UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN DICIEMBRE 2021 – ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

SISTEMAS DE CONTROL DE AMENAZAS EN REDES DOMÉSTICAS BASADAS EN SOLUCIONES DE BAJO COSTO.

ESTUDIANTE:

MULLO MULLO EDISON GABRIEL

TUTOR:

ING. SOTO VALLE CARLOS JULIO

AÑO 2022

ÌNDICE GENERAL

ÌNDICE DE ANEXOS

1. RESUMEN

Las amenazas en las redes domésticas son una preocupación creciente para los propietarios de hogares. Las amenazas pueden incluir virus, malware, hacker, robo de identidad y otras actividades maliciosas. La solución adecuada para proteger una red doméstica depende del presupuesto, la ubicación, el número de usuarios y el nivel de seguridad requerido. Afortunadamente, hay una variedad de soluciones de bajo costo que pueden ayudar a los propietarios de casas a proteger sus redes. Una de las opciones más económicas para proteger una red doméstica es el uso de un cortafuegos. Los cortafuegos son dispositivos que se conectan a la red para bloquear el tráfico entrante no deseado. Estos dispositivos también pueden ayudar a controlar quién puede tener acceso a la red. Algunos cortafuegos también pueden proporcionar una capa adicional de seguridad mediante la monitorización de los paquetes de datos entrantes y salientes. Otra solución de bajo costo para proteger una red doméstica es el uso de software antivirus. El software antivirus se encarga de detectar y eliminar el malware de una computadora. La mayoría de los programas antivirus también ofrecen herramientas para ayudar a los usuarios a identificar y eliminar los virus. Estas herramientas pueden ayudar a prevenir que los usuarios se vean expuestos a amenazas en línea. Un tercer método para aumentar la seguridad de una red doméstica es el uso de la criptografía. Esta técnica se utiliza para cifrar la información que se transmite a través de la red de una computadora. Esto dificulta la tarea de un hacker o un ladrón de identidad para acceder a información sensible almacenada en la red. Los usuarios pueden utilizar la criptografía para enviar y recibir información de forma segura. Finalmente, los propietarios de hogares pueden usar soluciones de bajo costo para ayudar a proteger sus redes domésticas. Estas soluciones incluyen cortafuegos, software antivirus, criptografía y otras soluciones de seguridad. Estas soluciones pueden ayudar a los usuarios a estar seguros de que sus redes domésticas están protegidas contra amenazas externas.

Palabras clave: Redes domésticas, amenazas, sistemas de control.

SUMMARY

Home network threats are a growing concern for homeowners. Threats can include viruses, malware, hackers, identity theft, and other malicious activities. The right solution to protect a home network depends on budget, location, number of users and the level of security required. Fortunately, there are a variety of low-cost solutions that can help homeowners protect their networks. One of the cheapest options to protect a home network is to use a firewall. Firewalls are devices that connect to the network to block unwanted incoming traffic. These devices can also help control who can access the network. Some firewalls can also provide an additional layer of security by monitoring incoming and outgoing data packets. Another low-cost solution to protect a home network is the use of antivirus software. Antivirus software is responsible for detecting and removing malware from a computer. Most antivirus programs also offer tools to help users identify and remove viruses. These tools can help prevent users from being exposed to online threats. A third method of increasing the security of a home network is the use of cryptography. This technique is used to encrypt information that is transmitted over a computer network. This makes it difficult for a hacker or identity thief to access sensitive information stored on the network. Users can use cryptography to send and receive information securely. Finally, homeowners can use low-cost solutions to help protect their home networks. These solutions include firewalls, antivirus software, cryptography, and other security solutions. These solutions can help users to be sure that their home networks are protected against external threats.

Keywords: Home networks, threats, control systems.

2. INTRODUCCIÓN

En este estudio de sistemas de control de amenazas en redes domesticas basadas en soluciones de bajo costo, se plantearon diversas actividades necesarias para dar solución al problema la investigación, se realizó un análisis de documentos, revistas, paginas académicas de internet con la finalidad de aportar y recopilar con información. Toda esta información recopilada sirvió como base para plasmar buenas prácticas de ciberseguridad.

Según lo explica López, M. (2022).En Ecuador ya es común hablar de Ciudad Inteligente (Smart City) , dispositivos que se conectan a los teléfonos para recopilar todo tipo de información cada vez son más comunes en los hogares, industrias, en el área de la salud y entidades gubernamentales, así como también, el acceso a internet se ha convertido en un servicio básico en los hogares ecuatorianos al establecer comunicación con todas las áreas urbanas y rurales de la región, en este sentido el gobierno, se ha visto comprometido en alcanzar un alto nivel de desarrollo digital que permita mejorar las condiciones de vida de los ciudadanos a través del uso de las tecnologías.

En este sentido resulta importante analizar las amenazas más frecuentas y evaluar los niveles de seguridad que presentan los dispositivos. La característica principal de este tipo de amenazas es el riesgo el acceso a datos personales, sitios bancarios, plataformas web y similares.

Para analizar esta problemática es necesario mencionar sus causas. Una de ellas es que el mundo del internet ha sufrido una transformación radical en los últimos tiempos, a tal punto de convertirse en el medio global de comunicación de fácil acceso y cotidiano, las amenazas se combinan y evolucionan, dando lugar a nuevas amenazas que hacen complejo el trabajo de seguridad.

Por lo cual, se convierte en un reto para el trabajo de seguridad en las redes permitiendo alcanzar una idea de hacia dónde dirigir los esfuerzos en el desarrollo de implementaciones de protección. El control de amenazas en redes domésticas basadas en

soluciones de bajo costo es una necesidad cada vez más urgente. Esto se debe a la creciente cantidad de amenazas cibernéticas que acechan a los usuarios de Internet. Los ciberataques se han vuelto cada vez más sofisticados y destructivos, lo que significa que los usuarios deben estar preparados para protegerse y sus datos.

Afortunadamente, existen soluciones de seguridad de bajo costo y fáciles de usar que pueden ayudar a los usuarios domésticos a protegerse contra amenazas como malware, ransomware, ataques de phishing y otros. Estas soluciones pueden incluir firewalls domésticos, software antivirus, filtrado de contenido, control de aplicaciones y herramientas de seguridad de redes. Estas herramientas pueden ser configuradas para bloquear el tráfico sospechoso, detectar malware y alertar al usuario cuando se encuentre una amenaza.

Además, los usuarios domésticos deben tomar precauciones básicas para aumentar su seguridad en línea. Esto incluye la creación de contraseñas seguras, la instalación de actualizaciones de software y la configuración de la seguridad de la red. Estas medidas básicas de seguridad pueden ayudar a reducir el riesgo de un ciberataque exitoso.

En resumen, el control de amenazas en redes domésticas basadas en soluciones de bajo costo es una necesidad cada vez más importante. Estas soluciones pueden ser una forma efectiva de protegerse contra amenazas cibernéticas, siempre y cuando se tomen precauciones básicas para aumentar la seguridad en línea.

3. PLANTEAMIENTO DEL PROBLEMA

El propósito de este proyecto es desarrollar una solución de bajo costo para controlar amenazas que se presentan en redes domésticas. Esta solución debe ser capaz de detectar, prevenir y bloquear amenazas como el malware, el phishing, el ransomware y el ataque de denegación de servicio (DDoS). La solución debe ser lo suficientemente robusta como para garantizar la seguridad de los datos y la privacidad de los usuarios finales, al mismo tiempo que ofrece la mejor relación calidad-precio. Además, la solución debe ser fácil de implementar y configurar, y debe ser compatible con la mayoría de los sistemas operativos y dispositivos existentes.

En la actualidad, el uso de internet y las redes domésticas es cada vez más común en el Barrio San Silvestre del Cantón Caluma, como en muchas otras partes del mundo. Sin embargo, la mayoría de los usuarios no están conscientes de las amenazas en línea y no toman las medidas necesarias para proteger sus redes domésticas. Esto se debe en gran parte a la falta de conocimiento y capacitación en cuanto a la seguridad en línea.

A pesar de que se han implementado sistemas de seguridad en el Barrio San Silvestre, como antivirus, estos sistemas no son suficientes para garantizar una protección completa de las redes domésticas. Las amenazas en línea, como virus, malware, phishing y ataques de hacking, pueden penetrar estas defensas y poner en riesgo la privacidad y seguridad de los datos de los usuarios.

El problema se agrava aún más debido a que muchos usuarios en el Barrio San Silvestre del Cantón Caluma utilizan soluciones de bajo costo para proteger sus redes domésticas. A menudo, estas soluciones no son suficientes para detectar y prevenir amenazas en línea, lo que los hace más vulnerables a los ataques cibernéticos.

Por lo tanto, es necesario analizar los sistemas de control en amenazas de redes

domésticas basadas en soluciones de bajo costo en el Barrio San Silvestre del Cantón Caluma para identificar las vulnerabilidades de seguridad existentes, definir herramientas y técnicas que permitan detectar y prevenir estas amenazas, explicar las prácticas óptimas para configurar y administrar el sistema de control de amenazas y capacitar a los usuarios sobre las mejores prácticas de seguridad en línea.

De esta manera, se busca reducir los riesgos de amenazas en línea y mejorar la seguridad de las redes domésticas en el Barrio San Silvestre del Cantón Caluma. Es importante destacar que la capacitación de los usuarios en las mejores prácticas de seguridad en línea es esencial para reducir los riesgos de amenazas y garantizar una navegación segura en la red.

Por lo tanto, este caso de estudio tiene como objetivo abordar estos problemas y proporcionar soluciones prácticas y efectivas para mejorar la seguridad de las redes domésticas en el Barrio San Silvestre del Cantón Caluma.

4. JUSTIFICACIÓN

El control de amenazas en redes domésticas basadas en soluciones de bajo costo es una solución valiosa para aumentar la seguridad de las redes domésticas, especialmente en lo que respecta a la protección contra ciberataques. Esto se debe a que la mayoría de los ciberataques, como el malware, los ataques de denegación de servicio y el robo de información, están dirigidos a sistemas de bajo costo y de menor seguridad. Estos ataques pueden amenazar la integridad de una red doméstica al permitir el acceso no autorizado, el acceso a los archivos y la modificación de los sistemas operativos.

Las soluciones de bajo costo permiten a los usuarios de redes domésticas instalar y configurar herramientas de seguridad de una forma más sencilla y económica. Estas herramientas incluyen cortafuegos, controladores de acceso y otras soluciones de seguridad. Estas herramientas se pueden configurar para proporcionar un nivel de seguridad adecuado para la red doméstica, lo que significa que los usuarios no tienen que invertir en soluciones de seguridad más caras para proteger sus datos.

Además, los usuarios pueden personalizar fácilmente la seguridad de su red doméstica mediante la configuración de reglas para bloquear direcciones de IP específicas, limitar el tráfico entrante y saliente y asegurar la conexión a Internet utilizando SSL. Estas soluciones también permiten a los usuarios realizar copias de seguridad de los datos, lo que les permite recuperar los archivos en caso de que un ataque cibernético tenga éxito.

En conclusión, el control de amenazas en redes domésticas basadas en soluciones de bajo costo es una solución importante para aumentar la seguridad de las redes domésticas. Esto significa que los usuarios de redes domésticas pueden aprovechar la seguridad y la facilidad de uso que ofrecen estas soluciones sin tener que gastar grandes cantidades de dinero en soluciones de seguridad más costosas.

El acceso a internet se ha convertido en una necesidad en la mayoría de los hogares en el Barrio San Silvestre del Cantón Caluma, permitiendo a los usuarios conectarse con el mundo y tener acceso a una variedad de servicios en línea. Sin embargo, la falta de protección adecuada de las redes domésticas puede resultar en amenazas de seguridad en línea, como virus, malware, ataques de phishing, entre otros, que pueden comprometer la privacidad y la seguridad de la información de los usuarios.

Es importante analizar los sistemas de control en amenazas de redes domésticas basadas en soluciones de bajo costo en el Barrio San Silvestre del Cantón Caluma, con el fin de proporcionar soluciones prácticas y efectivas para mejorar la seguridad de las redes domésticas y reducir los riesgos de amenazas en línea. La capacitación de los usuarios sobre las mejores prácticas de seguridad en línea también es esencial para reducir los riesgos de amenazas y garantizar una navegación segura.

Para el efecto se toma en cuenta los siguientes aspectos fundamentales:

1. La seguridad de la red doméstica debe ser una prioridad para los usuarios de Internet y debe abordarse con la misma atención que se da a la seguridad de las redes empresariales. Esto se debe a que la mayoría de los usuarios domésticos no cuentan con los recursos financieros para invertir en seguridad de alto nivel.

2. Las amenazas a la seguridad de las redes domésticas se deben abordar con soluciones de bajo costo, como el uso de firewall, el cifrado de datos, el control de acceso y el monitoreo de la red. Estas soluciones son eficaces para detectar y bloquear amenazas comunes, como el malware, el spam y los ataques de fuerza bruta.

3. Las soluciones de seguridad de bajo costo también permiten a los usuarios domésticos realizar una auditoría de la red. Esto permitirá a los usuarios identificar cualquier vulnerabilidad y tomar medidas para corregirla antes de que un atacante la

explote.

4. Los usuarios también deben considerar el uso de contraseñas seguras para proteger sus dispositivos. Las contraseñas seguras significan que los usuarios deben usar una contraseña única para cada dispositivo y que la contraseña debe ser difícil de adivinar.

5. Finalmente, los usuarios deben asegurarse de que sus dispositivos estén siempre actualizados. Esto significa que los usuarios deben instalar y mantener actualizados los parches de seguridad para sus dispositivos y aplicaciones. Esto ayudará a prevenir que los atacantes exploten vulnerabilidades conocidas.

5. OBJETIVOS

5.1 Objetivo General:

- Analizar los sistemas de control de amenazas en redes domésticas basado en soluciones de bajo costo.

5.2 Objetivos específicos:

- Identificar los riesgos de seguridad en redes domésticas para prevenir la sustracción de la información.
- Determinar el desempeño del sistema de seguridad y realizar ajustes según sea necesario.
- Proporcionar recomendaciones para la mejora continua de la seguridad de la red doméstica.

6 LÍNEAS DE INVESTIGACIÒN

Línea de investigación:

- Sistemas de información y comunicación, emprendimiento e innovación.

Sub línea de investigación:

- Redes y tecnologías inteligentes de software y hardware

7 MARCO CONCEPTUAL

7.1 Redes domésticas

Una red doméstica o LAN es un tipo de red que conecta dos o más computadoras en una ubicación residencial. Esta red permite compartir archivos entre las computadoras, así como compartir dispositivos como impresoras y escáneres que estén conectados a una sola computadora. Además, la red puede ser utilizada para compartir una conexión a Internet con múltiples dispositivos mediante el uso de un enrutador. (Mauricio, 2019)

7.2 Componentes de una red domestica

Una red doméstica se compone de varios dispositivos que se conectan entre sí para compartir recursos y datos (Taboada & Luis, 2021). Los componentes más comunes son:

1. **Router:** Es el dispositivo que permite la conexión de la red doméstica a Internet. Los routers tienen puertos Ethernet y Wi-Fi para conectar dispositivos a la red.

2. **Dispositivos finales:** Son los dispositivos que se conectan a la red para compartir recursos. Estos dispositivos pueden ser computadoras, laptops, tabletas, teléfonos inteligentes, impresoras, televisores inteligentes, entre otros.

3. **Wi-Fi:** Es una tecnología que permite la conexión inalámbrica de dispositivos a la red doméstica. Los dispositivos compatibles con Wi-Fi se conectan al router a través de una red inalámbrica.

4. **Switch:** Es un dispositivo que se utiliza para conectar varios dispositivos a la red doméstica. Los switches tienen varios puertos Ethernet para conectar dispositivos a la red.

5. **Firewall:** Es una medida de seguridad que se encarga de filtrar el tráfico de red

entrante y saliente para prevenir ataques y accesos no autorizados. Los routers modernos incluyen un firewall integrado para proteger la red doméstica.

6. **SSID:** Es el nombre de la red Wi-Fi que se utiliza para identificar la red. El SSID se configura en el router y se utiliza para conectar dispositivos a la red.

7. **Protocolos de seguridad:** Son los mecanismos utilizados para proteger la red doméstica de amenazas externas. Los protocolos de seguridad más comunes son WPA y WPA2, que utilizan encriptación para proteger la información que se transmite por la red.

7.3 Seguridad de las redes domésticas

La seguridad de la red doméstica se refiere a la protección de los dispositivos digitales que se conectan a Internet en una residencia, incluyendo puntos de acceso inalámbricos, puntos de acceso por cable y otros componentes informáticos domésticos como enrutadores, computadoras, teléfonos inteligentes, impresoras y dispositivos IoT, tales como monitores para bebés habilitados para Wi-Fi, timbres con cámara, televisores inteligentes y asistentes digitales. Las redes domésticas permiten que varios dispositivos compartan archivos, impresoras y una conexión a Internet común. (Valero & Fernando, 2021)

7.4 Controles de las redes domésticas

Los controles de seguridad de la red en la red doméstica se utilizan para proteger la accesibilidad y la confidencialidad de los datos y las redes de los dispositivos informáticos. Estos controles son contramedidas que se utilizan para reducir el riesgo de que un exploit tenga éxito y se superponen para respaldar una estrategia de seguridad de defensa en profundidad. Para garantizar que varias capas de seguridad trabajen juntas para evitar infracciones, se combinan varios tipos de controles de seguridad de red en la red doméstica. (Salcedo et al., 2020)

Los controles técnicos de seguridad son componentes de hardware y software que incluyen cortafuegos, software antivirus, encriptación y mecanismos de control de acceso. Los controles de seguridad física se enfocan en evitar el acceso físico no autorizado a los componentes de la red y utilizan Touch ID, reconocimiento facial y cámaras de vigilancia. Por último, los controles de seguridad administrativos se centran en el comportamiento del usuario y se utilizan para evitar el uso de contraseñas inseguras, desactivar el escritorio remoto y mantener la conciencia de seguridad, especialmente para el correo electrónico. (Bernabé & Corina, 2022)

7.5 Amenazas en las redes domesticas

Las redes domésticas son cada vez más comunes y populares debido a la facilidad de acceso a Internet. Estas redes permiten a los usuarios conectarse a múltiples dispositivos y compartir recursos, como archivos e impresoras, en el hogar. Sin embargo, también presentan varios riesgos de seguridad que pueden comprometer la privacidad y la confidencialidad de los datos de los usuarios (Hernández et al., 2022) . A continuación, se describen algunas de las amenazas más comunes en las redes domésticas:

- **Malware:** El malware, o software malicioso, puede propagarse a través de las redes domésticas y comprometer los dispositivos conectados. El malware puede dañar los archivos del sistema, robar información personal y financiera, y proporcionar a los atacantes acceso a los dispositivos y la red.
- **Ataques de denegación de servicio (DDoS):** Los ataques DDoS pueden inundar una red doméstica con un gran volumen de tráfico, lo que puede hacer que los dispositivos y la red se vuelvan inaccesibles. Los ataques DDoS son comúnmente utilizados para interrumpir servicios o robar información.

- **Contraseñas débiles:** Las contraseñas débiles son una vulnerabilidad común en las redes domésticas. Los atacantes pueden usar herramientas de fuerza bruta para adivinar contraseñas y acceder a dispositivos y redes. Es importante utilizar contraseñas complejas y únicas para cada dispositivo y servicio.
- **Dispositivos no seguros**: Los dispositivos IoT pueden presentar una amenaza para la seguridad de las redes domésticas si no están protegidos adecuadamente. Los dispositivos sin parches de seguridad pueden ser explotados por los atacantes para acceder a la red y otros dispositivos.

7.6 Amenazas del malware

El malware es un término genérico que se refiere a todo tipo de software malicioso diseñado para causar daño a los sistemas informáticos. El malware puede ser introducido en un sistema de varias maneras, incluyendo descargas de software malicioso, correos electrónicos de phishing, anuncios engañosos y sitios web infectados. (Larreategui & Gregorio, 2021)

Los diferentes tipos de malware incluyen virus, gusanos, troyanos, spyware, ransomware y adware. Cada tipo de malware tiene una función específica y puede causar daños de diferentes maneras. Por ejemplo, los virus se replican y se propagan a través de archivos y programas, mientras que el spyware se instala en un sistema y recopila información sin el conocimiento o consentimiento del usuario.

Los efectos del malware pueden ser devastadores, incluyendo la pérdida de datos, el robo de información personal y financiera, y la toma de control del sistema. Los ciberdelincuentes utilizan el malware para obtener beneficios financieros, robar información, espiar a los usuarios y realizar ataques en línea. (Guevara-Vega et al., 2023)

7.6.1 Ataques a dispositivos IoT

Los dispositivos IoT (Internet de las cosas, por sus siglas en inglés) se han vuelto cada vez más comunes en los hogares, y pueden incluir desde electrodomésticos hasta cámaras de seguridad. Sin embargo, estos dispositivos suelen tener medidas de seguridad débiles y a menudo son vulnerables a ataques. Los atacantes pueden acceder a los dispositivos y utilizarlos como puerta de entrada a la red doméstica, poniendo en riesgo la seguridad de todos los dispositivos conectados. Para prevenir estos ataques, es importante asegurarse de que los dispositivos IoT estén actualizados y tengan contraseñas seguras. (Echazú, 2022)

7.6.2 Phishing

El phishing es una técnica de ingeniería social en la que los atacantes intentan engañar a los usuarios para que divulguen información personal o financiera. Los correos electrónicos de phishing pueden parecer legítimos, con mensajes que parecen ser de empresas conocidas o instituciones financieras, pero en realidad son falsos y están diseñados para engañar al usuario. Los ataques de phishing pueden llevar a la pérdida de información personal y financiera, así como a la instalación de malware en la red doméstica. Para evitar ser víctima de phishing, es importante no abrir correos electrónicos sospechosos o hacer clic en enlaces desconocidos. (Basit et al., 2021)

7.6.3 Ataques de fuerza bruta a contraseñas

Los ataques de fuerza bruta a contraseñas son un tipo de ataque en el que los atacantes intentan adivinar la contraseña correcta utilizando un software que prueba diferentes combinaciones de caracteres. Las contraseñas débiles o fáciles de adivinar son más susceptibles a este tipo de ataques. Si los atacantes logran adivinar la contraseña correcta, pueden acceder

a la red doméstica y a la información confidencial de los usuarios. Para prevenir estos ataques, es importante utilizar contraseñas fuertes y cambiarlas periódicamente. (Jain & Gupta, 2022)

7.6.4 Sistemas de control de amenazas

Los sistemas de control de amenazas son herramientas y tecnologías utilizadas para proteger las redes y los sistemas informáticos contra diversas amenazas. Estos sistemas tienen como objetivo detectar, prevenir y responder a las posibles amenazas de seguridad que puedan comprometer la integridad, la disponibilidad y la confidencialidad de los datos y la información en la red. (Morán & José, 2021)

7.7 Tipos de sistemas

Existen varios tipos de sistemas de control de amenazas, incluyendo firewalls, antivirus, anti-malware, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), sistemas de gestión de vulnerabilidades (VMS), sistemas de autenticación de usuarios, entre otros. Cada uno de estos sistemas tiene un propósito específico y una funcionalidad única. (Sánchez-Sánchez et al., 2021)

7.8 Características de los sistemas

Las características de los sistemas de control de amenazas pueden variar dependiendo del tipo de sistema y la tecnología utilizada. Algunas características comunes incluyen la capacidad de identificar y bloquear amenazas, la escalabilidad, la interoperabilidad con otros sistemas, la facilidad de uso, la personalización y la flexibilidad.

7.9 Funciones de los sistemas

Las funciones de los sistemas de control de amenazas incluyen la monitorización y el análisis del tráfico de red, la detección y la prevención de intrusiones, el análisis de vulnerabilidades y la gestión de parches, la autenticación de usuarios, la gestión de políticas de seguridad y la respuesta ante incidentes.

7.10 Arquitecturas

Las arquitecturas de los sistemas de control de amenazas pueden variar dependiendo del tipo de sistema y la organización. Algunos sistemas se integran en la red como dispositivos físicos, mientras que otros se implementan como software en sistemas operativos (Carrión-Barco et al., 2021). La arquitectura también puede incluir componentes de nube o servicios de seguridad gestionados.

7.11 Limitaciones

Los de los sistemas de control de seguridad para redes domésticas: A pesar de que los sistemas de control de seguridad pueden ser eficaces para proteger las redes domésticas, tienen ciertas limitaciones que deben ser consideradas. Algunas de estas limitaciones incluyen:

1. **Limitaciones técnicas:** Los sistemas de control de seguridad pueden ser limitados por la capacidad técnica de los dispositivos conectados a la red. Algunos dispositivos pueden no ser compatibles con los sistemas de control o pueden no tener suficiente capacidad para ejecutarlos adecuadamente.
2. **Falta de actualizaciones:** Los sistemas de control de seguridad requieren actualizaciones regulares para mantenerse al día con las últimas amenazas y

vulnerabilidades. Si estas actualizaciones no se realizan de manera regular, la red y los dispositivos conectados pueden quedar expuestos a nuevas amenazas.

3. **Error humano:** Los sistemas de control de seguridad pueden ser ineficaces si los usuarios no los utilizan adecuadamente. Las contraseñas débiles, la falta de actualización de software y el uso de dispositivos no seguros pueden hacer que los sistemas de control sean ineficaces.
4. **Costo:** Algunos sistemas de control de seguridad pueden ser costosos de implementar y mantener. Esto puede ser un obstáculo para los usuarios que buscan proteger su red doméstica.

7.12 Herramientas y técnicas de monitoreo y detección de amenazas en sistemas informáticos

Las herramientas y técnicas de monitoreo y detección de amenazas en sistemas informáticos son esenciales para garantizar la seguridad y protección de los sistemas y datos. Cada una de estas herramientas tiene características y funciones específicas, y su implementación depende de los requerimientos específicos de cada sistema y de los riesgos de amenazas existentes. (Navas & Alexander, 2021)

1. **Firewall:** es una herramienta de seguridad que se utiliza para monitorear y controlar el tráfico de red que entra y sale de una red. El firewall se encarga de bloquear el tráfico no autorizado y permitir el tráfico legítimo. Los firewalls pueden ser de software o hardware y se pueden configurar para bloquear ciertos tipos de tráfico y permitir otros.
2. **Antivirus:** el software antivirus es una herramienta de seguridad que se utiliza para detectar y eliminar virus, gusanos y otro tipo de malware de una computadora o red. El software antivirus se actualiza regularmente para detectar nuevas amenazas y mantener la protección contra ellas.

3. **Anti-malware**: el software anti-malware es una herramienta de seguridad que se utiliza para detectar y eliminar todo tipo de malware, incluyendo virus, spyware, adware, troyanos y otros. El software anti-malware utiliza técnicas de detección avanzadas para identificar amenazas y limpiar el sistema afectado.
4. **Sistemas de detección de intrusiones (IDS):** los sistemas de detección de intrusiones son herramientas de seguridad que monitorean la actividad de la red en busca de comportamientos sospechosos y ataques de intrusos. Los IDS alertan a los administradores de red sobre las posibles amenazas y les permiten tomar medidas preventivas para evitar el acceso no autorizado a la red.
5. **Sistemas de prevención de intrusiones (IPS):** los sistemas de prevención de intrusiones son herramientas de seguridad que se utilizan para prevenir los ataques de intrusos mediante la detección y bloqueo de tráfico malicioso en tiempo real. Los IPS son similares a los IDS, pero en lugar de simplemente alertar sobre las posibles amenazas, bloquean activamente el tráfico malicioso antes de que pueda llegar a su destino.
6. **Análisis de vulnerabilidades:** el análisis de vulnerabilidades es una técnica de seguridad que se utiliza para identificar las debilidades en los sistemas y aplicaciones de la red. Esta técnica puede ser realizada manualmente o con herramientas automatizadas para identificar y clasificar las vulnerabilidades, así como para sugerir medidas correctivas.
7. **Análisis de registro de eventos:** el análisis de registro de eventos es una técnica de seguridad que se utiliza para revisar los registros de eventos de la red para identificar cualquier actividad sospechosa. Los registros de eventos pueden proporcionar información valiosa sobre los intentos de acceso no autorizado, las vulnerabilidades de la red y las actividades maliciosas. (Chango & Damian, 2020)

7.13 Ingeniería social

La ingeniería social se refiere a la estrategia de manipular, influir o engañar a un individuo con el objetivo de obtener acceso a sistemas informáticos o robar información personal o financiera. Se basa en técnicas de manipulación psicológica para engañar a los usuarios para que cometan errores de seguridad o divulguen información confidencial. (Ortiz Lozano et al., 2019)

Los ataques de ingeniería social pueden involucrar varios pasos. En primer lugar, el atacante investiga a su posible víctima para recopilar información previa relevante, como debilidades en los protocolos de seguridad o puntos de entrada. Posteriormente, el perpetrador utiliza técnicas de pretexto, como la suplantación de identidad, para ganar la confianza de la víctima y provocar acciones que incumplen las prácticas de seguridad, como la divulgación de información confidencial o la concesión de acceso a recursos críticos.

Clasificar los tipos de ataques de ingeniería social puede ser difícil, ya que los atacantes pueden usar una variedad de técnicas para engañar a sus víctimas. Algunos ejemplos incluyen el phishing, donde se engaña a la víctima para que revele información confidencial a través de correos electrónicos fraudulentos, y el "vishing", donde se utilizan llamadas telefónicas para obtener información confidencial de la víctima.

La ingeniería social también puede ocurrir en persona, donde un atacante puede usar la persuasión o la intimidación para obtener acceso no autorizado a una red o sistema. Es importante que los usuarios estén al tanto de estos riesgos y tomen medidas para protegerse contra ellos. (Olmedo & Chaves, 2020)

7.14 Soluciones de bajo costo

La seguridad en línea es una preocupación importante en la era digital en la que vivimos, especialmente en lo que respecta a nuestras redes domésticas. Con tantos dispositivos conectados a Internet en nuestros hogares, desde computadoras y teléfonos inteligentes hasta dispositivos IoT como cámaras de seguridad, la necesidad de proteger nuestra red de amenazas externas es más importante que nunca. Afortunadamente, existen soluciones de seguridad asequibles y accesibles que pueden ayudar a proteger nuestra red doméstica contra virus, malware y otros tipos de amenazas. En este texto, exploraremos algunas opciones de seguridad gratuitas y de bajo costo para ayudar a los usuarios a proteger su red doméstica. (Castan & Antonio, 2021)

- **Antivirus gratuito:** Hay varias opciones de software antivirus gratuito que ofrecen protección básica contra malware y virus. Algunos ejemplos son Avast, AVG y Bitdefender.
- **Firewall integrado:** Muchos routers modernos vienen con un firewall integrado que puede configurarse para proteger la red doméstica de amenazas externas.
- **Solución de seguridad todo en uno:** Algunas compañías de seguridad ofrecen soluciones de seguridad todo en uno a un precio asequible para proteger múltiples dispositivos y redes. Ejemplos incluyen Norton 360 y McAfee Total Protection.
- **VPN gratuita:** Una VPN (red privada virtual) puede ayudar a proteger la privacidad en línea y mantener segura la información transmitida en una red doméstica. Hay opciones de VPN gratuitas, como ProtonVPN y Windscribe.
- **Actualizaciones regulares:** La actualización regular de software y firmware en dispositivos y routers es una forma importante y a menudo pasada por alto de mantener

la seguridad en una red doméstica. A menudo, estas actualizaciones pueden ser gratuitas y proporcionar protección adicional contra vulnerabilidades conocidas.

Es importante tener en cuenta que ninguna solución de seguridad es infalible y siempre se recomienda una combinación de soluciones para proteger la red doméstica de amenazas. Además, es importante evaluar regularmente las soluciones de seguridad implementadas y ajustarlas según sea necesario para garantizar la protección óptima de la red y sus dispositivos.

Por otra parte, las soluciones de seguridad de bajo costo pueden ser una opción adecuada para aquellos usuarios que no requieren un alto nivel de seguridad o que tienen un presupuesto limitado. Estas soluciones suelen incluir características básicas de protección, como un firewall básico, protección contra malware y filtrado de contenido web. Sin embargo, es importante tener en cuenta que estas soluciones pueden no ser suficientes para proteger contra amenazas avanzadas y sofisticadas. (Cañizares Rivera & Chacha Murillo, 2022)

Es recomendable que los usuarios investiguen y comparen diferentes soluciones de seguridad de bajo costo antes de seleccionar una. Es importante evaluar las características de seguridad que se ofrecen, así como también la reputación del proveedor de la solución. Además, se debe considerar la facilidad de uso de la solución y la compatibilidad con los dispositivos de la red doméstica. En última instancia, la elección de una solución de seguridad de bajo costo debe basarse en las necesidades y requisitos de seguridad específicos de cada usuario.

8 MARCO METODOLÓGICO

Las redes domésticas se han convertido en una parte esencial de nuestras vidas, y cada vez dependemos más de ellas para realizar nuestras actividades cotidianas. Sin embargo, con el aumento de la conectividad, también ha aumentado el riesgo de sufrir ciberataques y amenazas a la seguridad de nuestros dispositivos y datos personales. Para mitigar estos riesgos, se han desarrollado diversas soluciones de seguridad, incluyendo antivirus gratuitos, firewalls integrados, soluciones todo en uno y VPNs gratuitas, entre otros. (Sánchez-Sánchez et al., 2021)

Para evaluar la eficacia de estas soluciones en la protección de las redes domésticas, es importante realizar un estudio sistemático que utilice metodologías adecuadas. En este estudio, se utilizarán tres metodologías complementarias: la metodología aplicada, que permitirá probar las soluciones en un ambiente controlado y medir su impacto; la metodología descriptiva, que permitirá describir los distintos tipos de amenazas que enfrentan las redes domésticas y las soluciones de seguridad que se han desarrollado para abordarlas; y la metodología bibliográfica, que permitirá analizar la literatura existente sobre el tema y recopilar información relevante para el estudio.

A través de la combinación de estas metodologías, se espera obtener una visión integral de las soluciones de seguridad disponibles para las redes domésticas, así como su eficacia y limitaciones en la protección contra amenazas cibernéticas. Esta información permitirá a los usuarios de redes domésticas tomar decisiones informadas sobre qué soluciones de seguridad utilizar para proteger sus dispositivos y datos personales.

8.1 Identificación de la amenaza

Con el fin de controlar las amenazas en las redes domésticas basadas en soluciones de bajo costo, es necesario identificar las amenazas existentes. Esto incluiría amenazas como el malware, el spam, los ataques de denegación de servicio, la intrusión y el phishing.

8.2 Evaluación de riesgos

Una vez identificados los riesgos, es necesario evaluar su potencial impacto en la red y los dispositivos conectados. Esta evaluación debe incluir un análisis de las vulnerabilidades existentes, el potencial de propagación de la amenaza y los recursos disponibles para combatirla.

8.3 Establecer medidas de seguridad

Una vez que se ha evaluado el riesgo, es necesario establecer medidas de seguridad adecuadas para prevenir o controlar la amenaza. Estas medidas pueden incluir el uso de herramientas de seguridad, como firewalls, antivirus y antispyware, y la implementación de políticas de seguridad estrictas.

8.4 Implementación de la solución

Una vez que se han definido las medidas de seguridad, es necesario implementar la solución de seguridad. Esto incluiría la configuración de los dispositivos y la actualización del software.

8.5 Seguimiento y evaluación

Por último, es importante llevar a cabo un seguimiento y evaluación periódicos para asegurarse de que las medidas de seguridad se están implementando correctamente y que la red está a salvo de amenazas. Esto incluye realizar pruebas de penetración, realizar auditorías de seguridad y mantener un registro de incidentes.

9 RESULTADOS

En general, los resultados de la encuesta indican que los usuarios tienen cierto nivel de conocimiento en cuanto a virus informáticos y malware, y están tomando medidas para proteger sus dispositivos al instalar software antivirus y actualizar el software y firmware en sus dispositivos y router. Sin embargo, hay áreas en las que los usuarios podrían mejorar su seguridad en línea, como el uso de contraseñas seguras y diferentes para sus diferentes cuentas en línea y la configuración de un firewall en su router para proteger su red doméstica.

1. **¿Has oído hablar de virus informáticos y malware?**

   Resultados: 10 personas encuestadas.

- 10 personas (100%) respondieron afirmativamente.

Análisis: El 100% de las personas encuestadas han oído hablar de virus informáticos y malware, lo que indica que estos términos son bastante conocidos para los usuarios.

2. **¿Has instalado algún tipo de software antivirus en tu dispositivo?**

   Resultados: 10 personas encuestadas.

- 7 personas (70%) respondieron afirmativamente.
- 3 personas (30%) respondieron negativamente.

Análisis: El 70% de las personas encuestadas han instalado algún tipo de software antivirus en sus dispositivos, lo que indica que la mayoría de los usuarios están tomando medidas para proteger sus dispositivos. Sin embargo, el 30% de las personas no han instalado software antivirus, lo que representa un riesgo potencial para su seguridad.

3. **¿Utilizas contraseñas seguras y diferentes para tus diferentes cuentas en línea?**

   Resultados: 10 personas encuestadas.

- 4 personas (40%) respondieron afirmativamente.
- 6 personas (60%) respondieron negativamente.

Análisis: El 40% de las personas encuestadas utilizan contraseñas seguras y diferentes

para sus diferentes cuentas en línea, lo que indica que algunos usuarios están tomando medidas para proteger sus cuentas en línea. Sin embargo, el 60% de las personas no utilizan contraseñas seguras y diferentes, lo que representa un riesgo potencial para la seguridad de sus cuentas en línea.

4. **¿Actualizas regularmente el software y firmware en tus dispositivos y router?**

   Resultados: 10 personas encuestadas.

- 8 personas (80%) respondieron afirmativamente.
- 2 personas (20%) respondieron negativamente.

Análisis: El 80% de las personas encuestadas actualizan regularmente el software y firmware en sus dispositivos y router, lo que indica que la mayoría de los usuarios están tomando medidas para mantener sus dispositivos seguros y actualizados. Sin embargo, el 20% de las personas no actualizan regularmente su software y firmware, lo que representa un riesgo potencial para la seguridad de sus dispositivos.

5. **¿Has configurado un firewall en tu router para proteger tu red doméstica?**

   Resultados: 10 personas encuestadas.

- 5 personas (50%) respondieron afirmativamente.
- 5 personas (50%) respondieron negativamente.

Análisis: El 50% de las personas encuestadas han configurado un firewall en su router para proteger su red doméstica, lo que indica que algunos usuarios están tomando medidas para proteger su red. Sin embargo, el 50% de las personas no han configurado un firewall, lo que representa un riesgo potencial para la seguridad de su red doméstica.

6. **¿Has escuchado hablar de soluciones de seguridad todo en uno?**

   Resultados: 10 personas encuestadas.

- 3 personas (30%) respondieron afirmativamente.
- 7 personas (70%) respondieron negativamente.

Análisis: El 30% de las personas encuestadas han oído hablar de soluciones de seguridad todo en uno, lo que indica que estos términos no son muy conocidos para algunos usuarios. El 70% de las personas no han escuchado hablar de soluciones de seguridad todo en uno.

10 DISCUSIÓN DE RESULTADOS

Es alentador ver que el 100% de los encuestados han oído hablar de virus informáticos y malware, lo que indica que los usuarios tienen cierto nivel de conciencia sobre los riesgos de seguridad en línea. Además, el 70% de los encuestados han instalado algún tipo de software antivirus en sus dispositivos y el 80% actualizan regularmente el software y firmware en sus dispositivos y router, lo que demuestra que los usuarios están tomando medidas para proteger sus dispositivos.

Sin embargo, el hecho de que solo el 40% de los encuestados utilicen contraseñas seguras y diferentes para sus diferentes cuentas en línea y solo el 50% hayan configurado un firewall en su router para proteger su red doméstica indica que hay áreas en las que los usuarios necesitan mejorar su seguridad en línea. Esto es especialmente preocupante dado el aumento de los ataques de phishing y la facilidad con la que los hackers pueden acceder a las cuentas en línea a través de contraseñas débiles o reutilizadas. En general, se recomienda que los usuarios se capaciten más sobre las mejores prácticas de seguridad en línea para garantizar una protección más efectiva de sus dispositivos y datos personales.

11 CONCLUSIONES

En la actualidad hay una gran cantidad de soluciones de bajo costo para el control de amenazas en redes domésticas. Estas soluciones incluyen software de seguridad, firewalls, antivirus, IDS, IPS y aplicaciones de control de contenido. Estas soluciones son adecuadas para el uso doméstico y pueden proporcionar un nivel razonable de seguridad si se utilizan de forma adecuada. Sin embargo, los usuarios deben asegurarse de que estas soluciones se mantienen actualizadas y se instalan correctamente para garantizar una protección óptima. Además, los usuarios deben asegurarse de conocer los riesgos que implica el uso de Internet y mantener una buena higiene informática para mantener sus sistemas seguros.adas en soluciones de bajo costo. Se han discutido los diferentes enfoques y soluciones disponibles para mitigar los riesgos, incluyendo el uso de software de seguridad, la configuración de firewalls y la adopción de mejores prácticas de seguridad.

Además, se ha analizado la importancia de mantener actualizado el software, la necesidad de realizar copias de seguridad y el uso de soluciones de seguridad basadas en la nube para aumentar la protección.

En conclusión, el control de amenazas en redes domésticas basadas en soluciones de bajo costo es posible con el uso de las soluciones adecuadas. Los usuarios principiantes deberían considerar la adopción de una solución de seguridad integrada que ofrezca una protección robusta a un precio asequible.

- Las redes domésticas son vulnerables a una variedad de amenazas en línea y los usuarios deben estar conscientes de estas amenazas para tomar medidas preventivas adecuadas.

- La implementación de soluciones de seguridad gratuitas y de bajo costo, como el antivirus gratuito, el firewall integrado y las soluciones de seguridad todo en uno, puede proporcionar una protección básica pero efectiva contra el malware y las amenazas en

línea.

- Es importante que los usuarios mantengan sus dispositivos y routers actualizados con las últimas actualizaciones de software y firmware para evitar vulnerabilidades conocidas.

- La educación y capacitación de los usuarios sobre las mejores prácticas de seguridad en línea son fundamentales para prevenir las amenazas en línea en la red doméstica.

12 RECOMENDACIONES

- Usar un firewall: un firewall es una herramienta efectiva para evitar amenazas de red. Un buen firewall puede bloquear el tráfico no deseado y ayudar a proteger su red de ataques externos.
- Establecer un control de acceso: un control de acceso estricto es esencial para la seguridad de una red doméstica. Establecer reglas estrictas sobre quién puede y no puede acceder a la red es una forma eficaz de evitar amenazas. Instalar un software antivirus: un software antivirus es una de las mejores herramientas para detectar y prevenir amenazas de seguridad. Es importante asegurarse de que el software antivirus esté actualizado y configurado para detectar las últimas amenazas.
- Utilizar el cifrado: el cifrado es una forma eficaz de proteger la información en su red. Esto puede ayudar a evitar que los hackers accedan a la información confidencial almacenada en su red.
- Utilizar una conexión segura: al utilizar una conexión segura, puede evitar que los hackers accedan a su red. Esto también ayuda a prevenir intercepciones de contraseñas y otra información confidencial.
- Utilizar un cortafuegos en el router: los routers con cortafuegos incorporados son una forma efectiva de proteger su red doméstica. El cortafuegos ayuda a bloquear el tráfico entrante y saliente no deseado.
- Utilizar la seguridad Wi-Fi: la seguridad Wi-Fi es una forma útil de proteger su red doméstica de amenazas externas. Es importante configurar la seguridad Wi-Fi para proteger su red de intrusos no autorizados.

13 REFERENCIAS

López, M. (2022). Análisis de amenazas IOT en un sistema domótico. Pontifica Universidad Católica del Ecuador. Repositorio PUCE. https://repositorio.pucesa.edu.ec/bitstream/123456789/3769/1/78202.pdf

Basit et al., (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Bernabé, O., & Corina, N. (2022). *"Análisis cuantitativo y cualitativo de la seguridad en las redes domésticas del sector Sauces VIII. Guayaquil- Ecuador"*. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones.

Cañizares Rivera, E. A., & Chacha Murillo, M. A. (2022). *Evaluación de ataques ddos a un sistema de red y sus diferentes formas de protección*. Ecuador: Latacunga: Universidad Técnica de Cotopaxi (UTC).

Carrión-Barco, G., Sánchez-Chero, M.-J., Del Castillo Castro, C. I., Campos Flores, F. W., & Timaná Alvarez, M. (2021). Modelo de seguridad informática para un medio de conexión pública. *Revista de la Universidad del Zulia*, *12*(32), 344–357. https://doi.org/10.46925//rdluz.32.21

Castan, S., & Antonio, C. (2021). *Integridad y confidencialidad de datos en redes IoT LoRaWan*. http://192.100.164.85/handle/20.500.12249/2757

Chango, T., & Damian, C. (2020). *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A*. Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos.

Echazú, J. R. (2022). *Inteligencia artificial y aprendizaje automático para prevención de*

ataques DDoS en dispositivos IoT. https://ri.itba.edu.ar/entities/trabajo%20final%20de%20especializaci%C3%B3n/94c6c5d0-6783-40ca-88fc-04a49ef45dbb

Guevara-Vega et al., 2023. Vulnerabilidades y amenazas en los activos de información: Una revisión sistemática. *Revista Científica de Sistemas e Informática*, *3*(1), e461. https://doi.org/10.51252/rcsi.v3i1.461

Hernández, C. G. P., Pinchao, R. S. R., & Macías, R. W. M. (2022). Seguridad Informática de Redes Domésticas de la ciudad de El Carmen. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS - ISSN 2806-5794.*, *4*(6), 447–459. http://www.editorialalema.org/index.php/pentaciencias/article/view/373

Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527–565. https://doi.org/10.1080/17517575.2021.1896786

Larreategui, P., & Gregorio, J. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso*.

Mauricio, A. M. C. (2019). *EL ESTADO DEL ARTE SOBRE EL INTERNET DE LAS COSAS. AMENAZAS Y VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EVIDENCIADAS DESDE LA DOMOTICA*. https://repository.unad.edu.co/handle/10596/28446

Morán, C., & José, M. (2021). *Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones*.

Navas, V., & Alexander, N. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*.

Olmedo, M. R. M., & Chaves, V. E. J. (2020). Seguridad de la información en plataformas e-

learning en tiempos de pandemia COVID-19. *Revista UNIDA Científica*, *4*(1). https://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/9

Ortiz Lozano et al., (2019). La representación social de la problemática ambiental en profesores de ingeniería civil, de la Escuela Superior de Ingeniería y Arquitectura del Instituto Politécnico Nacional. *Revista de la educación superior*, *48*(190), 185–209. https://doi.org/10.36857/resu.2019.190.716

Salcedo et al., (2020). METODOLOGÍA PARA EVALUACIÓN DE SISTEMAS INFORMÁTICOS UTILIZANDO TÉCNICAS DE ETHICAL HACKING EN PLATAFORMAS DE HARDWARE Y SOFTWARE LIBRE. *Encuentro Internacional de Educación en Ingeniería ACOFI 2020*.

Sánchez-Sánchez et al.,(2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *CIT Informacion Tecnologica*, *32*(5), 121–128. https://doi.org/10.4067/s0718-07642021000500121

Taboada, P., & Luis, J. (2021). *La calidad del sistema de red y la satisfacción del personal usuario de la oficina de informática del gobierno regional de lima*. Universidad Nacional José Faustino Sánchez Carrión.

Valero, H., & Fernando, D. (2021). *Manual de buenas prácticas de seguridad informática en redes domésticas*. https://repository.unad.edu.co/handle/10596/39430

ANEXOS

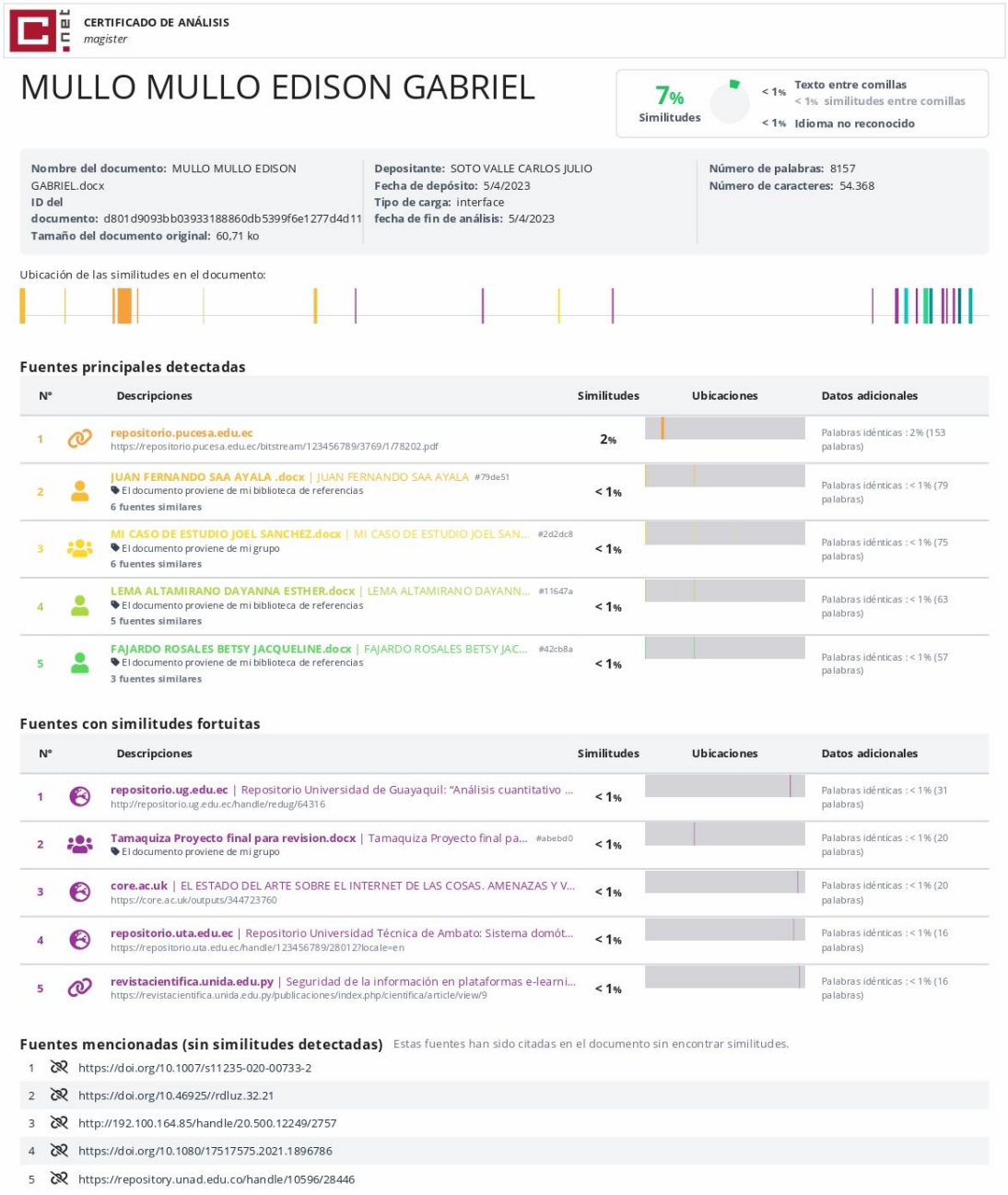
ANEXO A1.- Explicación sobre las amenazas en las redes domésticas y como poder prevenirlas


GUESS

ANEXO B1.- ENCUESTA

1. **¿Has oído hablar de virus informáticos y malware?**
    - Si
    - No
2. **¿Has instalado algún tipo de software antivirus en tu dispositivo?**
    - Si
    - No
3. **¿Utilizas contraseñas seguras y diferentes para tus diferentes cuentas en línea?**
    - Si
    - No
4. **¿Actualizas regularmente el software y firmware en tus dispositivos y router?**
    - Si
    - No
5. **¿Has configurado un firewall en tu router para proteger tu red doméstica?**
    - Si
    - No
6. **¿Has escuchado hablar de soluciones de seguridad todo en uno?**
    - Si
    - No

ANEXO C1.- Reporte anti-plagio



CERTIFICADO DE ANÁLISIS
magister

MULLO MULLO EDISON GABRIEL

7% Similitudes

< 1% Texto entre comillas
< 1% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: MULLO MULLO EDISON GABRIEL.docx
ID del documento: d801d9093bb03933188860db5399f6e1277d4d11
Tamaño del documento original: 60,71 ko

Depositante: SOTO VALLE CARLOS JULIO
Fecha de depósito: 5/4/2023
Tipo de carga: interface
fecha de fin de análisis: 5/4/2023

Número de palabras: 8157
Número de caracteres: 54.368

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.pucesa.edu.ec https://repositorio.pucesa.edu.ec/bitstream/123456789/3769/1/78202.pdf	2%		Palabras idénticas : 2% (153 palabras)
2	JUAN FERNANDO SAA AYALA .docx | JUAN FERNANDO SAA AYALA #79de51 El documento proviene de mi biblioteca de referencias 6 fuentes similares	< 1%		Palabras idénticas : < 1% (79 palabras)
3	MI CASO DE ESTUDIO JOEL SANCHEZ.docx | MI CASO DE ESTUDIO JOEL SAN... #2d2dc8 El documento proviene de mi grupo 6 fuentes similares	< 1%		Palabras idénticas : < 1% (75 palabras)
4	LEMA ALTAMIRANO DAYANNA ESTHER.docx | LEMA ALTAMIRANO DAYANN... #11647a El documento proviene de mi biblioteca de referencias 5 fuentes similares	< 1%		Palabras idénticas : < 1% (63 palabras)
5	FAJARDO ROSALES BETSY JACQUELINE.docx | FAJARDO ROSALES BETSY JAC... #42cb8a El documento proviene de mi biblioteca de referencias 3 fuentes similares	< 1%		Palabras idénticas : < 1% (57 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.ug.edu.ec | Repositorio Universidad de Guayaquil: "Análisis cuantitativo ... http://repositorio.ug.edu.ec/handle/redug/64316	< 1%		Palabras idénticas : < 1% (31 palabras)
2	Tamaquiza Proyecto final para revision.docx | Tamaquiza Proyecto final pa... #abebd0 El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% (20 palabras)
3	core.ac.uk | EL ESTADO DEL ARTE SOBRE EL INTERNET DE LAS COSAS. AMENAZAS Y V... https://core.ac.uk/outputs/344723760	< 1%		Palabras idénticas : < 1% (20 palabras)
4	repositorio.uta.edu.ec | Repositorio Universidad Técnica de Ambato: Sistema domót... https://repositorio.uta.edu.ec/handle/123456789/28012?locale=en	< 1%		Palabras idénticas : < 1% (16 palabras)
5	revistacientifica.unida.edu.py | Seguridad de la información en plataformas e-learni... https://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/9	< 1%		Palabras idénticas : < 1% (16 palabras)

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://doi.org/10.1007/s11235-020-00733-2
2 https://doi.org/10.46925//rdluz.32.21
3 http://192.100.164.85/handle/20.500.12249/2757
4 https://doi.org/10.1080/17517575.2021.1896786
5 https://repository.unad.edu.co/handle/10596/28446