por internet para extraer datos confidenciales. El ciberdelincuente recolecta datos e información de la víctima que tiende ser afectada por medio de procedimientos básicos y rápidos. Tecnológicamente este delito es operado a través de la colocación de malware en los correos con la técnica phishing para traicionar y descubrir datos privados como claves, cuentas bancarias etc. (Villalón Huerta, 2019)
- **Generación:** en opinión del autor Avenía (2017) la amenaza de generación consiste en añadir datos ficticios en el contenido del sistema informático vulnerable. Las amenazas se catalogan como las dos siguientes: accidentales e intencionales.

Políticas de seguridad

Alude Aguilera López, (2010) que, las políticas de seguridad se encargan de recoger las directrices u objetivos de empresas con respecto a la seguridad informática. Pertenecen al grupo de política general, por tanto, debe pasar por un proceso de aprobación de las directrices expuestas. Su principal objetivo es la redacción de una política de seguridad con el fin de sensibilizar a todo el personal de las empresas, y en particular al involucrado directamente con el sistema de información.

Materiales y métodos

Para el desarrollo de la presente investigación se aplicó una auditoría de seguridad informática con las siguientes fases:

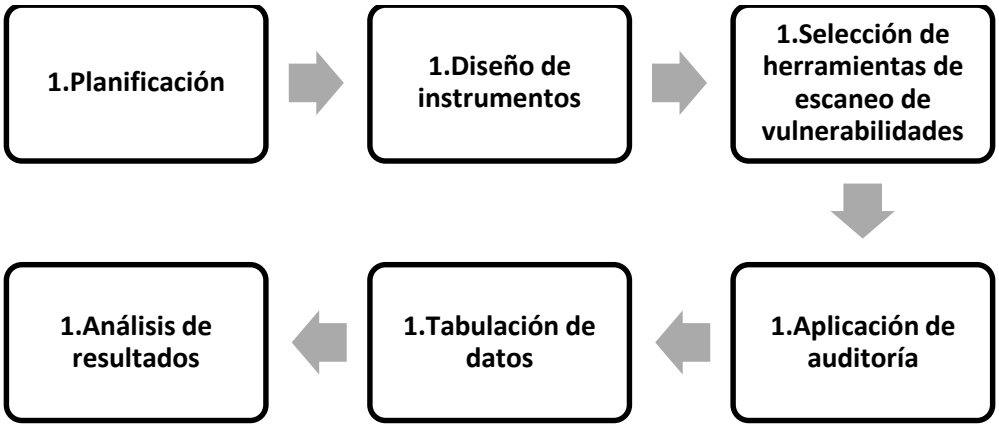


Figura 1 Fases de auditoría de seguridad

1. Planificación

Se elaboró un programa de auditoría cuyos objetivos fueron:

- Evaluar el nivel de riesgos de seguridad de las redes domésticas de la ciudad de El Carmen.
- Identificar principales vulnerabilidades de seguridad de información a las que están expuestas las redes domésticas de la ciudad de El Carmen.
- Determinar el nivel de influencia de diferentes factores en la seguridad de redes domésticas de la Ciudad de El Carmen.

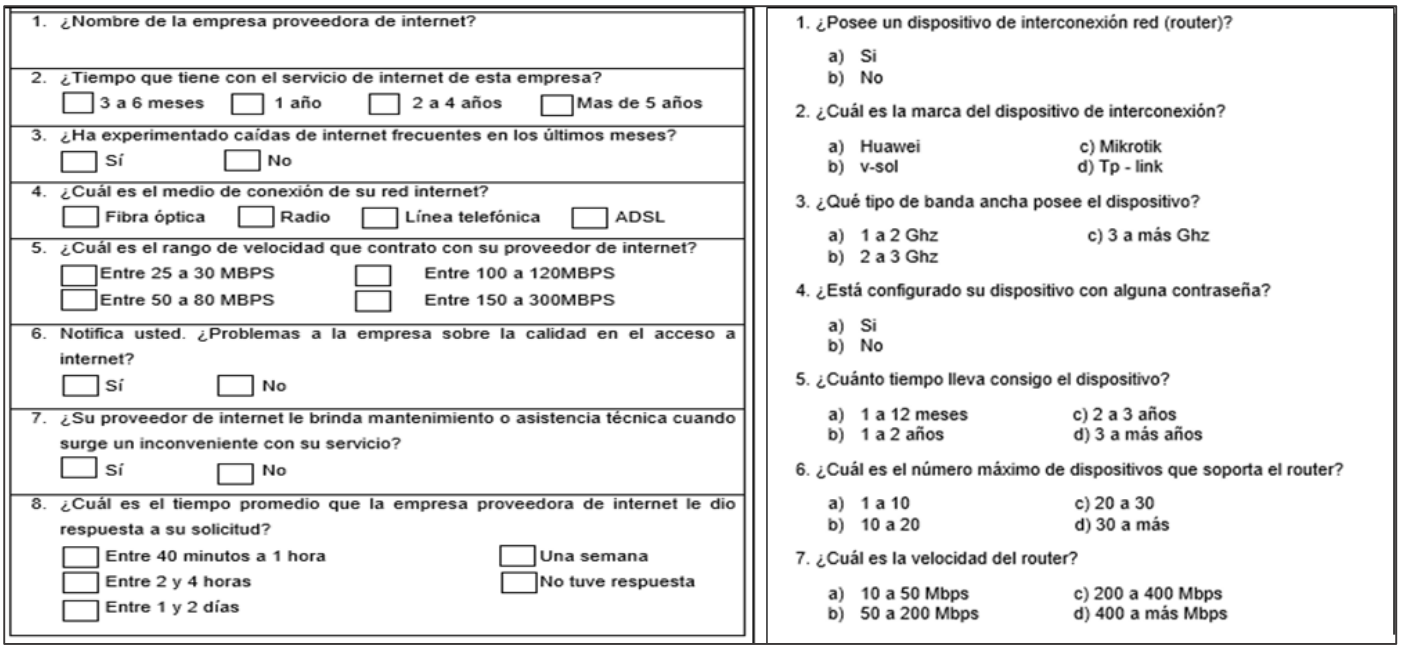
2. Diseño de instrumentos

Tomando como referencia la norma ISO 27001 segmento A9 Control de acceso y A13 Control de comunicaciones Objetivo 1: Gestión de la seguridad de red, se elaboró un checklist con 90 ítems para verificar la aplicación de políticas de seguridad incluidas en la norma Figura 2.

Nº	Cuestionario para identificar riesgos de seguridad infromática asociados a conexiones de red en hogares	CUMPLE		OBSERVACIONES
		SI	NO	
	27001 (CONTROL DE ACCESO)			
1	¿Ubica información personal en la contraseña de su Red Wifi?			
2	¿La clave de su Red Wifi está compuesta de letras?			
3	¿La clave utiliza mayúsculas y minúsculas?			
4	¿La clave está compuesta de números?			
5	¿La clave está compuesta de símbolos y caracteres?			
6	¿La contraseña de su red es fácil de descifrar?			
7	¿Cambia su contraseña frecuentemente?			
8	¿Sabe usted estructurar contraseñas seguras?			
9	¿Realiza personalmente el cambio de contraseña de su red wifi o router?			
10	¿Pide ayuda a su proveedor para el cambio de clave de su red?			
11	¿Hace uso de las mismas contraseñas para su red wifi, cuentas bancarias, aplicaciones, correos, redes sociales etc.?			
12	¿Usted comparte sus accesos o contraseñas con familiares o conocidos?			
13	¿Guarda las contraseñas en los navegadores para poder ingresar automáticamente a sus cuentas?			
14	¿Presenta problemas con la contraseña de acceso a la red al momento de conectarse con algún dispositivo?			
	ISO 27001 (A13 SEGURIDAD EN LAS COMUNICACIONES)			
15	¿Conoce alguna forma de actuar en el caso que su router presente un problema de seguridad?			
16	¿Tiene conocimiento de como actualizar al software del router de su hogar?			
17	¿Sabe administrar el router de su hogar?			
18	¿En su hogar dispone más de un router?			
19	¿Cuenta con un repetidor wifi conectado a su router?			
20	¿Ha sufrido algún daño su router en el tiempo que dispone de él?			
21	¿Se ha contactado con su Proveedor de servicio internet para solucionar inconvenientes con el router?			
22	¿Ha tenido respuestas inmediatas de su proveedor de internet cuando ha notificado problemas con su router?			
23	¿Tiene conectado su router a un regulador de voltaje para protegerlos?			
24	¿Su router se encuentra en un lugar accesible para emitir la señal a todo el hogar?			
25	¿Su router esta ubicado en un área que no afecte su funcionamiento?			
26	¿Dónde está situado el router está libre de electrodomésticos que afecte la señal?			

Figura 2 *Check list* para evaluar riesgos de seguridad de la red.

Con la finalidad de determinar factores que puedan influir en el nivel de seguridad de las redes se diseñó una encuesta para categorizar las conexiones de los hogares en el que se preguntó información sobre: proveedor de servicio de internet, tipo de conexión, características del dispositivo de conexión, entre otras, ver Figura 3.



1. ¿Nombre de la empresa proveedora de internet?

2. ¿Tiempo que tiene con el servicio de internet de esta empresa?
☐ 3 a 6 meses ☐ 1 año ☐ 2 a 4 años ☐ Mas de 5 años

3. ¿Ha experimentado caídas de internet frecuentes en los últimos meses?
☐ Sí ☐ No

4. ¿Cuál es el medio de conexión de su red internet?
☐ Fibra óptica ☐ Radio ☐ Línea telefónica ☐ ADSL

5. ¿Cuál es el rango de velocidad que contrato con su proveedor de internet?
☐ Entre 25 a 30 MBPS ☐ Entre 100 a 120MBPS
☐ Entre 50 a 80 MBPS ☐ Entre 150 a 300MBPS

6. Notifica usted. ¿Problemas a la empresa sobre la calidad en el acceso a internet?
☐ Sí ☐ No

7. ¿Su proveedor de internet le brinda mantenimiento o asistencia técnica cuando surge un inconveniente con su servicio?
☐ Sí ☐ No

8. ¿Cuál es el tiempo promedio que la empresa proveedora de internet le dio respuesta a su solicitud?
☐ Entre 40 minutos a 1 hora ☐ Una semana
☐ Entre 2 y 4 horas ☐ No tuve respuesta
☐ Entre 1 y 2 días

1. ¿Posee un dispositivo de interconexión red (router)?
a) Si
b) No

2. ¿Cuál es la marca del dispositivo de interconexión?
a) Huawei c) Mikrotik
b) v-sol d) Tp - link

3. ¿Qué tipo de banda ancha posee el dispositivo?
a) 1 a 2 Ghz c) 3 a más Ghz
b) 2 a 3 Ghz

4. ¿Está configurado su dispositivo con alguna contraseña?
a) Si
b) No

5. ¿Cuánto tiempo lleva consigo el dispositivo?
a) 1 a 12 meses c) 2 a 3 años
b) 1 a 2 años d) 3 a más años

6. ¿Cuál es el número máximo de dispositivos que soporta el router?
a) 1 a 10 c) 20 a 30
b) 10 a 20 d) 30 a más

7. ¿Cuál es la velocidad del router?
a) 10 a 50 Mbps c) 200 a 400 Mbps
b) 50 a 200 Mbps d) 400 a más Mbps

Figura 3. Encuesta sobre factores de conexión de internet.

3. Selección de herramientas de escaneo de vulnerabilidades

Como parte de la evaluación se consideró necesario la utilización de herramientas informáticas que permitan evaluar la seguridad en los dispositivos de conexión a internet, para ello, se evaluaron 4 herramientas tales como; OpenVAS, Wireshark, Zenmap y Nessus. Estas aplicaciones informáticas permiten auditar y realizar pruebas de vulnerabilidad en redes de internet domésticas, fueron seleccionadas dos para este estudio, el programa Zenmap y Openvas.

4. Aplicación de auditoría

Selección de Población y muestra

El cantón el Carmen está conformado por 4 parroquias, divididas en zonas urbanas y rurales. En las rurales consta Wilfrido Loor Moreira y San Pedro de Suma y en las urbanas el Carmen y 4 de diciembre con un total de 12.451 viviendas según censo 2010. Para este estudio se seleccionó la zona urbana, pero considerando hogares que tengan conexión a internet, debido a que el estudio requería la autorización para ejecutar un software de escaneo en la red finalmente se aplicó a 100 hogares que brindaron su colaboración estos pertenecen a los sectores de Paraíso 1, 24 de Julio y Very Loor, en el Lotización Roger, calle B y C, en Gran Chaparral, 17 de diciembre y nuevo paraíso, en el sector Las Vegas, calle Salustio Giler y Paján.

Para la obtención de datos, se contó con la colaboración de 5 estudiantes tesistas quienes visitaron en grupo cada uno de los hogares para entrevistar a representantes de cada domicilio y llenar tanto las fichas de

caracterización del hogar como el *checklist* de evaluación de riesgos. Además, con la autorización se ejecutaron los programas de escaneo de vulnerabilidades en las redes domésticas.

5. Tabulación de datos

La información recolectada de forma física en las visitas a los hogares participantes del estudio se tabuló y procesó mediante Microsoft Office, para el análisis de riesgos se aplicó la metodología Magerit. Se consideró para la valoración de riesgos la fórmula:

$$\text{GRAVEDAD DE RIESGO} = \text{PROBABILIDAD} * \text{IMPACTO} \quad (1)$$

Para el nivel de riesgos se utilizó la siguiente escala:

Tabla 1 Escala de seguridad.

Rango	Nivel de seguridad
1% - 10%	Muy bajo
11% - 30%	Bajo
31% - 50%	Medio Bajo
51% - 75%	Medio Alto
76% - 100%	Alto

Resultados y discusión

Los resultados de la investigación se describen a continuación:

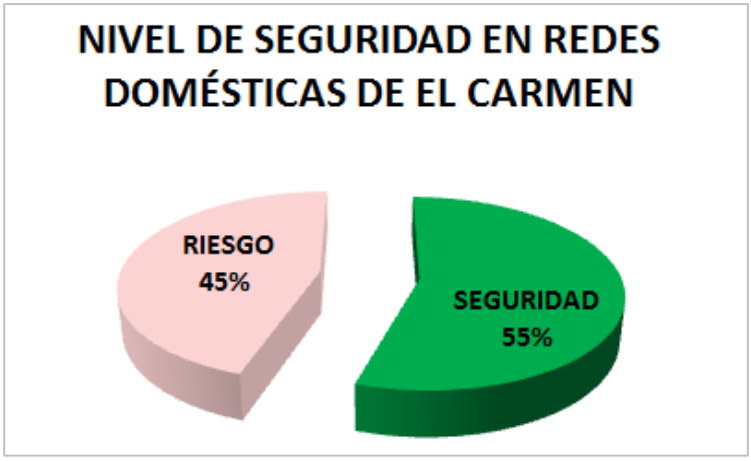


Figura 2 Nivel de seguridad general de las redes domésticas de El Carmen.

El nivel de seguridad se sitúa en MEDIO ALTO lo que significa que requiere de medidas para evitar posibles ataques ya que encuentra vulnerable. Entre las razones más recurrentes se encontraron:

- En los hogares no actualizan las contraseñas del router.
- No saben formular contraseñas seguras.
- Ingresan información personal en las contraseñas.
- Comparte las contraseñas a desconocidos.
- No tienen conocimiento al momento que el dispositivo tiende a fallar.
- No mantienen seguro las conexiones alámbricas de la red.
- En los hogares tienen desconocimiento del código de respuesta rápida.
- Desconocimiento de la capacidad que soporta el dispositivo de interconexión.
- No verifican la velocidad de respuesta del dispositivo.
- Se exceden en el número de dispositivos conectados.
- Desconocen de la cantidad de personas que se conectan en la red.
- No mantienen actualizados al antivirus.
- Desconocimiento de los virus malignos

En cuanto a los criterios considerados para analizar si tienen alguna incidencia en el nivel de seguridad de las redes se obtuvieron los siguientes resultados:

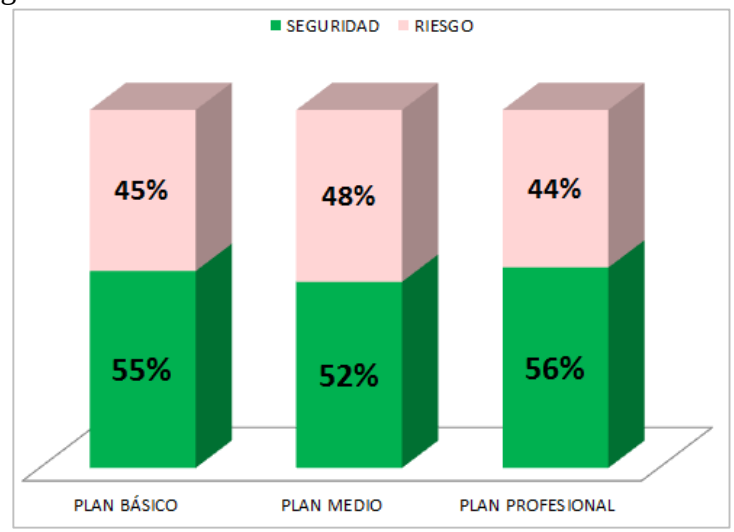


Figura 3 Nivel de seguridad según el plan de Internet contratado por el hogar.

El plan de internet contratado en los hogares no varía significativamente el nivel de seguridad de la red, debido a que se mantiene dentro del rango 51%- 75% considerado MEDIO ALTO.

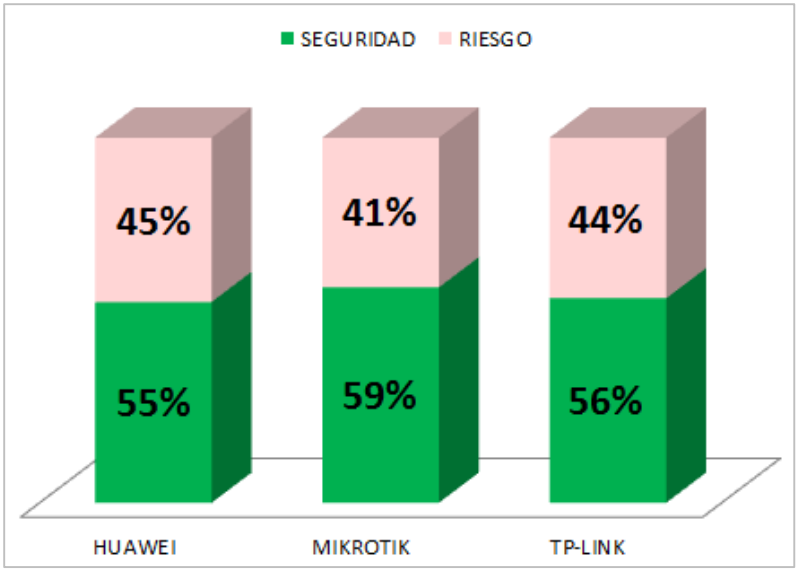


Figura 4 Nivel de seguridad de la red según marca del router del hogar

La marca de router utilizado en los hogares no influye en el nivel de seguridad, aunque se observa que aquellos de marca MICROTIK alcanzan un 59% de seguridad 4 puntos porcentuales por arriba de la seguridad general, sin embargo este valor corresponde al rango MEDIO ALTO.

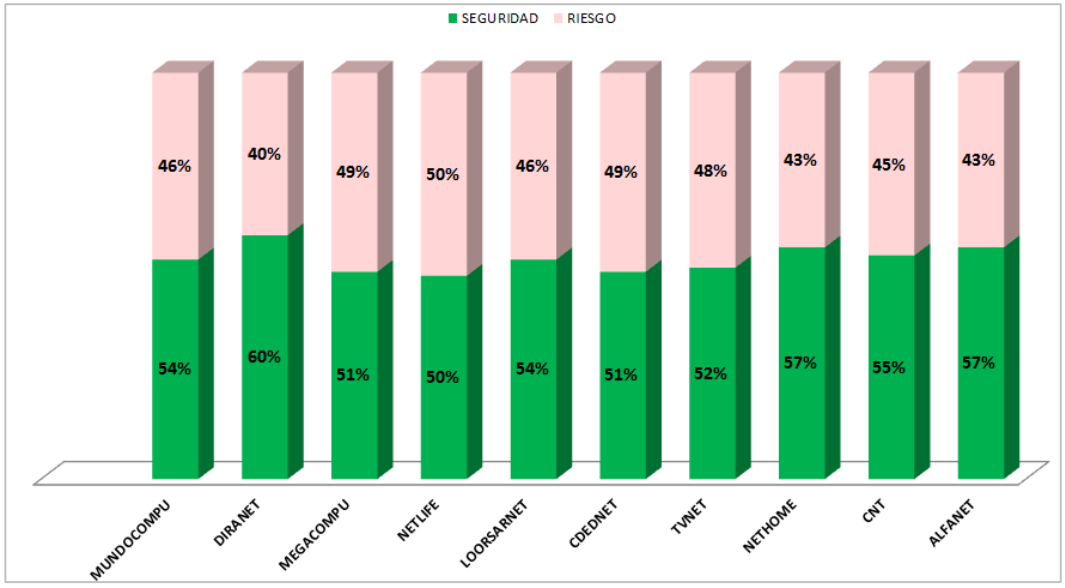


Figura 5. Nivel de seguridad de la red según Proveedor de servicio de Internet del hogar.

Analizando los resultados en relación al proveedor de servicio de internet de los hogares que participaron en el estudio, se obtiene que no hay influencia de este factor en el nivel de seguridad, existen diferencias entre

una empresa pero todas están en el rango de seguridad 51% a 75% MEDIO ALTO, cabe destacar que CDNET está en el margen inferior de la escala con 51% y DIRANET el más alto con 60%.

Tabla 2: Nivel de seguridad de redes domésticas analizadas por criterios.

Nivel de seguridad general	Según plan de internet contratado	Disponibilidad de un repetidor	Marca de dispositivo de conexión	Banda	Proveedor de internet
55%	Plan básico: 55% Plan medio: 52% PlanProfesional: 56%	SI: 57% NO:55%	Huawei: 55% Microtick: 59% Tp Link: 56%	2Gb: 53% 2 a 3 Gb: 55% 3+ Gb: 57%	Claro: 41% MundoCompu:54% NetLife: 50% Alfanet: 57% CNT: 55% NetHome: 57%

Al agrupar y comparar los datos según diferentes criterios para determinar la existencia de algún factor que influya en el nivel de seguridad de las redes domésticas de la ciudad de El Carmen se obtiene que se ubica en el mismo rango de nivel de seguridad con una diferencia porcentual en su mayoría de más menos 2 puntos porcentuales.

La principal causa de exposición a riesgos es el desconocimiento de los usuarios de los peligros que existen al utilizar la red sin las debidas precauciones, a igual conclusión llega Angie (Ovalle Vélez, 2019) en su trabajo, "Uso de herramientas informáticas para descubrir vulnerabilidades en las redes wifi domésticas" quien destaca: *" ..., se denota un uso inadecuado de las herramientas de seguridad que provee cada dispositivo (como es el uso de las actualizaciones automáticas) las cuales permiten que los dispositivos conectados no solo a la red hogareña sino también a redes externas ...., también con respecto al acceso externo desde la red por medio de la red Wifi la correcta configuración de la encriptación y clave de acceso a la red hogareña,...."* .

Conclusiones

El nivel de seguridad de las redes domésticas de los hogares de la ciudad de El Carmen es de 55% ubicándose según la escala utilizada en NIVEL MEDIO, las principales vulnerabilidades detectadas están relacionadas a la falta de conocimiento por parte de los usuarios sobre los peligros y riesgos a los que podrían exponer sus equipos en especial información personal que manejan y comparten a través de la red, misma que en caso de ser accedida por personas mal intencionadas causarían graves daños.

De los criterios que se utilizaron para analizar los resultados se concluye que ninguno influye en la seguridad de las redes de los hogares, puesto que si bien los porcentaje de seguridad oscilan entre 50 y 60% , todo este rango corresponde a NIVEL MEDIO.

La tecnología avanza y junto a los beneficios que trae se incluyen nuevos peligros que afectan a la seguridad de la información de los usuarios, es necesario evaluar los sistemas informáticos no solo empresariales sino también del hogar y personales para tomar medidas preventivas que ayuden a evitar riesgos y mitigar los posibles efectos negativos que pueden ocasionar, se recomienda que se realice de forma periódica y frecuente.

Referencias

Aguilera López, P. (2010). Seguridad informática. México: Editex.

Baca Urbina, G. (2016). Introducción a la seguridad informática. México: Patria.

Briceño, E. V. (2021). Seguridad de la información. Alzamora: Editorial Área de Innovación y Desarrollo,S.L.

CEP, E. (2019). Auxiliar Administrativo (Turno Libre). Junta de Andalucía. Temario Vol. III. Madrid: Editorial CEP S.L.

Curi, O. E. (2018). Auditoria en Sistemas. Lima: OECP.

Forero, E. B. (2017). Seguridad en redes. Colombia: Areandino.

Gascó, E. (2013). Seguridad Informática. Madrid: Macmillan Iberia.

Hernández, M., & Baquero, L. (2020). Ciclo de vida del desarrollo ágil de software seguro. Bogotá, Colombia: Los Libertadores.

Larrocha, E. R. (2017). Nuevas tendencias en los sistemas de información. Madrid - España: Editorial Universitaria Ramón Areces,S.A.

Larrocha, E., & Cortiñas, P. (2017). Nuevas tendencias en los sistemas de infromación. Madrid: Universitaroa RAmón Areces.

Murillo, Á., Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., . . . Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Alicante: Editorial Área de Innovación y Desarrollo, S.L.

Ovalle Vélez, K. (2019). Repository.ucatolica.edu.co. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/24062/1/Ciberseguridad%20WiFi%20en%20Hogares.pdf

Pérez Sánchez, V. (2017). Seguridad y salud. Málaga: IC.

Robles Torrente, D. (2015). Análisis de la seguridad privada. Barcelona: UOC.

Villalón Huerta, A. (2019). Seguridad en Unix y redes. Versión 2.1. España: Nau Llibres- Edicions Culturals Valencines, S.A.