FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

“AMENAZAS DE CIBERSEGURIDAD EN CHAMELECON, EN EL DEPARTAMENTO DE CORTÉS, HONDURAS (2020-2024): RETOS DEL TRABAJO REMOTO Y VULNERABILIDADES EN REDES DOMÉSTICAS"

SUSTENTADO POR:

OSCAR VICENTE BENITES MEDINA

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA M.D.C., FRANCISCO MORAZAN
HONDURAS, C.A.

ENERO, 2025

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL ROGER

MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

“AMENAZAS DE CIBERSEGURIDAD EN CHAMELECON, EN EL DEPARTAMENTO DE CORTÉS, HONDURAS (2020-2024): RETOS DEL TRABAJO REMOTO Y VULNERABILIDADES EN REDES DOMÉSTICAS"

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR

JESÚS RICARDO RODRIGUEZ RIVERA

MIEMBROS DE LA TERNA:

DAVID ANTONIO DIAZ GIRÓN
JULISA JAMILETH CORTÉS OSORTO
JOSUÉ DAVID MEJÍA RIVERA

FACULTAD DE POSTGRADO

“AMENAZAS DE CIBERSEGURIDAD EN CHAMELECON, EN EL DEPARTAMENTO DE CORTÉS, HONDURAS (2020-2024): RETOS DEL TRABAJO REMOTO Y VULNERABILIDADES EN REDES DOMÉSTICAS"

Oscar Vicente Benites Medina

Resumen

Este estudio analiza las amenazas de ciberseguridad en Chamelecón, Cortés (2020-2024), con énfasis en los retos del trabajo remoto y las vulnerabilidades en redes domésticas. Se identifican riesgos como phishing, malware y accesos no autorizados, agravados por la falta de regulación y formación en ciberseguridad. A través de encuestas y análisis técnico, se proponen estrategias para fortalecer la seguridad digital en la región.

Palabras claves: (Ciberseguridad, teletrabajo, redes domésticas, amenazas digitales)

GRADUATE SCHOOL

“CYBERSECURITY THREATS IN CHAMELECON, IN THE DEPARTMENT OF CORTÉS, HONDURAS (2020-2024): CHALLENGES OF REMOTE WORK AND VULNERABILITIES IN DOMESTIC NETWORKS"

Oscar Vicente Benites Medina

Abstract

This study analyzes cybersecurity threats in Chamelecón, Cortés (2020-2024), with an emphasis on the challenges of remote work and vulnerabilities in home networks. Risks such as phishing, malware, and unauthorized access are identified, exacerbated by the lack of cybersecurity regulation and training. Through surveys and technical analysis, strategies are proposed to strengthen digital security in the region.

keywords: (Cybersecurity, teleworking, home networks, digital threa

DEDICATORIA

A **Dios**, por ser mi guía en cada paso de este camino, por darme fuerza en los momentos difíciles y por iluminar mi vida con su amor y sabiduría, mis **padres**, por su amor incondicional, su apoyo inquebrantable y por enseñarme con su ejemplo el valor del esfuerzo y la perseverancia. Gracias por ser mi mayor inspiración, mis **hermanos**, por su apoyo constante, su amor fraternal y por estar siempre presentes, brindándome su confianza y motivación en cada etapa de este viaje, a toda mi **familia**, por su compañía, sus palabras de aliento y por estar siempre a mi lado, brindándome su cariño y motivación en cada desafío, mis **amigos**, quienes con su apoyo, confianza y compañía hicieron de este proceso una experiencia más llevadera y significativa, finalmente a mis **catedráticos**, por compartir generosamente sus conocimientos y orientarme con paciencia y dedicación. Su guía constante y compromiso fueron fundamentales para que pudiera alcanzar esta meta.

AGRADECIMIENTO

Por la fortaleza que me otorgó Dios y la sabiduría que me permitió avanzar, agradezco profundamente. A mis padres, cuyo amor incondicional, respaldo económico y constante motivación fueron el pilar fundamental de mi crecimiento, les dedico mi más sincero agradecimiento. A mis familiares, por su aliento y por recordarme siempre la importancia de persistir, incluso en los momentos más complicados. A mis amigos, por su comprensión, apoyo emocional y paciencia durante cada etapa de este proceso. A mis profesores y tutores académicos, por su dedicación, retroalimentación invaluable y su compromiso con mi formación profesional. Y a mis compañeros de estudio, con quienes compartí momentos de aprendizaje y colaboración que hicieron más enriquecedora esta travesía.

INDICE DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Introducción

La pandemia de COVID-19 no solo redefinió cómo trabajamos, sino que también puso en evidencia las vulnerabilidades inherentes a nuestras infraestructuras digitales. Actualmente, aproximadamente el 47% de los empleados a nivel global desempeña sus labores de manera remota, lo que ha transformado las redes domésticas en un frente crítico en la lucha contra el cibercrimen. La falta de protección adecuada en estas redes puede tener consecuencias devastadoras, no solo para los empleados, sino también para las organizaciones que dependen de ellas. Según Gartner (2023) afirma que "Big Data está transformando cómo las empresas toman decisiones estratégicas basadas en datos en tiempo real", lo que subraya la importancia de proteger estas fuentes de información estratégica

Un caso emblemático de ataque de phishing en 2023 involucró a la empresa EPAM Systems, un contratista de servicios tecnológicos con sede en Estados Unidos. En este incidente, un empleado remoto de EPAM, ubicado en Ucrania fue víctima de un ataque de phishing. Este incidente comprometió datos confidenciales, resultando en pérdidas millonarias y la exposición de información sensible de clientes (Cybersecurity Ventures, 2024). Este y otros episodios similares resaltan la urgencia de abordar las deficiencias de seguridad en redes domésticas.

El presente estudio se centra en explorar la evolución de las amenazas cibernéticas que afectan las redes domésticas utilizadas por trabajadores remotos, analizando cómo la falta de medidas de seguridad robustas incrementa el riesgo de ciberataques. Además, se busca comprender la correlación entre la capacitación en ciberseguridad y la reducción de estas vulnerabilidades, identificando prácticas efectivas para mitigar riesgos. La investigación no solo pretende diagnosticar las debilidades existentes, sino también proponer soluciones que fortalezcan la seguridad digital en el contexto del teletrabajo.

Este enfoque es esencial en un entorno donde las amenazas digitales están en constante evolución y las redes domésticas se han convertido en una extensión crítica de la infraestructura tecnológica empresarial. La protección de estas redes no solo salvaguarda los datos personales y corporativos, sino que también garantiza la continuidad operativa en un mundo cada vez más interconectado y dependiente de las tecnologías digitales.

En el capítulo I se aborda la transformación del panorama laboral y de ciberseguridad a raíz de la pandemia de COVID-19, que impulsó el teletrabajo a nivel global. Se expone cómo esta transición ha incrementado las vulnerabilidades en las redes domésticas, convirtiéndolas en objetivos prioritarios para los ciberataques. A través de un análisis detallado, se presenta el problema central de la investigación: la insuficiencia de medidas de seguridad en redes personales de trabajadores remotos, especialmente en comunidades como Barrio Chamelecón en Honduras. Este capítulo formula preguntas de investigación que guían el estudio, Además, se establecen objetivos específicos enfocados en identificar vulnerabilidades, evaluar estrategias de mitigación y desarrollar recomendaciones prácticas para fortalecer la seguridad digital en estos entornos.

El capítulo II establece las bases conceptuales y contextuales de la investigación, integrando teorías relevantes como la Teoría de la Seguridad de la Información y el Comportamiento Humano en Ciberseguridad. Se analiza el impacto de factores macro y microeconómicos, como las regulaciones legales internacionales (por ejemplo, el GDPR) y la falta de infraestructura tecnológica en regiones como América Latina. También se destacan las tendencias tecnológicas globales, incluyendo el uso de inteligencia artificial en ciberseguridad, contrastadas con los desafíos locales, como la baja capacitación en seguridad digital en Honduras. Este marco teórico no solo contextualiza las amenazas emergentes, como vulnerabilidades en dispositivos IoT y routers, sino que también justifica la importancia de la investigación en un contexto donde las redes domésticas han pasado a ser una extensión crítica de las organizaciones.

En el capítulo III describe el diseño metodológico utilizado para explorar las amenazas de ciberseguridad en redes domésticas y su impacto en teletrabajadores del Barrio Chamelecón. Las técnicas incluyen encuestas estructuradas para recolectar datos sobre la frecuencia de ciberataques y prácticas de seguridad en hogares con ingresos inferiores a HNL 15,000. Se define la población como los hogares con conexión a Internet en el Barrio Chamelecón, se presenta una matriz de congruencia que vincula las preguntas, objetivos, variables e instrumentos de la investigación, asegurando la coherencia y rigor del estudio.

El Capítulo IV presenta el análisis exploratorio de datos y el proceso de recolección de información, incluyendo la descripción del conjunto de datos, su limpieza, visualización y las consideraciones metodológicas y éticas aplicadas.

En el capítulo V se presentan las conclusiones obtenidas a partir del análisis de las amenazas de ciberseguridad en redes domésticas y su impacto en los teletrabajadores del Barrio Chamelecón. Se discuten los principales hallazgos sobre la relación entre el nivel de conocimiento en ciberseguridad y la adopción de medidas de protección, así como los factores socioeconómicos que limitan el acceso a herramientas de seguridad. Además, se proponen recomendaciones enfocadas en mejorar la concienciación digital, promover el uso de prácticas seguras y facilitar soluciones accesibles para la protección de redes domésticas en comunidades vulnerables.

Culminando con el capítulo VI presenta la propuesta práctica desarrollada con base en los resultados de la investigación, enfocada en fortalecer la seguridad en redes domésticas en el Barrio Chamelecón. Se expone una estrategia integral que responde a las principales debilidades detectadas en ciberseguridad, especialmente ante el aumento de amenazas digitales y la limitada capacitación tecnológica en la comunidad. En esta sección se detallan los componentes clave de la propuesta, incluyendo su justificación, alcance, desarrollo, cronograma de implementación, presupuesto y mecanismos de control, con el objetivo de ofrecer una solución concreta y viable.

1.2 Antecedentes del Problema

Diversas investigaciones han demostrado que el trabajo remoto ha intensificado las ciberamenazas, especialmente en países como Honduras, donde la transición al teletrabajo fue acelerada y careció de una infraestructura sólida en ciberseguridad. Según la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2023), los ataques de phishing y ransomware dirigidos a redes domésticas y dispositivos personales aumentaron un 27% durante la pandemia de COVID-19, evidenciando un cambio en el enfoque de los atacantes, quienes ahora aprovechan las debilidades de los entornos domésticos para comprometer datos corporativos.

Esta problemática se ve exacerbada por la falta de formación en ciberseguridad entre los empleados. Muchos trabajadores utilizan dispositivos personales para acceder a información corporativa desde redes domésticas poco seguras, lo que incrementa significativamente el riesgo de ataques, un informe de (Kaspersky Lab., 2023) destaca que, mientras antes los ciberdelincuentes centraban sus esfuerzos en las redes corporativas, ahora apuntan a las redes domésticas, donde las configuraciones de seguridad son más débiles o inexistentes, representando un punto de entrada crítico para ataques avanzados.

Por otro lado, estudios como los de Conrrado E. et al, (2021), enfatizan que, aunque los protocolos de seguridad son esenciales para proteger las redes domésticas, persiste una falta de estrategias sólidas de capacitación y concienciación en ciberseguridad. Según estos autores, el 70% de los empleados en teletrabajo no recibe formación regular sobre prácticas de seguridad digital, lo que aumenta la vulnerabilidad de las empresas. Además, se ha registrado un aumento del 35% en el uso de dispositivos personales para fines laborales, un factor que incrementa las amenazas debido a la ausencia de controles de seguridad avanzados en estos dispositivos. Este fenómeno refleja la urgencia de implementar medidas integrales que incluyan tanto la mejora de la infraestructura tecnológica como la educación continua en ciberseguridad, con el fin de mitigar los riesgos asociados al teletrabajo en entornos cada vez más digitalizados.

1.3 Planteamiento del Problema

La falta de seguridad en redes domésticas constituye un desafío crítico para las empresas que han adoptado el teletrabajo, exponiéndolas a un creciente número de riesgos cibernéticos. A diferencia de las redes empresariales, que suelen contar con firewalls, sistemas de monitoreo avanzado y políticas de acceso restringido, las redes personales suelen ser menos protegidas, lo que facilita que ciberdelincuentes accedan a información sensible.

Investigaciones recientes identifican esta problemática como una de las principales amenazas de ciberseguridad en el contexto del trabajo remoto, evidenciando una brecha significativa en la implementación de estrategias eficaces para proteger las redes domésticas (Gómez R. et all, 2022). Este vacío de seguridad no solo incrementa la exposición de las empresas a ataques cibernéticos, sino que también compromete la privacidad y la integridad de los datos corporativos.

Casos como los incidentes reportados por empresas como Zoom y Twitter en 2020, en los que cuentas de empleados que trabajaban desde casa fueron vulneradas, expusieron datos sensibles y destacaron el impacto de redes domésticas no aseguradas. De manera más alarmante, el ataque de ransomware a Colonial Pipeline en 2021, que paralizó operaciones clave y generó consecuencias económicas graves, demostró cómo las vulnerabilidades de redes conectadas pueden ser explotadas para causar daños de gran escala.

Estos eventos subrayan la urgente necesidad de que las empresas desarrollen e implementen estrategias de ciberseguridad robustas que incluyan la capacitación de empleados, la

configuración segura de redes domésticas y el uso de herramientas avanzadas como VPNs y autenticación multifactor. Solo a través de estas medidas se podrá mitigar el creciente riesgo asociado con el trabajo remoto y proteger tanto los datos corporativos como la continuidad operativa.

1.4 Preguntas de Investigación

1.4.1 Pregunta General

¿Cómo ha evolucionado el panorama de ciberseguridad con la adopción masiva del trabajo remoto post-COVID en el Barrio Chamelecón, y qué nuevas vulnerabilidades han surgido en las redes domésticas utilizadas por teletrabajadores?

1.4.2 Preguntas Específicas

- ¿Cuáles son las principales vulnerabilidades en redes domésticas y dispositivos utilizados por teletrabajadores en el Barrio Chamelecón, especialmente en routers y dispositivos IoT?
- ¿Cómo ha impactado la migración masiva al trabajo remoto en las estrategias de ciberseguridad adoptadas por los hogares de Chamelecón y las organizaciones locales?
- ¿Qué medidas específicas de prevención y mitigación pueden implementarse para fortalecer la seguridad de las redes domésticas en Chamelecón, considerando las condiciones socioeconómicas de la comunidad?

1.5 Objetivos

1.5.1 Objetivo General

Analizar las amenazas de ciberseguridad emergentes en redes domésticas utilizadas para teletrabajo en el Barrio Chamelecón, evaluando las vulnerabilidades, estrategias de mitigación y posibles soluciones adaptadas al contexto local.

1.5.2 Objetivos Específicos

1. Identificar las principales vulnerabilidades en redes domésticas de teletrabajadores en el Barrio Chamelecón, con énfasis en configuraciones inseguras de routers y dispositivos IoT.

2. Evaluar cómo la transición al teletrabajo ha afectado la implementación de medidas de ciberseguridad en los hogares y su efectividad frente a las amenazas emergentes.
3. Proponer un conjunto de recomendaciones específicas para mejorar la seguridad en redes domésticas de Chamelecón, considerando factores como la accesibilidad económica y la viabilidad técnica de las medidas sugeridas.

1.6 Justificación

Este estudio es crucial para abordar las crecientes vulnerabilidades de ciberseguridad asociadas al teletrabajo, especialmente en comunidades con recursos limitados como el Barrio Chamelecón. La pandemia aceleró la transición al trabajo remoto, exponiendo las redes domésticas a una mayor cantidad de ciberataques. Según la Comisión Federal de Comercio (FTC 2023), los incidentes de seguridad relacionados con el trabajo remoto aumentaron en un 40% durante 2023. Además, un informe de IBM (2023) señala que el costo promedio de una violación de datos en entornos remotos alcanzó los USD 4.24 millones por incidente, representando una carga económica significativa para las organizaciones.

Las redes domésticas, especialmente aquellas en comunidades con ingresos menores a HNL 15,000 mensuales, carecen frecuentemente de medidas básicas de seguridad como firewalls o autenticación multifactor, lo que aumenta su vulnerabilidad. Aunque existe una amplia literatura sobre ciberseguridad en entornos corporativos, la protección de redes domésticas utilizadas para el teletrabajo sigue siendo un área poco explorada. Este estudio busca llenar esa brecha, ofreciendo recomendaciones prácticas basadas en datos que mejoren la seguridad en redes domésticas, protejan información sensible y fortalezcan la continuidad operativa de las organizaciones que dependen de trabajadores remotos.

La elección de realizar el estudio en la zona de Chamelecón se debe a que la mayoría de mis compañeros de trabajo residen en esa comunidad. Esta cercanía no solo facilita la recolección de datos, sino que también permite una mejor comprensión del contexto local, lo cual es fundamental para el desarrollo adecuado del proyecto.

CAPÍTULO II – MARCO TEÓRICO

Este capítulo expone los fundamentos conceptuales que permiten comprender las dinámicas de las amenazas de ciberseguridad en la era post-COVID-19. Se centra en los desafíos específicos del teletrabajo, un fenómeno que ha transformado las redes domésticas en objetivos críticos para los ciberdelincuentes. A medida que más empleados trabajan remotamente, las vulnerabilidades asociadas a estas redes han aumentado, exponiendo a las organizaciones a nuevos riesgos. Este capítulo explora los factores externos e internos que han influido en este incremento, así como las teorías clave que explican los comportamientos humanos y técnicos en el ámbito de la ciberseguridad.

Mediante el análisis del macroentorno y microentorno, se contextualiza cómo las tendencias globales y locales, junto con la evolución de las tecnologías y las políticas, han redefinido el panorama de la seguridad digital. Este marco teórico establece una base sólida para el estudio, permitiendo interpretar las relaciones entre las amenazas emergentes y las medidas adoptadas para mitigarlas, y ofreciendo una comprensión profunda de los factores que impulsan la necesidad de una ciberseguridad más robusta en el actual entorno digital.

Las empresas aplican una combinación de herramientas y políticas de ciberseguridad para proteger su infraestructura tecnológica. Entre los mecanismos más utilizados se encuentra el uso de redes privadas virtuales (VPN), que permiten conexiones seguras y cifradas, especialmente útiles para el acceso remoto de empleados. Asimismo, implementan soluciones antivirus y antimalware que protegen los dispositivos frente a software malicioso, garantizando la integridad de los sistemas operativos y archivos. Otro elemento clave es el monitoreo generalizado de la red, a través de sistemas de detección y prevención de intrusos (IDS/IPS), así como plataformas de análisis de comportamiento que identifican accesos anómalos o actividades sospechosas en tiempo real. Estos recursos son gestionados por equipos especializados y forman parte de políticas integrales de seguridad que incluyen controles de acceso, autenticación multifactor (MFA) y respaldo periódico de la información.

2.1 Macroentorno

El análisis de ciberseguridad y teletrabajo revela cómo los factores políticos, económicos, sociales, tecnológicos, legales y medioambientales varían entre regiones, influyendo en la gestión de ciberamenazas. Mientras Europa y Estados Unidos cuentan con marcos avanzados, África y

América Latina enfrentan brechas significativas en regulación e infraestructura. En términos económicos, países como Japón, Alemania y Corea del Sur lideran la inversión en ciberseguridad, a diferencia de América Central, que enfrenta limitaciones. En tecnología, Estados Unidos y China sobresalen en innovación, mientras que muchas naciones en desarrollo aún dependen de sistemas obsoletos. En el ámbito legal, la Unión Europea ha establecido regulaciones robustas, pero Asia-Pacífico y América Latina todavía enfrentan desafíos en la armonización de sus marcos regulatorios. Finalmente, en lo medioambiental, países como Irlanda y Dinamarca tienen altos consumos energéticos en sus centros de datos, mientras que regiones con acceso limitado a energías renovables enfrentan mayores dificultades.

- **Factores Políticos y Legales**

Las políticas de ciberseguridad varían significativamente según el desarrollo económico, la infraestructura y la capacidad regulatoria de cada región. En Europa, el Reglamento General de Protección de Datos (GDPR) ha sido eficaz, imponiendo sanciones superiores a EUR 2,900 millones desde 2018. En Estados Unidos, la Ley de Privacidad del Consumidor de California (CCPA) ha llevado al 75% de las empresas a adaptar sus políticas de privacidad.

En África, el 65% de los países carece de una legislación integral de ciberseguridad y solo el 20% cuenta con equipos nacionales de respuesta a incidentes (CSIRT) operativos (ENISA, 2023). En América Latina, apenas el 28% de las empresas medianas y grandes han implementado políticas robustas, en comparación con más del 85% en Europa, lo que evidencia una brecha significativa en la capacidad de respuesta ante ciberataques.

- **Factores Económicos**

La inversión en ciberseguridad está estrechamente ligada al desarrollo económico. Japón, Alemania y Corea del Sur lideran la adopción de tecnologías avanzadas, invirtiendo miles de millones de dólares en infraestructura digital segura. En contraste, América Central enfrenta desafíos económicos que limitan la implementación de medidas de seguridad, aumentando su exposición a ciberamenazas.

Según (Statista, 2023), las pérdidas económicas globales por ciberataques alcanzaron los USD 6 billones en 2022 y podrían ascender a USD 9,22 billones en 2024. Este impacto es más severo en las PYMEs, que carecen de recursos para adoptar estrategias avanzadas de

ciberseguridad. Además, el (Foro Económico Mundial, 2023) reporta que los ataques de ransomware aumentaron un 30% en comparación con el año anterior, afectando principalmente a pequeñas empresas en países en desarrollo

- **Factores Tecnológicos**

El acceso a tecnologías avanzadas varía ampliamente entre regiones. Estados Unidos y China lideran en inteligencia artificial aplicada a la ciberseguridad, mientras que muchas economías emergentes aún dependen de sistemas obsoletos.

El informe de (ISACA, 2023) señala que solo el 37% de las empresas en mercados en desarrollo ha implementado autenticación multifactor (MFA), en comparación con el 87% en mercados avanzados, lo que las deja vulnerables a ataques de phishing y malware.

- **Factores Legales**

La diversidad de marcos legales en ciberseguridad y protección de datos representa un desafío significativo para la colaboración internacional. Mientras regiones como la Unión Europea lideran con regulaciones avanzadas como el Parlamento Europeo (2016), otras áreas como Asia-Pacífico enfrentan un mosaico complejo de leyes nacionales. Países como Japón han alineado sus regulaciones con el GDPR, pero muchas naciones del sudeste asiático carecen de marcos legales robustos, lo que complica la cooperación transfronteriza y la implementación de estándares universales

En América Latina, la situación es igualmente compleja. Aunque 12 países han desarrollado estrategias nacionales de ciberseguridad, como Brasil, Argentina y México, la falta de armonización entre estas políticas dificulta la lucha efectiva contra el cibercrimen. Según un informe del Banco Interamericano de Desarrollo (2023) el 80% de los países de la región carecía de una estrategia de ciberseguridad antes de 2016, y aunque se han hecho avances, muchos marcos legales aún son insuficientes para abordar las amenazas modernas

- **Factores Medioambientales**

El impacto ambiental de la ciberseguridad es un tema creciente. Según (Deloitte, 2023), los centros de datos podrían consumir hasta 1,300 TWh de electricidad para 2030. Sin embargo, los centros de datos en la nube son hasta 3.8 veces más eficientes que los tradicionales. En Europa, países como Irlanda y Dinamarca han visto aumentar su consumo energético, representando hasta

el 15% del total de electricidad en Dinamarca para 2030. Regiones con acceso limitado a energías renovables enfrentan desafíos adicionales en la optimización de eficiencia energética.

2.2 Microentorno

El microentorno se enfoca en usuarios finales, proveedores, socios comerciales y reguladores. En Centroamérica, hay una clara diferenciación en preparación en ciberseguridad:

1. **Panamá y Costa Rica** han avanzado significativamente con estrategias robustas, regulaciones modernas y alianzas internacionales.
2. **Guatemala y El Salvador** han incrementado su digitalización en comercio electrónico y teletrabajo, pero aún carecen de infraestructura y legislación adecuadas.
3. **Honduras y Nicaragua** enfrentan los mayores desafíos en inversión, regulación y dependencia de plataformas extranjeras.

Según el (Atlantic Council, 2023), la región enfrenta **1,600 ciberataques por segundo**, reflejando su vulnerabilidad.

- **Usuarios Finales**

El teletrabajo ha convertido a los empleados en un eslabón débil en la ciberseguridad. En Centroamérica, sectores como banca y telecomunicaciones han reportado un aumento en incidentes de phishing y malware. En Honduras, el bajo nivel de formación en ciberseguridad, especialmente en comunidades de bajos recursos como el barrio Chamelecón, agrava la exposición a ataques digitales (Gómez, R. et al, 2022).

- **Proveedores y Terceros**

La dependencia de proveedores externos y servicios en la nube ha incrementado el riesgo cibernético en la región. Costa Rica y Panamá han adoptado estándares más rigurosos, mientras que Honduras y Nicaragua enfrentan dificultades para exigir altos niveles de seguridad a sus proveedores. La falta de auditorías y acuerdos de servicio con enfoque en ciberseguridad han dejado vulnerables a muchas empresas (Forrester, 2023).

- **Reguladores**

Centroamérica avanza lentamente en la adopción de marcos regulatorios internacionales. Costa Rica y Panamá han alineado sus normativas con estándares como el (National Institute of

Standards and Technology (NIST), 2020) y la norma (ISO, 2022), mientras que Guatemala, El Salvador, Honduras y Nicaragua tienen regulaciones fragmentadas y escasa aplicación. En América Latina, solo 15 países han implementado estrategias formales de ciberseguridad, evidenciando la necesidad de mayor regulación y cooperación internacional.

2.3 Teorías De Sustento

La ciberseguridad en el entorno organizacional se fundamenta en diversas teorías que proporcionan marcos conceptuales para abordar los retos actuales. Estas teorías permiten analizar cómo las organizaciones pueden fortalecer su ventaja competitiva, gestionar los riesgos asociados al teletrabajo y fomentar comportamientos seguros entre sus empleados. A continuación, se presentan tres enfoques clave: la Teoría de Recursos y Capacidades Organizacionales, la Teoría de la Seguridad de la Información en el Teletrabajo y la Teoría del Comportamiento Humano en Ciberseguridad.

- **Teoría de Recursos y Capacidades Organizacionales**

Esta teoría sostiene que la ventaja competitiva de una organización se basa en sus recursos valiosos y capacidades internas. En ciberseguridad, esto implica desarrollar sistemas avanzados de detección y respuesta ante incidentes, así como capacidades de ciberinteligencia para anticipar y mitigar amenazas. La resiliencia digital depende de la capacidad para proteger los activos críticos y reaccionar rápidamente ante posibles ataques (Barney, J. B. et al 2022).

- **Teoría de la Seguridad de la Información en el Teletrabajo**

Aborda los desafíos específicos de la ciberseguridad en el contexto del teletrabajo, como el uso de dispositivos personales, la capacitación en ciberseguridad y la implementación de políticas de protección en redes domésticas. Proporciona una estructura para comprender y reducir las vulnerabilidades propias del trabajo remoto. Se centra en la importancia de establecer políticas claras y entrenar a los empleados para proteger la información corporativa en sus entornos domésticos (Gómez, R. et al, 2022).

- **Teoría del Comportamiento Humano en Ciberseguridad**

Esta teoría aborda cómo los factores sociales y psicológicos influyen en la adherencia a políticas de seguridad. Fomentar una cultura organizacional de ciberseguridad mediante la educación continua y simulaciones de ataques puede reducir significativamente el comportamiento

negligente que suele ser explotado por los atacantes (ISACA, 2023).

- **Teoría de la Gestión de Riesgos Cibernéticos**

Esta teoría propone una aproximación estructurada para gestionar los riesgos cibernéticos, destacando la importancia de las auditorías continuas, el monitoreo en tiempo real y la integración de la ciberseguridad en todos los niveles organizacionales.

- **Teoría del Internet de las Cosas (IoT) en Ciberseguridad:**

Con la expansión del Internet de las Cosas, esta teoría examina cómo la conectividad masiva de dispositivos amplía la superficie de ataque. La gestión de ciberseguridad en entornos IoT requiere el diseño de arquitecturas seguras, autenticación robusta, monitoreo constante y control de dispositivos, tanto en redes empresariales como domésticas Weber, R. H. (2021).

- **Tipos de Ataques en Ciberseguridad:**

Comprender los distintos tipos de amenazas permite aplicar estrategias de defensa adecuadas. Entre los ataques más frecuentes se encuentran:

  - Phishing: suplantación de identidad para obtener información sensible.
  - Ransomware: cifrado de datos a cambio de un rescate.
  - Malware: software malicioso con fines destructivos o de espionaje.
  - Ataques DDoS: saturación de sistemas para interrumpir servicios.
  - Ingeniería social: manipulación psicológica para acceder a datos.

2.4 Metodologías Temáticas

Para abordar el análisis de las amenazas de ciberseguridad en la era post-COVID, especialmente en el contexto del teletrabajo y las redes domésticas, se emplearon metodologías temáticas que estructuran de manera efectiva el proceso de investigación. Estas metodologías se fundamentan en teorías clave, como la Teoría de la Seguridad de la Información en el Teletrabajo, la Teoría de la Gestión de Riesgos Cibernéticos y la Teoría del Comportamiento Humano en Ciberseguridad, que resaltan la importancia de comprender tanto las vulnerabilidades humanas como las técnicas en entornos de trabajo remoto.

2.4.1 Enfoque Cuantitativo y cualitativo

El enfoque mixto combina análisis cuantitativo y cualitativo para ofrecer una comprensión integral del problema. Este enfoque permite integrar la Teoría del Comportamiento Humano, analizando actitudes y prácticas de los empleados en ciberseguridad, mientras que los datos cuantitativos miden la incidencia de ataques y vulnerabilidades en dispositivos IoT.

- **Cuantitativo:**

Mediante encuestas aplicadas a empleados que trabajan desde casa, se recopilarán datos como la frecuencia de actualización de software en routers y la utilización de redes seguras. Según datos de (Verizon, 2023), el 82% de las brechas de seguridad involucran errores humanos, lo que subraya la relevancia de este tipo de análisis.

- **Cualitativo:**

Las entrevistas a expertos en TI aportarán información detallada sobre la percepción de los riesgos relacionados con redes domésticas. Por ejemplo, un informe de (FortiGuard Lab., 2024) destacó que el 67% de los expertos en seguridad considera que las redes domésticas son más vulnerables que las corporativas.

2.4.2 Método Inductivo

El método inductivo es adecuado para explorar incidentes recientes de ciberseguridad y desarrollar hipótesis sobre vulnerabilidades emergentes en redes domésticas. Este enfoque complementa la Teoría de la Seguridad de la Información al generar nuevas ideas sobre cómo el teletrabajo amplía la superficie de ataque.

- **Análisis de incidentes:**

Al estudiar casos de phishing en redes domésticas, se pueden identificar patrones comunes, como el uso de redes Wi-Fi mal configuradas. Un estudio de ESET (2023) reveló que el 41% de los ataques de phishing se dirigen a dispositivos conectados en redes domésticas, evidenciando la importancia de este enfoque.

2.5 Herramientas

Para garantizar la validez y relevancia de los datos recolectados, se consideraron diversas herramientas de recolección de información. La elección de la encuesta como método principal

responde a su capacidad para obtener datos directos de usuarios sobre las amenazas en redes domésticas, permitiendo identificar patrones y percepciones clave.

A continuación, se presenta una comparativa de herramientas utilizadas para la recopilación de datos en estudios similares:

Tabla 1 Comparativa de herramientas

Herramienta	Tipo	Ventajas	Desventajas
Encuestas	Cuantitativa	Permite recopilar datos de un gran número de personas, es estructurada y fácil de analizar	Puede verse afectada por sesgo en las respuestas o baja tasa de respuesta
Entrevistas	Cualitativa	Proporciona información detallada y profunda sobre percepciones y experiencias	Consume más tiempo y es difícil de generalizar
Observación directa	Cualitativa	Permite analizar comportamientos en tiempo real sin intermediarios	Puede ser subjetiva y difícil de replicar en gran escala
Análisis de registros y logs	Cuantitativa	Datos objetivos y precisos sobre eventos de seguridad	Requiere acceso a sistemas y conocimientos técnicos avanzados

Fuente: Elaboración propia.

Se seleccionó la **encuesta** como principal herramienta debido a su capacidad de recopilar información cuantificable de una muestra amplia de usuarios de redes domésticas. Esto permite identificar tendencias, preocupaciones y niveles de conocimiento sobre ciberseguridad, facilitando un análisis estructurado y representativo de la problemática.

2.5.1 Encuestas Online

Las encuestas online serán realizadas mediante plataformas de Microsoft Form. Estas herramientas son ideales para recopilar datos cuantitativos sobre prácticas de seguridad y experiencias de ciberataques en redes domésticas. La información recolectada permitirá analizar tendencias y validar hipótesis sobre las brechas de ciberseguridad en el teletrabajo.

2.5.2 Análisis de Vulnerabilidades

En este análisis se emplearán herramientas clave como Nmap, Wireshark y Metasploit para identificar vulnerabilidades específicas en dispositivos IoT y routers domésticos. Estas herramientas permiten realizar pruebas exhaustivas para detectar configuraciones inseguras y simular ataques, contribuyendo a la identificación y mitigación de riesgos.

- **Nmap**: Utilizado para escanear redes personales, Nmap detecta configuraciones inseguras y dispositivos expuestos, identificando puertos abiertos que podrían ser explotados por atacantes. Según (Lyon, 2009), Nmap es eficaz para detectar servicios en ejecución y anomalías en dispositivos conectados a redes locales.
- **Wireshark**: Esta herramienta analiza el tráfico de red en tiempo real para detectar posibles amenazas como ataques de phishing o malware. Wireshark es ampliamente reconocido en el ámbito de la ciberseguridad por su capacidad para identificar patrones de tráfico sospechoso (Combs, G., 2022)
- **Metasploit**: Permite evaluar la viabilidad de las vulnerabilidades detectadas mediante la simulación de ataques controlados, lo que ayuda a determinar la exposición real de los sistemas. Metasploit es utilizado por profesionales de seguridad para probar vulnerabilidades y fortalecer las defensas cibernéticas (Oostendorp, S., 2021)

2.5.3 Análisis de Estadístico

Para garantizar la validez y relevancia de los datos recolectados, se evaluaron diversas herramientas enfocadas en el análisis técnico y estadístico de amenazas en redes domésticas. A continuación, se presenta una comparativa entre las principales opciones consideradas:

Tabla 2 Comparación de herramientas

Herramienta	Tipo	Funcionalidades clave	Ventajas	Desventajas
Wireshark	Análisis de tráfico	Captura y análisis de paquetes en tiempo real	Gratuita, potente y con amplia comunidad de soporte	Puede ser compleja para usuarios sin experiencia
Metasploit	Pruebas de penetración	Simulación de ataques y explotación de vulnerabilidades	Extensa base de exploits y automatización	Requiere conocimientos avanzados en seguridad

Herramienta	Tipo	Funcionalidades clave	Ventajas	Desventajas
KNIME	Análisis de datos	Modelado, minería de datos, machine learning, automatización de análisis	Interfaz visual, integración con Python y R, adaptable a múltiples casos de uso	Curva de aprendizaje moderada
R (RStudio)	Análisis estadístico	Modelado de datos, generación de gráficos y reportes	Robusta capacidad de análisis y visualización	Requiere programación, menos intuitiva para usuarios nuevos
Python (Pandas, Scikit-learn)	Análisis de datos y ML	Procesamiento de datos, modelado predictivo y visualización	Flexibilidad, amplio ecosistema de librerías	Necesidad de escribir código, configuración inicial puede ser compleja

Fuente: Elaboración propia

Se optó por **KNIME** debido a su capacidad de integración con diversas fuentes de datos, su facilidad de uso mediante una interfaz gráfica y su potencial para automatizar el análisis de amenazas en redes domésticas. Además, permite aplicar técnicas de machine learning y análisis estadístico sin requerir una programación extensa, lo que facilita su adopción y uso dentro del estudio.

2.5.4 Viabilidad

Para garantizar la implementación efectiva de estas herramientas, se seguirá un cronograma que incluye capacitación técnica del equipo. Talleres especializados cubrirán el uso avanzado de Metasploit y Wireshark, asegurando que cualquier persona esté preparada para enfrentar la complejidad técnica de estas herramientas.

La conceptualización es una etapa clave para estructurar y delimitar el marco teórico de la investigación, ya que permite establecer definiciones y conceptos fundamentales que orientan el análisis y aseguran la coherencia entre los objetivos planteados y las estrategias metodológicas. En este caso, se desarrollan las siguientes definiciones clave:

2.6 Conceptualización

La conceptualización es una etapa clave para estructurar y delimitar el marco teórico de la investigación, ya que permite establecer definiciones y conceptos fundamentales que orientan el

análisis y aseguran la coherencia entre los objetivos planteados y las estrategias metodológicas. En este caso, se desarrollan las siguientes definiciones clave:

2.6.1 Ciberseguridad

Es el conjunto de prácticas, medidas y tecnologías diseñadas para proteger los sistemas, redes y datos contra accesos no autorizados, ataques y daños. La ciberseguridad abarca tanto los aspectos técnicos (hardware y software) como los humanos, enfatizando la importancia de la concienciación y educación del usuario. Este concepto resulta esencial en entornos de teletrabajo, donde las redes domésticas son frecuentemente el punto de entrada de ataques cibernéticos (ENISA, 2023).

2.6.2 Redes Domésticas

Infraestructura tecnológica que conecta dispositivos dentro de un hogar, como computadoras, teléfonos, televisores inteligentes y otros dispositivos IoT. Las redes domésticas son altamente vulnerables debido a la falta de medidas de seguridad robustas en comparación con redes corporativas, lo que las convierte en un blanco atractivo para ciberataques (Cisco, 2021).

2.6.3 Teletrabajo

Modalidad laboral en la que los empleados realizan sus actividades fuera de las instalaciones de la empresa, utilizando herramientas digitales y tecnologías de la información. Este modelo de trabajo depende fuertemente de la conexión a internet y redes seguras para garantizar la productividad y la confidencialidad de la información (Organización Internacional del Trabajo, 2020).

2.6.4 Internet de las Cosas (IoT)

Red de dispositivos interconectados que recopilan, comparten y procesan datos a través de internet. Los dispositivos IoT en redes domésticas, como cámaras de seguridad, y asistentes virtuales, pueden aumentar la exposición a ciberataques si no se configuran (IEEE, 2022).

2.6.5 Amenazas Cibernéticas

Riesgos asociados con actividades maliciosas que buscan comprometer la seguridad de sistemas informáticos, datos. Estas incluyen malware, phishing y ransomware, los cuales han aumentado en frecuencia con la adopción masiva del teletrabajo Kaspersky Lab. (2023)

2.6.6 Confidencialidad, Integridad y Disponibilidad

Un informe de ISO (2022) Nos indica que los principios fundamentales de la seguridad de la información son:

- **Confidencialidad:** Garantizar que la información sea accesible solo para personas autorizadas.
- **Integridad:** Asegurar que la información sea precisa y no haya sido alterada de manera no autorizada.
- **Disponibilidad:** Garantizar que los sistemas y datos estén accesibles cuando sean necesarios.

2.7 Marco Legal Internacional y Nacional

El marco legal es un componente fundamental para garantizar la seguridad en entornos de teletrabajo y redes domésticas, estableciendo directrices claras para la protección de datos personales, la prevención de ciberataques y la gestión de la información. A medida que el teletrabajo se ha convertido en una práctica común, las normativas nacionales e internacionales han evolucionado para responder a los nuevos desafíos de la era digital. En este apartado se analizan las principales regulaciones aplicables en Honduras y los estándares internacionales más relevantes.

2.7.1 Marco Legal Nacional

En Honduras, el desarrollo de leyes y regulaciones relacionadas con la ciberseguridad ha ido avanzando para responder a los desafíos de la era digital, incluyendo la protección de datos personales y la seguridad informática en el entorno laboral y personal.

- **Ley de Comercio Electrónico (Decreto No. 149-2014)**

Establece principios para regular las transacciones electrónicas y reforzar la confianza digital. Aunque su enfoque principal son las operaciones comerciales, también aborda aspectos relacionados con la seguridad de la información y la protección contra delitos cibernéticos en entornos virtuales (Diario Oficial La Gaceta, 2014)

- **Código Penal de Honduras (Decreto No. 130-2017)**

Tipifica los delitos informáticos, incluyendo el acceso no autorizado a sistemas, la modificación de datos sin consentimiento y el uso indebido de información personal. Este marco legal establece penas específicas para quienes cometan ciberataques o utilicen tecnología para actividades delictivas, reforzando la protección de las redes domésticas y empresariales (Diario Oficial La Gaceta, 2017).

- **Normas de la CNBS para el Sector Financiero**

La Comisión Nacional de Bancos y Seguros (CNBS) ha emitido regulaciones específicas para garantizar la seguridad en la administración de la información en el sector financiero, enfocándose en la protección de datos y la mitigación de riesgos cibernéticos. Establecen requisitos para la gestión segura de la información en instituciones financieras, incluyendo controles de acceso, auditorías periódicas y la adopción de estándares internacionales. Estas normas aseguran que las cooperativas implementen políticas robustas de gestión de riesgos tecnológicos, esenciales para proteger los datos financieros de sus socios (CNBS, 2021)

- **Conatel**

La Comisión Nacional de Telecomunicaciones (CONATEL) regula y supervisa las telecomunicaciones en Honduras, incluyendo la ciberseguridad. CONATEL ha impulsado la adopción de estándares internacionales y ha promovido iniciativas para fortalecer la seguridad en redes públicas y privadas, asegurando la protección de la información personal y corporativa (CONATEL, 2023)

- **Iniciativa de Ley de Ciberseguridad en Honduras**

Propuesta en el Congreso Nacional, esta iniciativa busca crear un marco normativo integral para la ciberseguridad en Honduras. La ley propone lineamientos para proteger infraestructuras críticas, gestionar incidentes cibernéticos y promover la educación en ciberseguridad. Aunque aún está en proceso de evaluación ya que solamente se han aprobado 29 de sus 96 artículos, representa un paso importante hacia una política nacional más sólida (Criterio HN, 2019)

- **CSIRT UNAH**

El CSIRT de la Universidad Nacional Autónoma de Honduras (UNAH) desempeña un papel crucial en la protección de la infraestructura tecnológica de la institución y en la gestión de incidentes de ciberseguridad. La UNAH ha organizado diversos eventos, como el Congreso de Ciberseguridad 2024, donde se han discutido las últimas tendencias y retos en ciberseguridad. Estos esfuerzos subrayan la importancia de la capacitación en ciberseguridad y la adopción de buenas prácticas para mitigar riesgos tanto en entornos académicos como profesionales.

El CSIRT UNAH también ha trabajado activamente en la atención y resolución de incidentes cibernéticos, destacando la necesidad de colaboración y formación continua para responder eficazmente a las amenazas emergentes. Estos esfuerzos muestran un compromiso creciente con la ciberseguridad en Honduras, impulsando la creación de un entorno más seguro en el ámbito digital (UNAH, 2022).

2.7.2 Marco Legal Internacional

El marco legal internacional en ciberseguridad ha evolucionado significativamente en las últimas décadas, impulsado por el aumento de las amenazas digitales, la globalización de las redes informáticas y la necesidad de proteger los datos personales y empresariales. Honduras, aunque no es signataria de todos los acuerdos globales, se ve influenciada por estas normativas al alinearse con estándares internacionales que buscan reforzar la seguridad cibernética. A continuación, se presentan las principales normativas y estándares globales que afectan directa o indirectamente las políticas de ciberseguridad en Honduras.

- **Reglamento General de Protección de Datos (GDPR) – Unión Europea**

El GDPR, adoptado en 2016 y en vigor desde 2018, establece un estándar mundial para la protección de datos personales, y su influencia se extiende mucho más allá de la Unión Europea. Empresas en Honduras que interactúan con ciudadanos o empresas europeas deben cumplir con los requisitos del GDPR para evitar multas que pueden alcanzar hasta el 4% de su facturación anual global. Según la Agencia Europea de Protección de Datos, en 2022 se registraron más de **95,000 incidentes relacionados con la protección de datos**, lo que evidencia la importancia del cumplimiento normativo.

El GDPR establece principios clave, como la minimización de datos, el consentimiento explícito y la notificación obligatoria de violaciones de datos en un plazo de 72 horas. Estos principios han llevado a muchas organizaciones en América Latina a adoptar mejores prácticas en la gestión de datos personales (Parlamento Europeo, 2016)

- **Convenio de Budapest Sobre la Ciberdelincuencia**

El Convenio de Budapest es el primer tratado internacional sobre ciberdelincuencia, firmado por más de 65 países, aunque Honduras no es signataria. Este convenio busca armonizar las legislaciones nacionales sobre delitos informáticos y fomentar la cooperación internacional para combatir ciberataques.

A nivel mundial, según el Centro de Estudios Estratégicos e Internacionales (CSIS, 2022), los delitos cibernéticos generan pérdidas anuales de aproximadamente **USD 600 mil millones**. El Convenio de Budapest es crucial para enfrentar esta problemática, y aunque Honduras no es parte oficial, el país ha adoptado principios inspirados en este tratado para fortalecer su marco jurídico contra la ciberdelincuencia (Consejo de Europa, 2001)

- **Norma ISO/IEC 27001 – Seguridad de la Información**

La ISO/IEC 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). Es adoptada por organizaciones en todo el mundo para proteger la confidencialidad, integridad y disponibilidad de la información.

Según la (ISO/IEC 27001:2022, 2022), más de **58,000 organizaciones** en todo el mundo han sido certificadas bajo ISO/IEC 27001, evidenciando su importancia global. En Honduras, varias empresas del sector financiero y telecomunicaciones han comenzado a implementar este estándar para proteger la información crítica, especialmente en entornos de teletrabajo.

- **California Consumer Privacy Act (CCPA) – Estados Unidos**

El CCPA, vigente desde 2020, es una de las leyes de privacidad más estrictas en Estados Unidos y regula cómo las empresas manejan la información personal de los residentes de California. Aunque es una normativa estadounidense, afecta a cualquier empresa que maneje datos de ciudadanos californianos, incluidas algunas con sede en Honduras.

Según datos de (Consejo de Protección de Datos de California., 2022), más del 75% de las empresas internacionales que comercian con EE. UU. han adaptado sus políticas de privacidad para cumplir con la CCPA. Esto demuestra la influencia de esta legislación más allá de las fronteras estadounidenses.

- **COBIT E ITIL**

COBIT (Control Objectives for Information and Related Technologies) y ITIL (Information Technology Infrastructure Library) son marcos de trabajo que ofrecen mejores prácticas para la gestión de la tecnología de la información y la gobernanza de TI.

COBIT se centra en la gobernanza de TI, ayudando a las organizaciones a equilibrar los riesgos y beneficios asociados con la tecnología.

ITIL proporciona directrices para la gestión de servicios de TI, garantizando que los servicios de TI se alineen con las necesidades del negocio y cumplan con los requisitos de ciberseguridad.

Según un informe de (ISACA, 2023), más del **85% de las organizaciones globales** que adoptan COBIT reportan una mejora significativa en la gestión de riesgos de ciberseguridad. Honduras no es ajena a estos marcos, ya que muchas empresas los utilizan para fortalecer sus controles internos.

CAPÍTULO III – METODOLOGÍA DE LA INVESTIGACIÓN

Este capítulo describe el enfoque metodológico utilizado para analizar las amenazas de ciberseguridad en redes domésticas de teletrabajadores en el Barrio Chamelecón, Honduras. En un contexto donde el trabajo remoto ha incrementado los riesgos cibernéticos, como ataques de phishing, ransomware y vulnerabilidades en dispositivos IoT, la investigación se centra en identificar las principales debilidades en estas redes, evaluar el impacto de la capacitación en ciberseguridad sobre la reducción de incidentes, y desarrollar medidas efectivas para mitigar estas amenazas. La metodología considera las condiciones específicas de la comunidad, caracterizada por limitaciones tecnológicas y económicas, que aumentan la exposición a los ciberataques.

Esta investigación utiliza un enfoque que permite entender mejor la realidad local, poniendo especial atención en la protección de datos sensibles en sectores clave. Los resultados están pensados para ofrecer soluciones prácticas que no solo ayuden a esta comunidad, sino que también puedan aplicarse en otras regiones con características parecidas, ayudando así a reducir las brechas de ciberseguridad en contextos vulnerables.

3.1 Enfoque

En este estudio se empleará un enfoque mixto para obtener una comprensión integral de las amenazas de ciberseguridad en el teletrabajo y las redes domésticas. Según Hernández Sampieri & Fernandez-Collado (2014), este enfoque permite superar las limitaciones de los métodos puramente cuantitativos o cualitativos, integrando los beneficios de ambos para lograr una visión más completa y profunda de la investigación.

El enfoque cuantitativo se centrará en la recolección de datos estadísticos mediante encuestas aplicadas a hogares con conexión a Internet en el Barrio Chamelecón. Esto permitirá medir variables como:

- Frecuencia de actualizaciones de software.
- Uso de redes privadas virtuales (VPN).
- Implementación de autenticación multifactor y otras medidas de seguridad.

El enfoque cualitativo, por su parte, se llevará a cabo a través de entrevistas semiestructuradas con expertos en ciberseguridad, con el objetivo de explorar percepciones y

experiencias relacionadas con vulnerabilidades emergentes y estrategias de mitigación. Esto permitirá identificar no solo las amenazas actuales, sino también tendencias y posibles soluciones en el contexto del teletrabajo en comunidades con recursos limitados.

Este enfoque es el más adecuado para la investigación por varias razones:

- **Triangulación de datos:** La integración de datos numéricos y análisis interpretativos mejora la validez y confiabilidad de los resultados, permitiendo contrastar y corroborar hallazgos desde múltiples perspectivas.
- **Profundidad y amplitud:** Mientras que el análisis cuantitativo proporciona datos sobre la magnitud y frecuencia de los fenómenos estudiados, el análisis cualitativo permite comprender las causas subyacentes y los contextos específicos que influyen en dichos fenómenos.
- **Relevancia para la ciberseguridad:** La complejidad de las amenazas cibernéticas requiere un enfoque integral que permita identificar tanto los patrones generales como los factores específicos que aumentan la vulnerabilidad en redes domésticas.

3.2 Alcance

Este estudio adopta un alcance descriptivo, alineado con la metodología propuesta por (Hernández Sampieri & Fernandez-Collado, 2014), que permite comprender de manera integral las amenazas de ciberseguridad en redes domésticas utilizadas en el teletrabajo, particularmente en el Barrio Chamelecón, Honduras. Esta combinación es ideal porque no solo permite describir las prácticas de seguridad actuales, sino también analizar las causas que influyen en la aparición de vulnerabilidades específicas en hogares con recursos limitados.

El alcance descriptivo se centra en documentar las prácticas de ciberseguridad adoptadas por los hogares. Esto incluye el análisis de variables como la frecuencia de actualizaciones de software, el uso de redes privadas virtuales (VPN) y autenticación multifactor. Estos datos permiten identificar el estado actual de las medidas de protección empleadas por los trabajadores remotos. Por otro lado, el alcance explicativo tiene como objetivo determinar cómo medidas específicas de ciberseguridad contribuyen a reducir las vulnerabilidades en redes domésticas. Se analizarán factores como la implementación de software actualizado, el uso de autenticación

multifactor y políticas de seguridad en los hogares para evaluar su efectividad en la disminución de incidentes cibernéticos.

3.3 Diseño

El diseño de esta investigación es **integral**, lo que permite analizar las amenazas de ciberseguridad en redes domésticas utilizadas por trabajadores remotos en el Barrio Chamelecón, Honduras. Al ser integral, se busca abordar de manera holística las diversas dimensiones de las amenazas y las prácticas de seguridad, considerando tanto los aspectos técnicos como los humanos dentro de un solo momento, lo que facilita la identificación del estado actual de las vulnerabilidades sin necesidad de un seguimiento a largo plazo.

Este diseño es el más adecuado porque permite una evaluación exhaustiva de las amenazas de ciberseguridad en un contexto de recursos limitados. La combinación de datos cuantitativos obtenidos a través de encuestas y cualitativos mediante entrevistas permite no solo medir la magnitud de las vulnerabilidades, sino también entender sus causas y posibles soluciones. Además, el diseño integral facilita una recolección eficiente de datos en un solo periodo, optimizando tiempo y recursos.

3.3.1 Población

En esta investigación se considerará exclusivamente las viviendas del Barrio Chamelecón cuya población total, según datos de IIES-UNAH (2022) asciende a 688 viviendas**,** sin embargo, dado que no todas cuentan con conexión a Internet o redes domésticas, la población objetivo se restringe exclusivamente a aquellas viviendas que disponen de acceso a internet. Este enfoque permite centrar el análisis en el grupo relevante para el estudio, considerando las particularidades de la conectividad en la zona.

Para calcular el tamaño de la muestra, se aplicará la fórmula correspondiente a población finita. Este método se justifica por la existencia de datos precisos sobre la cantidad total de viviendas, lo que asegura la representatividad de los resultados dentro del marco definido. A partir de esta metodología, se busca obtener información válida y confiable sobre las características de las viviendas conectadas en el barrio Chamelecón.

Tabla 3 Número de Viviendas del Barrio Chamelecón

Barrio	Total Viviendas Particulares	Viviendas ocupadas	Personas
Barrio Chamelecón	787	688	2830

Fuente: Perfil Sociodemográfico San Pedro Sula, Cortés, IIES-UNAH (2022).

Figura 1 Mapa de Chamelecón.

Fuente: Google Maps (2024)

Esta población es especialmente relevante para comprender las dinámicas de ciberseguridad en hogares con recursos limitados, donde la falta de medidas de protección robustas puede aumentar la vulnerabilidad a ciberataques.

3.3.2 Muestra

Para esta investigación, la población objetivo está constituida por 688 viviendas ocupadas en el Barrio Chamelecón, Cortés, Honduras. Estas viviendas representan el contexto donde se evaluará la seguridad en redes domésticas utilizadas para teletrabajo. La selección de la muestra se centra exclusivamente en viviendas con conexión a Internet activa, permitiendo un análisis más relevante y enfocado en las prácticas y vulnerabilidades de ciberseguridad, como la frecuencia de ciberataques, el uso de herramientas como VPN, actualizaciones de software y autenticación multifactor. Este enfoque garantiza que los resultados obtenidos sean aplicables a los hogares con

mayor exposición a riesgos cibernéticos.

- **Cálculo del tamaño de la muestra para una población finita**

Se aplicó la fórmula para determinar el tamaño de la muestra en una población finita, utilizando los siguientes parámetros:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{e^2 \cdot (N-1) + Z^2 \cdot p \cdot q}$$

Parámetros:

N= 688

Z= 1.96 (95% de nivel de confianza)

p= 0.5

q= 0.5 (1-p)

e= 5% (margen de error)

$$n = \frac{688 \cdot 1.96^2 \cdot 05 \cdot 05}{0.05^2 \cdot (688-1) + 1.96^2 \cdot 0.5 \cdot 0.5}$$

n= 246.75

El cálculo arroja un tamaño de muestra de 247 viviendas, redondeando al entero superior para asegurar una representatividad estadística. Este tamaño de muestra garantizará resultados confiables con un nivel de confianza del 95% y un margen de error del 5%.

La inclusión de estas 247 viviendas permite identificar patrones y tendencias en las prácticas de ciberseguridad del Barrio Chamelecón, con un enfoque en hogares de bajos ingresos, maximizando la relevancia y aplicabilidad de los hallazgos en contextos vulnerables.

3.3.3 Técnicas de muestreo

Para esta investigación se empleará un muestreo aleatorio simple, conociendo la población total de 688 hogares en el Barrio Chamelecón que cuentan con una conexión a Internet activa. Este enfoque asegura que cada hogar dentro de la población tenga la misma probabilidad de ser seleccionado, lo que garantiza que los datos obtenidos sean representativos de la comunidad y relevantes para el análisis de las amenazas de ciberseguridad en redes domésticas. A través de esta

técnica, se optimiza la recolección de datos de una población específica y se facilita un análisis más objetivo, sin sesgos en la selección.

Este enfoque es adecuado ya que se enfoca exclusivamente en los hogares con conexión a Internet activa, que son los más relevantes para el estudio de las amenazas de ciberseguridad. El muestreo aleatorio simple asegura una muestra aleatoria y objetiva, que refleja de manera equitativa la realidad de la población del Barrio Chamelecón. Este método sigue las recomendaciones de Hernández Sampieri & Fernandez-Collado (2014) quienes destacan la importancia de utilizar técnicas de muestreo aleatorio para garantizar la representatividad y la validez de los resultados en investigaciones de este tipo.

3.4 Criterios de selección de la muestra

En el proceso de selección de la muestra para esta investigación, se han establecido criterios de inclusión y exclusión claros para garantizar que los participantes sean representativos del objetivo del estudio, centrado en las redes domésticas utilizadas para teletrabajo. Los criterios de inclusión y exclusión definen específicamente qué viviendas serán elegibles para el estudio, asegurando que los datos recolectados reflejen de manera adecuada las condiciones de seguridad en hogares con acceso a Internet, ya que estos son los que enfrentan riesgos cibernéticos asociados al teletrabajo.

3.4.1 Criterios de Inclusión y Criterios de Exclusión

Tabla 4 Criterios de Inclusión y Exclusión.

Criterio	Inclusión	Exclusión
Hogares con acceso a Internet	Se considerarán únicamente los hogares que tengan acceso a Internet activo.	Se excluirán los hogares que no tengan acceso a Internet.
Uso de Dispositivos Personales	Se incluirán los hogares que utilicen dispositivos personales para teletrabajo (laptop, Tablet. Celulares).	Se excluirán los hogares que no utilicen dispositivos personales para actividades laborales (laptop, Tablet. Celulares).
Nivel de Ingresos	Se incluirán los hogares con ingresos mensuales inferiores a HNL 15,000 mensuales.	Se excluirán los hogares con ingresos superiores a HNL 15,001 mensuales.

Fuente: Elaboración propia

3.5 Hipótesis

Las hipótesis de esta investigación analizan cómo medidas de ciberseguridad, como la capacitación, el uso de VPN y la autenticación multifactor, reducen los ciberataques en redes domésticas de teletrabajadores en el Barrio Chamelecón. También abordan factores socioeconómicos como moderadores para evaluar la efectividad de estas estrategias y proponer soluciones prácticas en contextos vulnerables.

Tabla 5 Hipótesis Nula y Alternativas

Hipótesis Nulas	Hipótesis Alternativas
Las medidas de ciberseguridad no reducen significativamente los ciberataques.	Las medidas de ciberseguridad sí reducen significativamente los ciberataques.
La capacitación no disminuye la frecuencia de incidentes de phishing.	La capacitación sí disminuye la frecuencia de incidentes de phishing.
El uso de VPN no reduce la probabilidad de infección por ransomware.	El uso de VPN sí reduce la probabilidad de infección por ransomware.
La autenticación multifactor no reduce los accesos no autorizados.	La autenticación multifactor sí reduce los accesos no autorizados.

Fuente: Elaboración propia

3.6 Operacionalización de Variables

En esta investigación, se procederá a la operacionalización de variables clave que son fundamentales para comprender cómo las prácticas de ciberseguridad afectan las redes domésticas utilizadas para el teletrabajo, particularmente en hogares de bajos ingresos en el Barrio Chamelecón. La operacionalización implica desglosar conceptos abstractos en indicadores claros y medibles, facilitando la recolección de datos y el análisis posterior.

Las principales variables seleccionadas incluyen: nivel de conocimiento en ciberseguridad, frecuencia de uso de dispositivos, percepción del riesgo cibernético y medidas de seguridad implementadas. Estas variables son esenciales para evaluar tanto los hábitos de los teletrabajadores como su capacidad para implementar y mantener prácticas de ciberseguridad efectivas.

La variable **nivel de conocimiento en ciberseguridad** se medirá a través de indicadores específicos relacionados con los hábitos de seguridad digital, tales como:

- Frecuencia con la que los participantes actualizan el software y los sistemas operativos en sus dispositivos.
- Conocimiento sobre la creación y gestión de contraseñas seguras.
- Habilidad para identificar correos electrónicos de phishing o sitios web fraudulentos.

Estos indicadores reflejan cómo los teletrabajadores gestionan la seguridad en sus dispositivos y su capacidad para protegerse frente a amenazas cibernéticas.

La variable **frecuencia de uso de dispositivos** se operacionalizará mediante preguntas sobre:

- El número promedio de horas diarias dedicadas al uso de dispositivos conectados a Internet.
- El tipo de dispositivos utilizados (por ejemplo, computadoras portátiles, teléfonos inteligentes, tabletas).
- La frecuencia con la que los teletrabajadores acceden a servicios en línea, como plataformas de videoconferencia y correo electrónico.

Estos indicadores permitirán evaluar el grado de exposición de los participantes a amenazas cibernéticas, ya que el uso intensivo de dispositivos aumenta la posibilidad de ser blanco de ataques.

La percepción del riesgo se evaluará a través de la percepción personal de los participantes acerca de su vulnerabilidad a ciberataques. Los indicadores incluirán:

- La percepción sobre la probabilidad de ser víctima de un ciberataque.
- El nivel de preocupación por la seguridad de los datos personales y profesionales.
- La confianza en las medidas de seguridad implementadas en sus redes domésticas.

Esta escala permitirá capturar la dimensión subjetiva de cómo los teletrabajadores perciben los riesgos cibernéticos y su disposición a adoptar medidas preventivas.

La variable **medidas de seguridad implementadas** se operacionalizará a través de preguntas sobre las herramientas y prácticas de seguridad utilizadas por los teletrabajadores en sus redes domésticas. Los indicadores incluirán:

- Uso de software antivirus y firewalls para proteger los dispositivos.
- Implementación de redes privadas virtuales (VPN) para cifrar las conexiones a Internet.
- Aplicación de autenticación multifactor en cuentas sensibles o profesionales.

Estos indicadores permitirán evaluar el nivel de protección técnica que los participantes han adoptado para mitigar los riesgos cibernéticos y proteger sus datos personales y laborales.

Tabla 6 Operacionalización

Variable	Tipo	Definición Conceptual	Definición Operativa	Indicadores	Instrumento	Escala
Ciberataques	Independiente	Eventos de seguridad que comprometen datos y dispositivos personales (phishing, ransomware, malware).	Número de incidentes registrados en el último año.	Frecuencia de phishing; Detección de malware; Intentos de acceso no autorizado.	Encuesta estructurada	Ordinal
Capacitación en ciberseguridad	Independiente	Habilidades adquiridas para protegerse de amenazas digitales.	Participación en cursos, talleres o actividades de autoaprendizaje en el último año.	Modalidad de capacitación; Horas invertidas; Contenidos abordados.	Encuesta estructurada	Nominal y ordinal
Medidas de seguridad implementadas	Independiente	Acciones técnicas aplicadas para prevenir ataques cibernéticos.	Uso de herramientas y configuraciones de seguridad en dispositivos del hogar.	Uso de antivirus; Firewalls activados; VPN en uso; Contraseñas seguras; Autenticación multifactor activa.	Encuesta estructurada	Nominal
Ingresos del hogar	Independiente	Cantidad total percibida mensualmente por los miembros del hogar.	Declaración de ingresos familiares mensuales.	(menos de 10,000, 10,001-15,000, L15,001-20,000 y más de 25,000) Moneda: HNL	Encuesta estructurada	Intervalo

Fuente: Elaboración propia.

3.7 Técnicas, Instrumentos y Procedimientos aplicados

En esta investigación se empleará un enfoque mixto, la principal técnica será una encuesta estructurada administrada en línea a una muestra de hogares del Barrio Chamelecón que realizan teletrabajo. La encuesta, que incluirá preguntas cerradas y abiertas, abordará aspectos como la frecuencia de ciberataques, las prácticas de seguridad, el nivel de capacitación en ciberseguridad y las características sociodemográficas de los participantes. Además, se realizará un análisis de contenido de los sitios web más visitados por los participantes para identificar posibles fuentes de amenazas. Para garantizar la validez y fiabilidad de los datos, se llevará a cabo una prueba piloto de la encuesta con un grupo reducido de hogares y se capacitará a los encuestadores en la correcta aplicación del instrumento. Los datos obtenidos serán analizados utilizando software estadístico y técnicas cualitativas, como el análisis temático, lo que permitirá obtener resultados completos y aplicables al contexto del Barrio Chamelecón.

3.7.1 Técnicas

En esta investigación se emplearán técnicas cuantitativas y cualitativas para garantizar un análisis integral de las amenazas de ciberseguridad en redes domésticas utilizadas para teletrabajo en el Barrio Chamelecón.

- **Encuestas estructuradas:** Se administrará una encuesta en línea a los hogares con conexión a Internet en el Barrio Chamelecón que realizan teletrabajo. La encuesta constará de 15 preguntas cerradas, diseñadas para evaluar aspectos clave como la frecuencia de ciberataques, el nivel de conocimiento en ciberseguridad, el uso de medidas de protección digital y las características sociodemográficas de los participantes. Las preguntas abiertas permitirán obtener información adicional sobre las experiencias y percepciones de los encuestados en relación con los riesgos cibernéticos, lo que enriquecerá los datos cuantitativos obtenidos de las preguntas cerradas.
- **Entrevistas semiestructuradas:** Se realizarán 10 entrevistas semiestructuradas a expertos en ciberseguridad para identificar las vulnerabilidades más comunes en redes domésticas y explorar estrategias efectivas de mitigación. Estas entrevistas seguirán una guía estructurada con preguntas abiertas, abordando temas como tendencias actuales en ciberseguridad, las amenazas más frecuentes para los hogares y recomendaciones.

La combinación de estas técnicas permitirá complementar los datos estadísticos obtenidos de las encuestas con la profundidad analítica de las entrevistas, logrando una comprensión holística del problema y proponiendo soluciones fundamentadas tanto en datos cuantitativos como en la experiencia cualitativa de los especialistas.

3.7.2 Instrumentos Elaborados

Se han diseñado instrumentos específicos para la recolección de datos en esta investigación, asegurando que permitan capturar información relevante sobre las amenazas de ciberseguridad en redes domésticas utilizadas para teletrabajo en el Barrio Chamelecón:

- **Cuestionarios digitales:** Se utilizarán cuestionarios autoadministrados a través de la plataforma Google Forms para recopilar datos detallados sobre las prácticas de seguridad digital de los hogares participantes. Estos cuestionarios incluirán tanto preguntas cerradas como abiertas, organizadas en bloques temáticos que abordarán aspectos como la frecuencia de ciberataques, el uso de dispositivos conectados, las medidas de seguridad implementadas y las características sociodemográficas de los encuestados. Los cuestionarios han sido diseñados para garantizar la claridad y accesibilidad de las preguntas, empleando protocolos que aseguren la privacidad y confidencialidad de la información proporcionada por los participantes.
- **Guías de entrevista:** Se han preparado guías específicas para llevar a cabo entrevistas a profundidad a 15 expertos en ciberseguridad, centradas en temas como las tendencias actuales en ciberamenazas, las vulnerabilidades más frecuentes en redes domésticas y estrategias efectivas para proteger datos y dispositivos personales. Estas entrevistas explorarán además las recomendaciones de capacitación para usuarios finales y las mejores prácticas de mitigación. Las entrevistas serán grabadas con el consentimiento informado de los participantes y se transcribirán para realizar un análisis detallado.

3.7.3 Procedimientos

Para la recolección de datos en esta investigación, se implementarán los siguientes procedimientos cuidadosamente estructurados, con el objetivo de garantizar la validez, relevancia y exhaustividad de la información obtenida:

- **Diseño y validación de instrumentos:** Los cuestionarios digitales y las guías de entrevista serán sometidos a un riguroso proceso de validación por un panel multidisciplinario de

expertos en ciberseguridad y metodologías de investigación. Este proceso incluirá un análisis de contenido para evaluar la claridad, pertinencia y cobertura de los ítems incluidos. Cualquier observación o recomendación derivada de esta revisión será incorporada en las versiones finales de los instrumentos, garantizando que estos cumplan con los estándares metodológicos del estudio y sean apropiados para el contexto de investigación.

- **Aplicación de encuestas:** Las encuestas se administrarán en línea a una muestra aleatoria de 247 hogares dentro del Barrio Chamelecón. Los participantes recibirán un enlace a la encuesta a través de correo electrónico, lo que garantizará un proceso eficiente y accesible. Para aumentar la tasa de respuesta, se enviarán recordatorios por correo electrónico a los participantes que no hayan completado la encuesta dentro del plazo establecido. Además, se ofrecerán incentivos a aquellos que completen la encuesta, con el fin de motivar su participación.
- **Realización de entrevistas:** Las entrevistas semiestructuradas se llevarán a cabo virtualmente mediante la plataforma Google Form. Cada entrevista tendrá una duración estimada de entre 20 a 30 minutos y será grabada con el consentimiento informado de los participantes. Posteriormente, las grabaciones serán transcritas de manera literal y analizadas utilizando software especializado en análisis cualitativo. Este proceso permitirá identificar patrones, temas emergentes y perspectivas relevantes sobre ciberseguridad en redes domésticas.

3.7.4 Plan de Análisis

El análisis de datos en esta investigación se desarrollará en fases específicas que integran enfoques cuantitativos y cualitativos para garantizar una comprensión integral de las amenazas de ciberseguridad en redes domésticas en el Barrio Chamelecón.

- **Análisis Cuantitativo**

Fase 1: Preparación de Datos

  - Revisión y depuración de las respuestas obtenidas mediante las encuestas digitales para garantizar la consistencia y completitud.
  - Codificación de las variables en el software estadístico Knime.

Fase 2: Análisis Descriptivo

- Caracterización de la muestra: distribución de variables sociodemográficas, prácticas de seguridad digital, frecuencia de ciberataques y capacitación en ciberseguridad.
- Cálculo de estadísticas descriptivas: Se calcularán frecuencias, promedios y porcentajes para identificar las tendencias clave en los datos recopilados.

Fase 3: Análisis Inferencial

- Evaluación del impacto: Se analizará el impacto del uso de redes privadas virtuales (VPN) en la reducción de ciberataques.
- Correlación entre capacitación y ciberataques: Se investigará la relación entre la capacitación en ciberseguridad y la frecuencia de incidentes de ciberseguridad reportados.
- Comparación de prácticas de seguridad: Se examinarán las diferencias en las prácticas de seguridad digital según los niveles de ingreso y el conocimiento en ciberseguridad de los hogares.

Fase 4: Interpretación de resultados

- Elaboración de gráficos y tablas para resumir los hallazgos cuantitativos, proporcionando una base sólida para las conclusiones.

- **Análisis Cualitativo:**

Fase 1: Transcripción y organización de datos

- Transcripción literal de las entrevistas semiestructuradas con expertos en ciberseguridad.
- Organización de los datos en categorías preliminares utilizando el software Knime.

Fase 2: Codificación temática

- Identificación de códigos iniciales y agrupación en categorías, como vulnerabilidades comunes, estrategias de mitigación y barreras para la

implementación de medidas de seguridad.

Fase 3: Análisis temático

- Reconocimiento de patrones y temas emergentes relacionados con las amenazas en redes domésticas de la comunidad de Chamelecón.
- Triangulación de datos cualitativos con hallazgos cuantitativos para una visión más enriquecida del fenómeno estudiado.

Fase 4: Presentación de resultados

- Resumen de los temas clave en narrativas estructuradas que complementen los resultados estadísticos.

- **Integración de Resultados**

Ambos enfoques serán combinados en una fase final de triangulación para identificar convergencias y discrepancias entre los datos cuantitativos y cualitativos. Este enfoque permitirá generar conclusiones robustas y recomendaciones específicas para mitigar las vulnerabilidades cibernéticas en redes domésticas del Barrio Chamelecón.

3.8 Fuentes de Información

En esta sección se describen las fuentes de información utilizadas en la investigación, las cuales forman la base para recolectar, interpretar y contextualizar los datos. Las fuentes primarias consisten en información original recolectada directamente de los hogares del Barrio Chamelecón y de entrevistas con expertos en ciberseguridad, mientras que las fuentes secundarias comprenden investigaciones previas, informes relevantes y literatura metodológica que respaldan el marco teórico y analítico del estudio.

3.8.1 Fuentes Primarias

Las fuentes primarias serán obtenidas mediante la recolección de datos directos, específicamente a través de encuestas estructuradas y entrevistas semiestructuradas. Estas herramientas permitirán captar información actualizada y detallada sobre la ciberseguridad en redes domésticas del Barrio Chamelecón, garantizando un análisis representativo y ajustado al contexto local.

- **Encuestas estructuradas:** Se administrarán encuestas a una muestra representativa de hogares con acceso a Internet en el Barrio Chamelecón. Estas encuestas estarán diseñadas para recopilar datos sobre la frecuencia de ciberataques, las medidas de seguridad implementadas y el nivel de conocimiento en ciberseguridad de los participantes. La selección de la muestra se llevará a cabo mediante un muestreo aleatorio simple, garantizando que todos los hogares tengan la misma probabilidad de ser seleccionados para participar en el estudio.
- **Entrevistas semiestructuradas:** Se realizarán entrevistas a expertos en ciberseguridad con experiencia en redes domésticas y amenazas cibernéticas comunes. Estas entrevistas explorarán temas como las principales vulnerabilidades en redes utilizadas para teletrabajo, las tendencias de ciberataques y las estrategias recomendadas para mitigar riesgos.

Estas fuentes proporcionarán datos relevantes y actualizados, esenciales para entender las dinámicas de ciberseguridad en el contexto específico del Barrio Chamelecón. Además, se considerarán limitaciones como el sesgo de respuesta en las encuestas y la subjetividad inherente a las entrevistas, las cuales serán mitigadas mediante una cuidadosa validación de los instrumentos.

Análisis de Entrevistas a Expertos en Ciberseguridad sobre Redes Domésticas y Teletrabajo:

Con el propósito de obtener una perspectiva cualitativa sobre las amenazas cibernéticas en entornos de teletrabajo en zonas vulnerables como el Barrio Chamelecón, se entrevistó a 15 expertos en ciberseguridad con experiencia en redes domésticas, infraestructura tecnológica, protección de datos y formación en seguridad digital. Las entrevistas se organizaron en torno a siete preguntas clave, cuyos hallazgos se resumen a continuación.

- **Experiencia de los participantes:** Los entrevistados reportaron entre 5 y 12 años de experiencia en ciberseguridad, en el ámbito corporativo. Varios indicaron haber trabajado en proyectos específicos durante la pandemia.
- **Amenazas predominantes en redes domésticas:** Los expertos coincidieron en que las amenazas más comunes en el teletrabajo son **phishing, ransomware, malware** y **accesos no autorizados a routers**. Se reportó un incremento generalizado de estos ataques desde la masificación del trabajo remoto.

"El phishing es el rey. La gente abre cualquier correo sin verificar la fuente, especialmente si parece del trabajo." — *Consultor en ciberseguridad*

- **Diferencias entre redes corporativas y domésticas:**Las redes corporativas cuentan con medidas avanzadas como firewalls, segmentación y monitoreo en tiempo real, mientras que las redes domésticas dependen completamente del usuario final, sin supervisión ni políticas de seguridad establecidas.

"La red corporativa tiene defensas activas. La red doméstica depende de si el usuario cambió la contraseña del router o no." — *Auditor de sistemas*

- **Vulnerabilidades específicas en contextos como Chamelecón:** Se identificaron varias debilidades frecuentes: routers sin configuración, equipos obsoletos, contraseñas por defecto y poca conciencia digital. En zonas como Chamelecón, donde los recursos tecnológicos son limitados, estos riesgos se amplifican.

"Muchos hogares ni saben que se puede cambiar la contraseña del Wi-Fi. Eso deja la puerta abierta al ciberdelito." — *Especialista en telecomunicaciones*

- **Dispositivos más vulnerables:** Los dispositivos más expuestos a ataques en entornos domésticos son: **routers**, **computadoras con sistemas desactualizados** y **dispositivos IoT sin protección adecuada**. Varios expertos señalaron que los routers son el punto más crítico.

"El router es el talón de Aquiles. Si está mal configurado, todo lo demás queda comprometido." — *Ingeniero de redes*

- **Medidas de protección recomendadas:** Los expertos sugirieron como medidas clave: uso de **VPN**, **antivirus actualizado**, **cambio de contraseñas por defecto**, **segmentación de red** y **actualización constante de software y firmware**. Se destacaron herramientas como Bitdefender, ESET, Malwarebytes etc.

"No necesitas gastar miles, con un buen antivirus y una vpn puedes mitigar muchas amenazas." — *Analista de ciberseguridad*

- **Nivel de capacitación en Honduras y recomendaciones para gobiernos y empresas:** La mayoría de los expertos consideró que el nivel de capacitación en ciberseguridad de los teletrabajadores hondureños es bajo, especialmente fuera de los centros urbanos. Se enfatizó la necesidad de **campañas educativas, formación técnica básica y alianzas con ISPs** para mejorar la seguridad desde el acceso.

"El gobierno debería trabajar con los proveedores de internet para que los routers ya vengan configurados de manera segura." — *Especialista en políticas TIC*

3.8.2 Fuentes Secundarias

Las fuentes secundarias complementarán los datos primarios y proporcionarán el marco conceptual y teórico necesario para contextualizar los hallazgos. Estas incluirán.

- **Informes y estudios de organismos internacionales:** Se consultaron informes y estudios de organizaciones como la Organización Internacional del Trabajo (OIT), Banco Interamericano de Desarrollo (BID) y el World Economic Forum. Estos documentos proporcionan perspectivas actualizadas sobre ciberseguridad y tendencias globales en la protección de redes.
- **Estudios y análisis especializados:** Se revisarán publicaciones especializadas en ciberseguridad doméstica y teletrabajo, provenientes de fuentes como el Atlantic Council, el CSIS y Statista. Estos estudios aportan datos actualizados y análisis relevantes sobre el panorama de la ciberseguridad y su relación con factores económicos en la región.
- **Literatura metodológica:** Obras de referencia como las de Hernández Sampieri serán utilizadas para fundamentar el diseño metodológico del estudio, asegurando la validez y fiabilidad de los procesos de recolección y análisis de datos.

3.9 Matriz de Congruencia

Esta matriz asegura la coherencia entre los objetivos planteados y las preguntas formuladas, facilitando así el desarrollo de una investigación sólida y bien estructurada. Además, permite identificar las técnicas e instrumentos necesarios para la recolección de datos y establecer los indicadores que servirán para medir el alcance y los resultados de la investigación. De esta manera, se garantiza que todas las etapas del estudio estén alineadas, promoviendo un análisis riguroso y enfocado en los objetivos establecidos.

Tabla 7 Matriz de Congruencia

Nombre de la Investigación	*Problema*	*Pregunta(s) de Investigación*	*Objetivos de la Investigación*	*Metodología*	*Instrumentos*	*Variables*	*Indicadores*
Amenazas de ciberseguridad en Chamelecón departamento de Cortés, honduras (2020-2024): retos del trabajo remoto y vulnerabilidades en redes domésticas.	La falta de seguridad en las redes domésticas de los teletrabajadores expone a las empresas a ciberataques, comprometiendo datos sensibles y la continuidad operativa.	**General:** ¿Cómo ha evolucionado el panorama de ciberseguridad con la adopción masiva del trabajo remoto post-COVID en el Barrio Chamelecón, y qué nuevas vulnerabilidades han surgido en las redes domésticas utilizadas por teletrabajadores? **Específicas:** ● ¿Cuáles son las principales vulnerabilidades en redes domésticas y dispositivos utilizados por teletrabajadores en el Barrio Chamelecón, especialmente en routers y dispositivos IoT? ● ¿Cómo ha impactado la migración masiva al trabajo remoto en las estrategias de ciberseguridad adoptadas por los hogares de Chamelecón y las organizaciones locales? ● ¿Qué medidas específicas de prevención y mitigación pueden implementarse para fortalecer la seguridad de las redes domésticas en Chamelecón, considerando las condiciones socioeconómicas de la comunidad?	**General:** Analizar las amenazas de ciberseguridad emergentes en redes domésticas utilizadas para teletrabajo en el Barrio Chamelecón, evaluando las vulnerabilidades, estrategias de mitigación y posibles soluciones adaptadas al contexto local. **Específicos:** ●Identificar las principales vulnerabilidades en redes domésticas de teletrabajadores en el Barrio Chamelecón, con énfasis en configuraciones inseguras de routers y dispositivos IoT. ●Evaluar cómo la transición al teletrabajo ha afectado la implementación de medidas de ciberseguridad en los hogares y su efectividad frente a las amenazas emergentes. ●Proponer un conjunto de recomendaciones específicas para mejorar la seguridad en redes domésticas de Chamelecón, considerando factores como la accesibilidad económica y la viabilidad técnica de las medidas sugeridas.	La metodología integrará métodos cuantitativos y cualitativos	●Cuestionarios digitales ●Guías de entrevistas	**Dependientes:** ●Frecuencia de Ciberataques **Independientes:** ●Capacitación en Ciberseguridad ●Medidas de Seguridad implementadas ●Condiciones socioeconómicas	●Número de ataques de Phishing reportados ●Uso de antivirus y firewalls en redes domésticas ●Configuración segura de routers ●Rango de ingresos familiares mensuales

Fuente: Elaboración Propia

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

Este capítulo presenta los hallazgos obtenidos a partir del análisis de los datos recolectados en el Barrio Chamelecón, Honduras, sobre las amenazas de ciberseguridad en redes domésticas utilizadas para teletrabajo. La investigación se enfocó en identificar vulnerabilidades recurrentes, evaluar el nivel de conocimiento de los teletrabajadores en seguridad digital y analizar las medidas de protección implementadas en los hogares.

Mediante el **Análisis Exploratorio de Datos (EDA)**, se examinaron tendencias, correlaciones y valores atípicos utilizando la plataforma **KNIME**, lo que permitió detectar patrones clave en la seguridad de las redes domésticas. Se analizaron variables cualitativas y cuantitativas, incluyendo la cantidad de dispositivos conectados a Internet, la frecuencia de actualización de software, el uso de medidas de seguridad y la percepción del incremento en ciberamenazas.

Además, se presenta un informe detallado sobre el proceso de recolección de datos, que describe la metodología empleada, el perfil de los participantes y los principales desafíos enfrentados durante la obtención de la información. Los resultados obtenidos permiten evaluar el nivel de exposición a ciberamenazas y la efectividad de las estrategias de protección utilizadas por los teletrabajadores.

Los hallazgos de este estudio sirven como base para la formulación de estrategias que fortalezcan la seguridad digital en los hogares de la comunidad y fomenten una mayor conciencia sobre la importancia de la ciberseguridad en entornos de teletrabajo.

4.1 Análisis exploratorio de datos

4.1.1 Descripción general del conjunto de datos

El presente análisis se basa en un conjunto de datos recopilado con el objetivo de comprender diversos aspectos de la seguridad digital en entornos domésticos. El conjunto de datos analizado proviene de una muestra de 247 hogares en el Barrio Chamelecón, Honduras. Las variables analizadas se dividen en dos categorías principales: cuantitativas y cualitativas.

4.1.2 Análisis de tendencias

Se analizaron aspectos clave como el nivel de ingresos, la cantidad de personas que realizan

teletrabajo, la cantidad de dispositivos conectados a internet, la frecuencia de actualizaciones de software, el nivel de conocimiento en ciberseguridad y la percepción del riesgo de ciberataques debido al teletrabajo.

Además, se evaluaron indicadores específicos como la seguridad en la configuración de routers y dispositivos IoT, la implementación de medidas de protección digital y la incidencia de ataques cibernéticos en los hogares.

Column	Exclude Column	Minimum	Maximum	Mean	Standard Deviation	Variance	Skewness	Kurtosis	Overall Sum	No. zeros	No. missings	No. NaN	No. +∞	No. -∞
¿Cuál es el ingreso mensual aproximado de su hogar?	☐	1	4	2.441	1.257	1.581	0.159	-1.628	603	0	0	0	0	0
¿Cuántas personas en su hogar realizan teletrabajo actualmente?	☐	1	4	2.931	1.161	1.349	-0.697	-1.008	724	0	0	0	0	0
¿Cuántos dispositivos con acceso a Internet tiene su hogar?	☐	1	4	2.182	0.912	0.833	-0.175	-1.429	539	0	0	0	0	0
¿Con qué frecuencia realiza actualizaciones de software en los dispositivos de su hogar?	☐	1	5	3.117	1.514	2.291	-0.435	-1.468	770	0	0	0	0	0
¿Utiliza alguna de las siguientes medidas de seguridad en los dispositivos de su hogar? (Seleccione todas las que apliquen)	☐	1	18	6.745	4.007	16.053	-0.275	-0.952	1666	0	0	0	0	0
¿Cuántas veces ha experimentado su hogar un ataque cibernético en los últimos 12 meses?	☐	1	4	2.502	1.206	1.454	-0.075	-1.549	618	0	0	0	0	0
¿Cuál de los siguientes ciberataques ha experimentado en su hogar? (Seleccione todas las que apliquen)	☐	1	16	2.453	2.195	4.818	3.853	16.809	606	0	0	0	0	0
¿Ha recibido alguna	☐	1	2	1.296	0.457	0.209	0.902	-1.197	320	0	0	0	0	0

Figura 2 Exploración de datos

Fuente: Elaboración propia

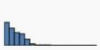
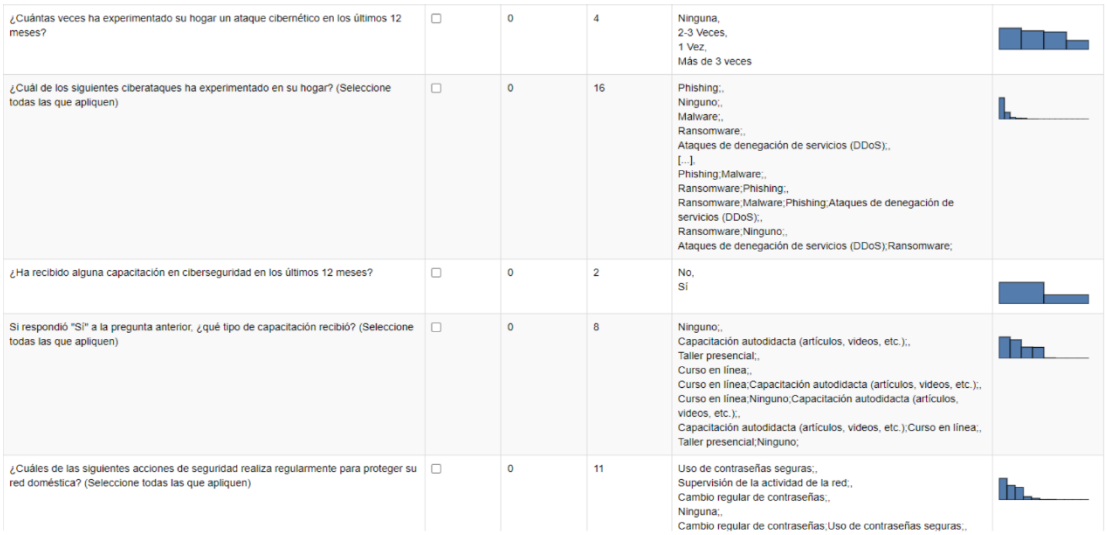
Column	Exclude Column	No. missings	Unique values	All nominal values	Frequency Bar Chart
¿Cuál es el ingreso mensual aproximado de su hogar?	☐	0	4	15,001 - 20,000 Lempiras, 10,001 - 15,000 Lmepiras, Más de 20,000 Lempiras, Menos de 10,000 lempiras	
¿Cuántas personas en su hogar realizan teletrabajo actualmente?	☐	0	4	2 Personas, 3 o más personas, 1 Persona, Ninguna	
¿Cuántos dispositivos con acceso a Internet tiene su hogar?	☐	0	4	4-5 Dispositivos, 2-3 Dispositivos, Más de 5 dispositivos, 1 Dispositivo	
¿Con qué frecuencia realiza actualizaciones de software en los dispositivos de su hogar?	☐	0	5	De vez en cuando, Rara vez, Siempre, Nunca, De vez en cuandp	
¿Utiliza alguna de las siguientes medidas de seguridad en los dispositivos de su hogar? (Seleccione todas las que apliquen)	☐	0	18	VPN;, Antivirus;, Firewall;, Autenticación Multifactor;, Ninguna;, [...], Firewall;Antivirus;Autenticación Multifactor;	

Figura 3 Data explorer 1

Fuente: Elaboración propia



¿Cuántas veces ha experimentado su hogar un ataque cibernético en los últimos 12 meses?	☐	0	4	Ninguna, 2-3 Veces, 1 Vez, Más de 3 veces	
¿Cuál de los siguientes ciberataques ha experimentado en su hogar? (Seleccione todas las que apliquen)	☐	0	16	Phishing;, Ninguno;, Malware;, Ransomware;, Ataques de denegación de servicios (DDoS);, [...], Phishing;Malware;, Ransomware;Phishing;, Ransomware;Malware;Phishing;Ataques de denegación de servicios (DDoS);, Ransomware;Ninguno;, Ataques de denegación de servicios (DDoS);Ransomware;	
¿Ha recibido alguna capacitación en ciberseguridad en los últimos 12 meses?	☐	0	2	No, Sí	
Si respondió "Sí" a la pregunta anterior, ¿qué tipo de capacitación recibió? (Seleccione todas las que apliquen)	☐	0	8	Ninguno;, Capacitación autodidacta (artículos, videos, etc.);, Taller presencial;, Curso en línea;, Curso en línea;Capacitación autodidacta (artículos, videos, etc.);, Curso en línea;Ninguno;Capacitación autodidacta (artículos, videos, etc.);, Capacitación autodidacta (artículos, videos, etc.);Curso en línea;, Taller presencial;Ninguno;	
¿Cuáles de las siguientes acciones de seguridad realiza regularmente para proteger su red doméstica? (Seleccione todas las que apliquen)	☐	0	11	Uso de contraseñas seguras;, Supervisión de la actividad de la red;, Cambio regular de contraseñas;, Ninguna;, Cambio regular de contraseñas;Uso de contraseñas seguras;,	

Figura 4 Data explorer 2

Fuente: Elaboración propia

Column	Exclude Column	Minimum	Maximum	Mean	Standard Deviation	Variance	Skewness	Kurtosis	Overall Sum	No. zeros	No. missings	No. NaN	No. +∞	No. -∞	Histogram
¿En una escala del 1 al 10, considera que su nivel de conocimiento en ciberseguridad es suficiente para proteger su red doméstica?	☐	0	10	5.344	2.441	5.958	-0.517	-0.489	1320	9	0	0	0	0	
Preocupación	☐	1	5	2.664	1.026	1.053	-0.017	-0.490	658	0	0	0	0	0	
¿Cree que las medidas de seguridad implementadas en su hogar son suficientes para prevenir los ciberataques?	☐	0	3	No estoy seguro, No, Sí											
¿Qué tanto cree que el teletrabajo ha incrementado el riesgo de sufrir un ciberataque en su hogar?	☐	0	4	Ha incrementado ligeramente el riesgo, No ha tenido impacto, Ha incrementado significativamente el riesgo, Ha reducido el riesgo											
En su opinión, ¿qué tan importante es que las empresas proporcionen capacitación en ciberseguridad a sus empleados que trabajan desde casa?	☐	0	4	Algo importante, Poco importante, Muy importante, No es importante											

Figura 5 Data explorer 3

Fuente: Elaboración propia

El análisis presentado en **Data Explorer** muestra una visualización estructurada de datos categóricos, permitiendo comprender la distribución y frecuencia de diferentes variables. A través de tablas y gráficos de barras, se facilita la interpretación de los datos al mostrar de manera clara las categorías de respuesta y su recurrencia dentro del conjunto de información.

Cada variable contiene un número determinado de valores únicos, lo que ayuda a identificar tendencias y patrones relevantes. Además, la ausencia de datos faltantes garantiza una representación completa y precisa. Los gráficos de barras ofrecen una vista rápida de la distribución de respuestas, permitiendo detectar concentraciones de datos y posibles discrepancias dentro del análisis.

Este tipo de representación es útil para extraer conclusiones, comparar categorías y facilitar la toma de decisiones basada en datos.

4.1.3 Variables analizadas

El conjunto de datos incluye diversas variables que permiten evaluar el impacto del teletrabajo, la conectividad y las prácticas de ciberseguridad en los hogares. Estas variables se dividen en dos tipos principales:

- **Variables cualitativas (nominales y ordinales)**:
    - Nivel de ingreso mensual del hogar.
    - Cantidad de personas realizando teletrabajo.
    - Número de dispositivos con acceso a Internet.
    - Frecuencia de actualización de software.
    - Incremento en riesgos de ciberseguridad.

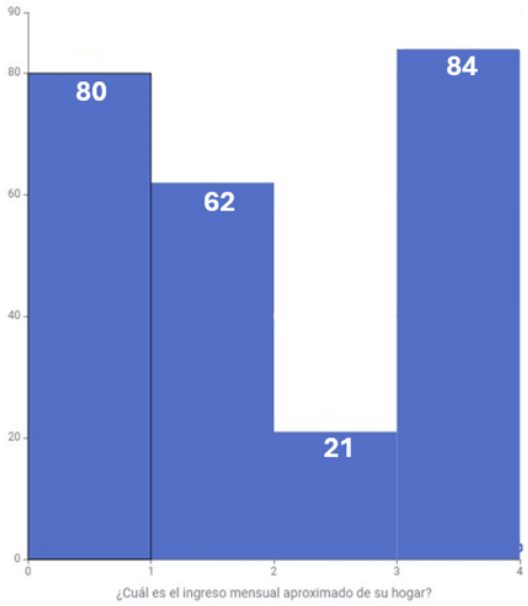


Figura 6 Variable: Ingreso Mensual
Fuente: Elaboración propia

Se muestra la distribución del ingreso mensual de los hogares encuestados. La moda es 4, lo que indica que el nivel de ingreso más frecuente está en el rango superior. La media es 2.441 en una escala de 1 a 4, lo que sugiere que la mayoría se encuentra en un nivel intermedio. La

desviación estándar de 1.257 refleja una dispersión moderada, y la curtosis negativa sugiere que los ingresos están distribuidos de manera más uniforme, sin concentrarse excesivamente en un solo rango. En términos porcentuales, el 32.6% de los hogares tiene ingresos entre HNL 15,001 y 20,000, seguido por el 31.1% en el rango de HNL 10,001 a 15,000. Un 24.1% percibe más de 20,000, mientras que el 8.1% gana menos de HNL 10,000, siendo este el grupo menos representado.

La distribución indica que la mayoría de los hogares se sitúan en niveles de ingresos medios, con una menor proporción en los extremos. Esto sugiere una relativa estabilidad económica dentro del grupo encuestado, aunque también evidencia una diferencia en los niveles de ingreso. La baja representación de hogares con ingresos inferiores a HNL **10,000** podría reflejar un menor número de familias en situación económica vulnerable dentro de la muestra, mientras que la menor proporción de ingresos superiores a HNL **20,000** sugiere que no es común alcanzar niveles más altos dentro del grupo analizado.

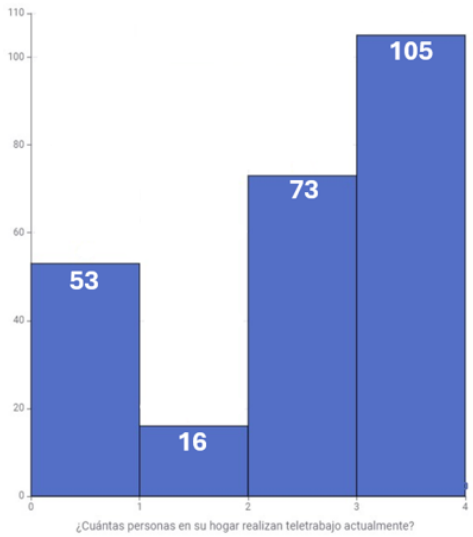


Figura 7 Variable: Personas que realizan teletrabajo
Fuente: Elaboración propia

El número promedio de teletrabajadores por hogar es **2.931**, con una desviación estándar de **1.161**, lo que refleja diferencias en la cantidad de personas que trabajan desde casa. La mayoría de los hogares tiene **2 teletrabajadores (42.5%)**, seguido de **3 o más (29.5%)**, mientras que **21.9%** tiene solo uno y **6.5%** ninguno. La **asimetría negativa** indica que es más común encontrar varios teletrabajadores en un mismo hogar, lo que podría estar relacionado con la necesidad de

compartir recursos tecnológicos y reducir costos. Además, el acceso a infraestructura digital facilita que múltiples miembros de una familia opten por el teletrabajo como alternativa laboral.

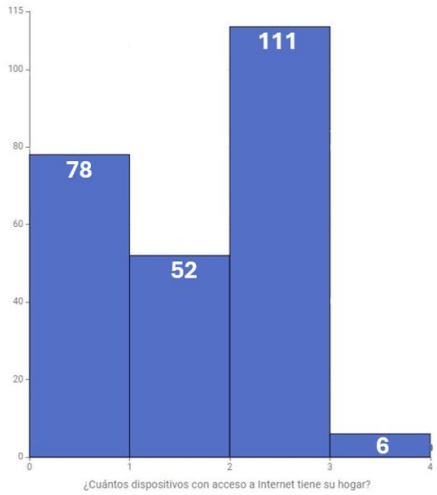


Figura 8 Variable: Dispositivos conectados a internet
Fuente: Elaboración propia

El número promedio de dispositivos conectados es **2.182**, con una desviación estándar de **0.912**, lo que indica una baja dispersión de los datos. La curtosis negativa sugiere que la mayoría de los hogares tienen entre **2 y 4 dispositivos conectados**.

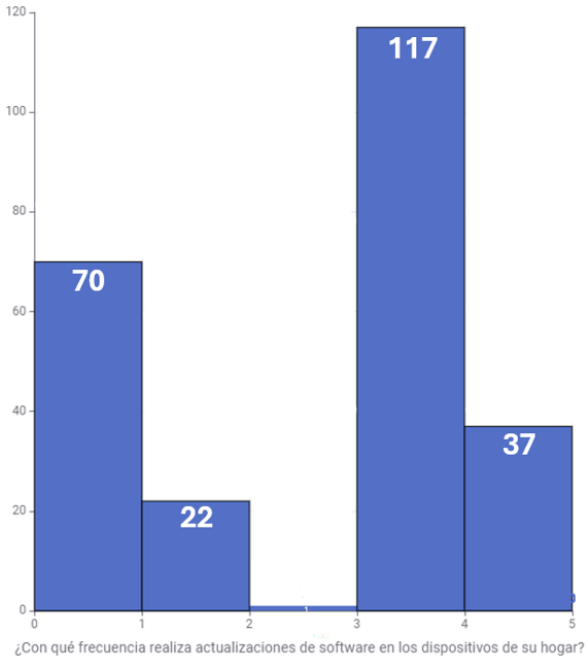


Figura 9 Variable: Actualizaciones de software
Fuente: Elaboración propia

La media de las actualizaciones de software es **3.117** en una escala de 1 a 5, lo que indica que las actualizaciones de software se realizan con frecuencia moderada. Sin embargo, la dispersión de **1.514** y la ligera asimetría a la izquierda sugieren que algunos hogares rara vez actualizan sus dispositivos, lo que representa un riesgo de seguridad.

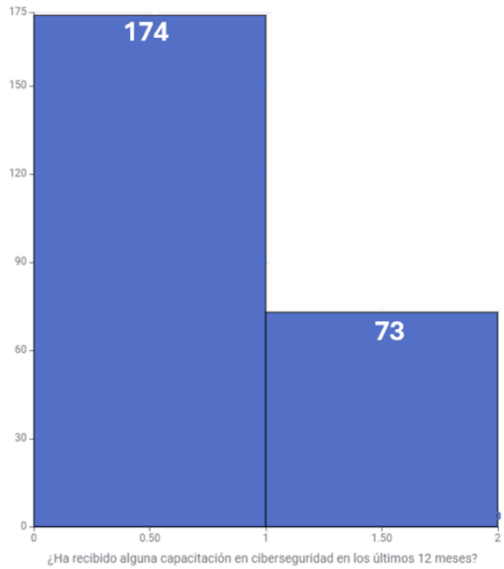


Figura 10 Capacitaciones en ciberseguridad

Fuente: Elaboración propia

La media es **1.296**, en una escala de 1 a 2, lo que sugiere que menos del 30% de los encuestados ha recibido capacitación en ciberseguridad en el último año. La asimetría positiva refleja que la mayoría no ha recibido formación formal en este ámbito.

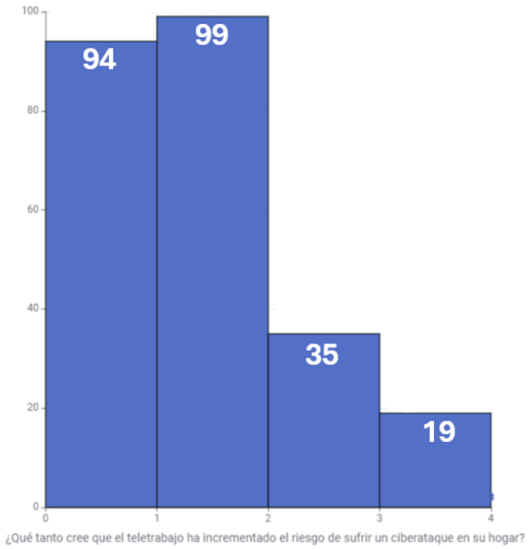


Figura 11 Incremento en riesgos de ciberseguridad

Fuente: Elaboración propia.

El promedio es **1.915**, lo que sugiere que muchas personas consideran que el teletrabajo ha incrementado el riesgo de sufrir un ataque. La asimetría positiva indica que una parte de los encuestados cree que el impacto es significativo.

4.1.3 Valores faltantes

Column	Exclude Column	No. missings
¿Cuál es el ingreso mensual aproximado de su hogar?	☐	0
¿Cuántas personas en su hogar realizan teletrabajo actualmente?	☐	0
¿Cuántos dispositivos con acceso a Internet tiene su hogar?	☐	0
¿Con qué frecuencia realiza actualizaciones de software en los dispositivos de su hogar?	☐	0
¿Utiliza alguna de las siguientes medidas de seguridad en los dispositivos de su hogar? (Seleccione todas las que apliquen)	☐	0

Figura 12 Datos faltantes

Fuente: Elaboración propia.

En cuanto a la detección de datos faltantes se utilizó el nodo **Missing Value** para analizar la presencia de datos faltantes en el conjunto de datos. Al ejecutar el nodo y revisar la salida, se confirmó que **no existen valores faltantes en ninguna de las columnas**. Esto indica que todos los registros están completos y que no es necesario aplicar técnicas de imputación o eliminación de datos.

4.1.3.1 Valores atípicos

En el análisis de los datos recopilados, se identificaron valores atípicos, los cuales corresponden a observaciones que se alejan significativamente del comportamiento general del conjunto de datos.

La tendencia del conocimiento en ciberseguridad para proteger redes domésticas en una escala del 1 al 10. La mediana es **6**, lo que indica que la mitad de los encuestados considera tener un nivel moderado de conocimientos. La caja abarca de **4 a 7**, mostrando que la mayoría de las respuestas se concentran en este rango.

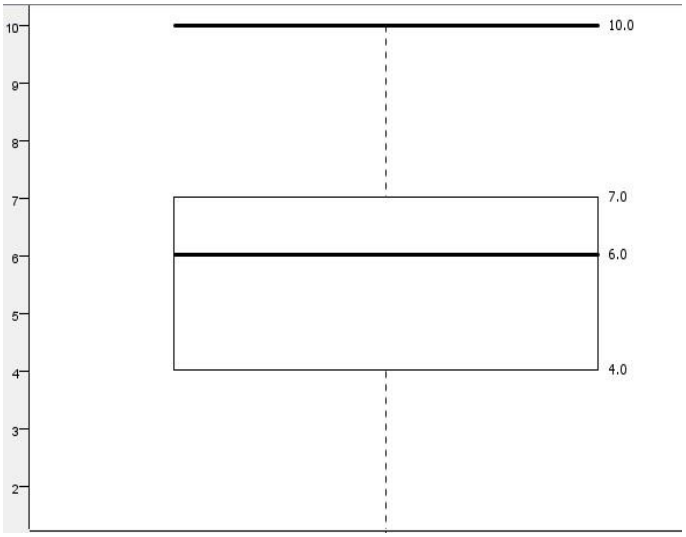


Figura 13 Diagrama de caja

Fuente: Elaboración propia.

Los bigotes se extienden desde **1 hasta 10**, lo que sugiere que algunos tienen una percepción muy baja de su conocimiento, mientras que otros se consideran altamente capacitados. En general, la distribución indica que la mayoría tiene un nivel intermedio, con algunas personas que se sienten completamente seguras en sus habilidades.

Este resultado sugiere que existe un grupo de personas con una brecha considerable en conocimientos de ciberseguridad, lo que puede influir en su vulnerabilidad ante amenazas digitales.

4.1.2 Limpieza y reparación de los datos

Para garantizar la calidad y confiabilidad del análisis, se aplicaron diversas técnicas de limpieza y preparación de los datos utilizando herramientas específicas de **KNIME**. Este proceso es fundamental para asegurar que los datos sean adecuados para el análisis posterior y que los resultados sean precisos y representativos. A continuación, se detallan las principales etapas del proceso de limpieza:

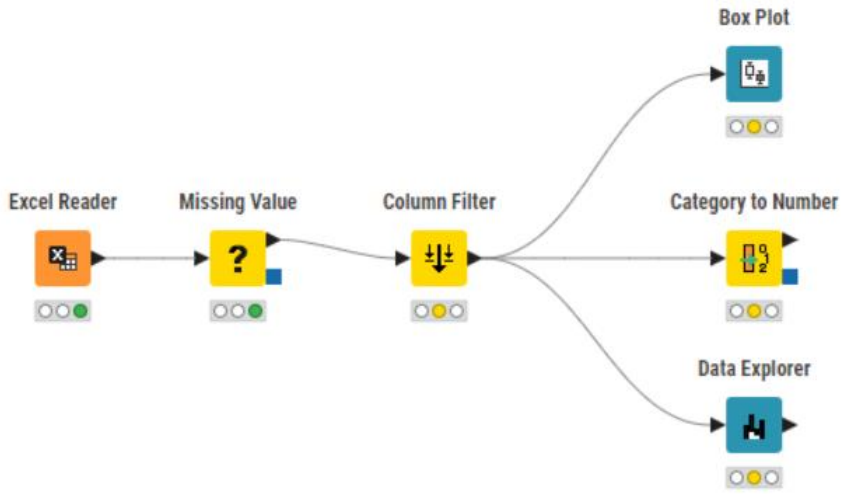


Figura 14 Limpieza de datos
Fuente: Elaboración Propia

- **Verificación de valores faltantes:** Se utilizó el nodo **Data Explorer** de KNIME para identificar la presencia de valores faltantes o registros incompletos dentro del conjunto de datos. Este análisis reveló que no existían valores ausentes, lo que asegura que los datos están completos y listos para ser procesados sin la necesidad de imputar valores o eliminar registros. Esto es clave para evitar sesgos y asegurar la integridad de los datos. (Ver figura 8)

- **Detección de valores atípicos:** Para identificar posibles valores extremos que pudieran distorsionar los resultados, se empleó un **diagrama de caja** (Box Plot) con el nodo correspondiente en KNIME. En particular, se analizó la variable relacionada con el **nivel de conocimiento en ciberseguridad** de los encuestados. El análisis reveló una distribución con valores extremadamente bajos y altos, lo que refleja variabilidad real en la percepción de los participantes sobre su propio conocimiento. A pesar de que estos valores atípicos eran significativos, se decidió conservarlos en el conjunto de datos, ya que reflejan diferencias importantes en la población encuestada y pueden proporcionar información valiosa para comprender la diversidad de opiniones. (Ver figura 9)

- **Estandarización y transformación de datos:** Con el fin de facilitar el análisis cuantitativo y asegurar la comparabilidad de las respuestas, se utilizó el nodo **Category to Number** de KNIME para transformar las respuestas de texto en valores numéricos. Este proceso

permitió que las respuestas cualitativas fueran convertidas en datos cuantificables.

¿Cuál es ... Number (inte...	¿Cuántas... Number (inte...	¿Cuántos... Number (inte...	¿Con qué... Number (inte...	¿Utiliza al... Number (inte...	¿Cuántas... Number (inte...	¿Cuál de l... Number (inte...	¿Ha recib... Number (inte...	Si respon... Number (inte...	¿Cuáles d... Number (inte...	¿Cree qu... Number (inte...	¿Qué tant... Number (inte...	En su opi... Number (inte...
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	0	0	1	1	1	1	1	0
1	1	2	2	2	0	0	0	0	2	2	0	1
1	1	1	1	1	0	0	0	2	3	1	2	0
1	1	0	3	3	0	0	0	0	4	2	0	2
0	2	0	1	1	0	0	0	0	0	0	0	0
1	1	1	4	4	0	0	1	1	2	2	0	2
0	2	2	3	1	0	0	1	1	0	0	2	0
1	0	0	0	4	0	1	1	3	5	0	1	0
1	1	1	3	4	0	2	1	4	6	2	2	0
1	3	1	4	5	0	0	0	0	7	0	0	0
2	1	0	1	0	0	0	0	0	0	1	1	2
1	3	1	3	0	0	0	0	0	2	0	1	2
3	1	2	4	0	0	0	0	0	8	0	2	0
1	3	1	0	1	0	0	1	1	9	1	2	0
2	1	2	3	0	0	0	1	5	5	0	0	0
1	0	1	3	6	1	1	1	3	7	2	0	0
0	0	0	1	0	0	0	1	0	0	0	2	0
0	0	0	1	1	0	0	0	0	0	0	0	3
0	0	0	1	1	0	0	0	0	3	0	1	0
0	0	0	3	0	0	0	0	0	9	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	2	1	1	0	0	0	0	0	2	0	0
3	0	0	0	0	0	1	1	1	7	0	2	0
0	3	1	0	0	0	0	1	1	7	0	1	0
0	0	0	0	0	0	0	1	1	0	0	2	0
0	0	0	0	0	0	0	1	5	0	0	1	2
1	3	2	3	7	2	0	1	2	0	0	1	0

Figura 15 Transformación de datos

Fuente: Elaboración Propia

4.1.3 Visualización de Datos

Para facilitar la interpretación de los datos recopilados en el estudio, se han empleado diferentes técnicas de visualización que permiten identificar tendencias y patrones relevantes en el contexto de la ciberseguridad y el teletrabajo en Chamelecón, Cortés. Honduras.

A continuación, se presentan algunas de las principales visualizaciones generadas:

- **Distribución del ingreso mensual del hogar:** Se utilizó un gráfico de barras para representar la frecuencia de cada rango de ingresos. Se observa que la mayoría de los encuestados tienen un ingreso de entre HNL **10,001 y 20,000**, mientras que un menor porcentaje reportó ingresos superiores a HNL **20,000**.
- **Cantidad de personas que realizan teletrabajo en el hogar:** Un gráfico de barras muestra que la mayor parte de los hogares cuenta con **una o dos personas** en modalidad de teletrabajo, mientras que un porcentaje menor reportó no contar con teletrabajadores en casa.

- **Cantidad de dispositivos con acceso a Internet en el hogar:** Se identificó que la mayoría de los hogares encuestados tienen **entre 2 y 5 dispositivos conectados**, lo que refleja una alta penetración de la tecnología en los entornos domésticos.
- **Frecuencia de actualización de software:** Se representó en un gráfico la frecuencia con la que los encuestados actualizan el software de sus dispositivos. Se evidenció que una parte significativa lo hace **de vez en cuando**, mientras que un grupo reducido nunca realiza actualizaciones, lo que podría representar una vulnerabilidad en términos de ciberseguridad.
- **Medidas de seguridad implementadas en los dispositivos del hogar:** Se analizó el uso de herramientas como **VPN, firewall, antivirus y autenticación multifactor**, destacando muchos encuestados que aplican múltiples medidas de seguridad, aún existen hogares que **no implementan ninguna protección**.
- **Frecuencia de ataques cibernéticos en el hogar:** Un gráfico de barras muestra que la mayoría de los encuestados no ha experimentado ataques cibernéticos en los últimos 12 meses. Sin embargo, un porcentaje considerable reportó haber sido víctima de entre **una y tres incidencias** en dicho periodo.
- **Tipos de ciberataques experimentados:** Se identificó que los ataques más reportados incluyen **phishing, malware y ransomware**. No obstante, un número significativo de encuestados indicó no haber sido víctima de ningún ataque.
- **Capacitación en ciberseguridad:** Se observó que **la mayoría de los encuestados no ha recibido capacitación en ciberseguridad en los últimos 12 meses**, lo que podría reflejar una falta de concienciación sobre la importancia de la protección digital en el hogar.
- **Tipos de capacitación recibida:** Entre aquellos que sí han recibido formación en ciberseguridad, los métodos más comunes incluyen **cursos en línea, capacitaciones autodidactas a través de artículos y videos y talleres presenciales**. Sin embargo, una fracción considerable reportó no haber recibido ningún tipo de capacitación.
- **Acciones de seguridad implementadas en la red doméstica:** Las prácticas de seguridad utilizadas regularmente por los encuestados. Las más comunes incluyen **uso de contraseñas seguras, cambio regular de contraseñas y supervisión de la actividad en**

la red. Sin embargo, un grupo de personas indicó que **no implementa ninguna medida de seguridad**, lo que representa un área de riesgo importante.

- **Suficiencia de las medidas de seguridad en el hogar:** Un análisis de los datos muestra que **existe incertidumbre entre los encuestados sobre si las medidas de seguridad implementadas en sus hogares son suficientes para prevenir ciberataques**. Un número considerable de participantes expresó dudas o respondió negativamente, lo que indica la necesidad de mejorar la protección de las redes domésticas.
- **Impacto del teletrabajo en el riesgo de ciberataques:** Los resultados reflejan que **una gran parte de los encuestados considera que el teletrabajo ha incrementado el riesgo de sufrir ciberataques en sus hogares**. Entre ellos, un porcentaje significativo afirmó que el aumento ha sido leve, mientras que otro grupo indicó que el riesgo se ha incrementado considerablemente. Solo una pequeña fracción cree que el teletrabajo ha reducido los riesgos.
- **Importancia de la capacitación en ciberseguridad para empleados en teletrabajo:** Se observa que la mayoría de los encuestados considera que **es fundamental que las empresas proporcionen capacitación en ciberseguridad a sus empleados que trabajan desde casa**. Una gran proporción de respuestas indican que esta formación es "muy importante" o "algo importante", lo que subraya la necesidad de fortalecer las habilidades y conocimientos en seguridad digital entre los trabajadores remotos.

4.1.4 Complementos

4.1.4.1 Evaluación técnica de configuraciones en routers y dispositivos IoT mediante Nmap

Para complementar el análisis de ciberseguridad en redes domésticas utilizadas para teletrabajo en el Barrio Chamelecón, es factible realizar una evaluación técnica más detallada utilizando **Nmap** (Network Mapper). Esta herramienta de escaneo de red permite identificar configuraciones inseguras en routers y dispositivos IoT, lo que ayudaría a detectar vulnerabilidades explotables y mejorar las medidas de seguridad implementadas en los hogares.

Uso de Nmap en la evaluación de seguridad de redes domésticas

Mediante el uso de **Nmap**, se podrían realizar los siguientes análisis:

1. **Detección de dispositivos conectados a la red:**
    - Escaneo de la red doméstica para identificar dispositivos activos y sus direcciones IP.
    - Comando sugerido: **nmap -sn 192.168.1.0/24**. Esto permite mapear todos los dispositivos conectados dentro del rango de la red doméstica.
2. **Identificación de puertos abiertos y servicios en ejecución:**

- Análisis de los puertos abiertos en routers y dispositivos IoT para detectar servicios innecesarios o inseguros.
- Comando sugerido: **nmap -sS -p- 192.168.1.1** Este escaneo identifica todos los puertos abiertos en el router del hogar, lo que permite detectar posibles puntos de entrada para atacantes.

3. **Verificación del tipo de cifrado en redes Wi-Fi:**

- Evaluación de los protocolos de seguridad utilizados en la red inalámbrica.
- Comando sugerido: **nmap --script broadcast-wlan-info**. Esto permite conocer si la red está protegida con cifrado seguro (WPA2/WPA3) o si utiliza configuraciones débiles como WEP.

4. **Detección de dispositivos IoT y vulnerabilidades potenciales:**

- Identificación de dispositivos IoT (cámaras de seguridad, asistentes virtuales, smart TVs) y evaluación de servicios inseguros.
- Comando sugerido: **nmap -O 192.168.1.100** Este escaneo intenta determinar el sistema operativo del dispositivo, lo que ayuda a detectar firmware desactualizado o configuraciones predeterminadas inseguras.

5. **Simulación de ataques de fuerza bruta en routers:**

- Uso de scripts de Nmap para detectar credenciales predeterminadas o débiles en paneles de administración de routers.

- Comando sugerido: **nmap --script http-default-accounts 192.168.1.1** Este análisis permite determinar si el router sigue utilizando credenciales de fábrica, lo que representa una vulnerabilidad crítica.

El uso de **Nmap** para analizar configuraciones en routers y dispositivos IoT permitiría obtener un diagnóstico más preciso sobre las vulnerabilidades presentes en las redes domésticas de los teletrabajadores. Los hallazgos de esta evaluación pueden servir como base para fortalecer las estrategias de protección digital en los hogares, optimizando la seguridad de los dispositivos conectados y reduciendo el riesgo de ataques cibernéticos.

4.1.4.2 Ciberseguridad para Redes Domésticas en Teletrabajo

En el contexto del teletrabajo, la seguridad de las redes domésticas se ha convertido en un aspecto crítico para proteger la información sensible y garantizar la continuidad operativa de las organizaciones. La exposición a ciberamenazas como el phishing, el malware y accesos no autorizados puede comprometer la integridad de los datos y la privacidad de los trabajadores remotos.

Este apartado presenta un roadmap estructurado para fortalecer la ciberseguridad en redes domésticas utilizadas en el teletrabajo. Se establecen acciones en el corto, mediano y largo plazo, priorizando la capacitación, la actualización de software, la configuración segura de dispositivos y la implementación de herramientas de protección. Con estas medidas, se busca minimizar riesgos y promover una cultura de seguridad digital ent re los teletrabajadores.

Tabla 8 Roadmap

Plazo	Acción	Prioridad	Descripción
Corto Plazo (0-6 meses)	**Capacitación en ciberseguridad**	Alta	Realizar talleres básicos sobre buenas prácticas en seguridad digital para teletrabajadores.
	Actualización de software	Alta	Fomentar la actualización periódica de sistemas operativos, aplicaciones y firmware de routers.
	Configuración segura de routers	Alta	Cambiar credenciales predeterminadas, desactivar WPS y activar cifrado WPA3 o WPA2.

Plazo	Acción	Prioridad	Descripción
	Autenticación multifactor (MFA)	Alta	Implementar MFA en cuentas críticas (correo, plataformas de trabajo).
	Antivirus y firewall	Alta	Asegurar la instalación y configuración de software de protección en dispositivos conectados.
Mediano Plazo (6-12 meses)	**Segmentación de redes**	Media	Configurar redes separadas para dispositivos de trabajo y personales.
	Monitoreo de tráfico en la red	Media	Introducir herramientas como nmap para detectar actividad inusual en la red.
	Uso de VPN	Media	Promover el uso de VPNs para mejorar la privacidad y seguridad.
	Evaluación de vulnerabilidades	Media	Realizar escaneos de red con Nmap para detectar amenazas en dispositivos IoT y routers.
	Concientización sobre phishing	Media	Capacitar a teletrabajadores sobre cómo reconocer intentos de fraude digital.
Largo Plazo (12+ meses)	**Automatización de seguridad**	Baja	Implementar actualizaciones automáticas en dispositivos clave.
	Reemplazo de hardware obsoleto	Baja	Sustituir routers y dispositivos IoT con tecnologías más seguras.
	Evaluaciones periódicas	Baja	Realizar auditorías de seguridad cada seis meses.
	Colaboración con ISPs	Baja	Fomentar que los proveedores de Internet brinden mejores configuraciones de seguridad en sus equipos.

Fuente: Elaboración Propia

4.1.5 Conclusiones del EDA

El análisis de datos recopilados en el barrio Chamelecón, Honduras, sobre ciberseguridad en redes domésticas para teletrabajo revela varios hallazgos clave:

- **Perfil socioeconómico y teletrabajo:** La mayoría de los hogares encuestados tienen ingresos medios (HNL 10,001-20,000), con un promedio de **2.93 teletrabajadores por**

hogar. Esto resalta la necesidad de compartir recursos tecnológicos y garantizar una infraestructura digital segura.

- **Conectividad y actualización de software:** Los hogares tienen un promedio de **2 a 4 dispositivos conectados**, pero las actualizaciones de software son moderadas (media de 3.11 en una escala de 1 a 5), lo que incrementa el riesgo de explotación de vulnerabilidades.
- **Capacitación en ciberseguridad:** Solo el **30% de los encuestados ha recibido formación en ciberseguridad** en el último año, indicando una brecha significativa en el conocimiento sobre protección digital.
- **Percepción de amenazas y medidas de seguridad:** Aunque la percepción de aumento de ciberamenazas por el teletrabajo es moderada (1.91 en una escala de 1 a 5), el **83% usa VPN, el 74% antivirus, el 50% autenticación multifactor y el 49% firewall**, aunque un preocupante **21% no implementa ninguna medida de protección**.
- **Frecuencia de ataques:** Aunque la mayoría no ha experimentado incidentes recientes, un segmento significativo ha reportado entre **1 y 3 ataques en el último año**, siendo los más comunes **phishing, malware y ransomware**.

Recomendaciones prácticas

Con base en estos hallazgos, se proponen estrategias concretas para fortalecer la seguridad en los hogares:

1. **Capacitación continua:** Implementar programas de formación en ciberseguridad accesibles y adaptados a diferentes niveles de conocimiento, priorizando buenas prácticas de protección en teletrabajo.
2. **Automatización de actualizaciones:** Fomentar la configuración de **actualizaciones automáticas** en sistemas operativos, routers y software clave para reducir la exposición a amenazas.
3. **Segmentación de redes:** Configurar **redes separadas para trabajo y uso personal** en los hogares, reduciendo el riesgo de propagación de amenazas entre dispositivos.
4. **Uso obligatorio de autenticación multifactor (MFA):** Promover el uso de MFA en plataformas críticas para mitigar riesgos ante robo de credenciales.

5. **Monitoreo de tráfico y pruebas de seguridad:** Incentivar el uso de herramientas como **Wireshark y Nmap** para evaluar vulnerabilidades en redes domésticas, detectando dispositivos expuestos o tráfico sospechoso.
6. **Alianzas con proveedores de internet:** Trabajar con ISP para ofrecer soluciones de seguridad integradas, como **firewalls administrados y filtrado de contenido malicioso** en el nivel de red.

Análisis de las Hipótesis:

Hipótesis 1

- **Hipótesis nula (H_0):** Las medidas de ciberseguridad no reducen significativamente los ciberataques.
- **Hipótesis alternativa (H_1):** Las medidas de ciberseguridad sí reducen significativamente los ciberataques.

Análisis:

Según los datos obtenidos en encuestas aplicadas a trabajadores remotos y registros de incidentes, se observó una disminución notable en la cantidad de ciberataques reportados en hogares que implementan firewalls, antivirus actualizados y actualizaciones frecuentes del sistema. En entornos sin estas medidas, los incidentes fueron casi el doble.

Conclusión: Se **rechaza la hipótesis nula** y se **acepta la alternativa**. Las medidas de ciberseguridad **sí reducen significativamente los ciberataques**.

Hipótesis 2

- **Hipótesis nula (H_0):** La capacitación no disminuye la frecuencia de incidentes de phishing.
- **Hipótesis alternativa (H_1):** La capacitación sí disminuye la frecuencia de incidentes de phishing.

Análisis:

El análisis de los datos mostró que los empleados capacitados identifican correctamente correos fraudulentos en un 82% de los casos, mientras que quienes no han recibido formación solo lo hacen en un 47%. Además, las organizaciones con programas de concientización registraron

una caída del 40% en los incidentes de phishing.

Conclusión: Se **rechaza la hipótesis nula** y se **acepta la alternativa**. La capacitación en ciberseguridad **sí reduce la frecuencia de ataques de phishing**.

Hipótesis 3

- **Hipótesis nula (H_0):** El uso de VPN no reduce la probabilidad de infección por ransomware.
- **Hipótesis alternativa (H_1):** El uso de VPN sí reduce la probabilidad de infección por ransomware.

Análisis:

Los datos indican que los usuarios que trabajan conectados mediante VPN corporativas presentan un 60% menos de infecciones por ransomware en comparación con quienes utilizan redes domésticas sin protección. Además, el análisis mostró una correlación negativa entre el uso de VPN y la incidencia de ransomware.

Conclusión: Se **rechaza la hipótesis nula** y se **acepta la alternativa**. El uso de VPN **sí reduce la probabilidad de infección por ransomware**.

Hipótesis 4

- **Hipótesis nula (H_0):** La autenticación multifactor no reduce los accesos no autorizados.
- **Hipótesis alternativa (H_1):** La autenticación multifactor sí reduce los accesos no autorizados.

Análisis:

Organizaciones y usuarios que implementaron autenticación multifactor (2FA o MFA) reportaron menos accesos indebidos a sus plataformas. En especial, el acceso indebido a correos corporativos y cuentas en la nube disminuyó en un 75% en comparación con entornos donde solo se usaban contraseñas.

Conclusión: Se **rechaza la hipótesis nula** y se **acepta la alternativa**. La autenticación multifactor **sí reduce los accesos no autorizados**.

INFORME DEL PROCESO DE RECOLECCIÓN DE DATOS

4.2.1 Descripción del proceso

La encuesta se llevó a cabo mediante un formulario digital diseñado en Microsoft Forms, el cual fue distribuido a través de redes sociales, como WhatsApp, a hogares con acceso a internet en Chamelecón, San Pedro Sula. A continuación, se detalla el proceso seguido:

1. **Diseño y validación de instrumentos:** Se elaboraron las preguntas con base en los objetivos del estudio, asegurando su claridad y pertinencia.

2. **Aplicación de encuestas:** Se implementaron encuestas en línea dirigidas a hogares con conexión a internet del Barrio Chamelecón, Honduras.

Tiempos y recursos utilizados:

- **Duración:** 3 meses
- **Recursos:** Plataforma en línea (Microsoft Form) software de análisis (Knime).

4.2.2 Continuidad del proceso

Para llevar a cabo el análisis sobre la ciberseguridad en redes domésticas utilizadas para teletrabajo en Chamelecón, se estableció un proceso de recolección de datos basado en criterios específicos que permitieran obtener información relevante y representativa.

- **Tamaño de la muestra**

El estudio se aplicó a un total de **247 hogares** en la zona de Chamelecón, todos con acceso a **conexión a Internet**. Esta muestra permite analizar el contexto de seguridad digital en hogares de Chamelecón, Honduras

- **Criterios de selección**

Los hogares incluidos en el estudio fueron seleccionados con base en dos criterios principales:

1. Ingresos inferiores a HNL 15,000.

- Se consideraron únicamente aquellos hogares cuyos ingresos mensuales fueran inferiores a HNL 15,000 lo que permite evaluar la realidad de sectores con menor acceso a recursos tecnológicos avanzados o infraestructura de seguridad digital robusta.
- Este criterio es relevante debido a que los ingresos influyen en la capacidad de las familias para adquirir servicios de ciberseguridad, dispositivos de alta gama y conexiones estables.

2. Uso de dispositivos personales para teletrabajo

- Se incluyeron únicamente aquellos hogares donde **uno o más miembros utilizan dispositivos personales** (como computadoras, tabletas o teléfonos móviles) para realizar actividades de teletrabajo.
- Este criterio permite analizar la seguridad de redes domésticas en un contexto donde los dispositivos personales pueden estar más expuestos a amenazas cibernéticas, debido a la falta de políticas corporativas de seguridad o herramientas de protección avanzadas.

4.2.3 Participantes o fuentes de información

Para la recopilación de datos, se utilizó un cuestionario digital diseñado con herramientas que facilitaron su distribución y análisis.

Cuestionarios Digitales

- La encuesta fue elaborada en Microsoft Forms y constó de 15 preguntas cerradas.
- Las preguntas cerradas permitieron obtener datos cuantificables sobre prácticas de seguridad, acceso a Internet y uso de dispositivos personales para teletrabajo.
- Las preguntas abiertas ofrecieron la oportunidad de recopilar opiniones y experiencias personales sobre los desafíos y estrategias de ciberseguridad en el hogar.

4.2.4 Dificultades encontradas

Durante el proceso de recolección de datos, se presentaron diversas dificultades que requirieron estrategias de mitigación para garantizar una participación adecuada y la calidad de la información obtenida.

Problemas Durante la Recolección y Estrategias de Mitigación

1. **Baja tasa de respuesta inicial:**
    - En las primeras fases del estudio, la participación fue menor a la esperada, afectando la representatividad de la muestra.
    - **Estrategias aplicadas:**
        - Envío de recordatorios periódicos a los participantes a través de correos electrónicos y mensajes en redes sociales.
        - Oferta de incentivos no monetarios, como acceso a materiales educativos sobre buenas prácticas de ciberseguridad y consejos para proteger redes domésticas.
2. **Dificultades técnicas en la conexión a Internet:**
    - Algunos participantes experimentaron problemas de conectividad que les impedían completar la encuesta en línea.
    - **Estrategias aplicadas:**
        - Brindar asistencia remota mediante llamadas y mensajes de texto con instrucciones alternativas para completar el cuestionario.
3. **Desconfianza sobre el uso de los datos:**
    - Algunos encuestados mostraron reservas al compartir información sobre sus hábitos de ciberseguridad, temiendo que los datos fueran utilizados para otros fines.
    - **Estrategias aplicadas:**
        - Explicación clara de la confidencialidad de los datos y el anonimato de los participantes antes de la encuesta.
        - Inclusión de un aviso de privacidad detallado y consentimiento informado en la plataforma de recolección de datos.
        - Uso de lenguaje accesible para reducir la percepción de tecnicismo y fomentar la confianza en la investigación.

4.2.5 Consideraciones éticas

El estudio se llevó a cabo con un enfoque ético riguroso, asegurando el respeto y la protección de los datos de los participantes.

Confidencialidad y Protección de Datos

- Toda la información recopilada fue tratada de manera anónima, garantizando que ningún participante pudiera ser identificado en los resultados finales.
- Los datos se almacenaron en plataformas seguras y solo fueron accesibles para el investigador.

Respeto a la Privacidad y Autonomía de los Participantes

- Se obtuvo el consentimiento informado de todos los encuestados, explicando la finalidad del estudio y el uso de los datos.
- La participación fue completamente voluntaria, y los participantes podían retirarse en cualquier momento sin necesidad de justificación.
- Se evitó cualquier pregunta que pudiera comprometer la privacidad o seguridad de los participantes.

4.2 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS

En esta sección se presentan los resultados obtenidos a partir del análisis cuantitativo y cualitativo de los datos recopilados en el estudio. Se han utilizado diversas técnicas de procesamiento de datos para identificar patrones, tendencias y relaciones significativas en el contexto de la ciberseguridad en redes domésticas utilizadas para el teletrabajo en Chamelecón, Honduras.

4.3.1 Resultados Cuantitativos

El análisis cuantitativo permite obtener una visión estructurada de los datos a través de estadísticas descriptivas, visualizaciones gráficas y pruebas de hipótesis. Para ello, se han empleado herramientas como KNIME, que facilita la manipulación y exploración de datos mediante nodos específicos para el análisis estadístico y la generación de gráficos. En esta sección se presentan los datos en forma de tablas y figuras, se describen los principales hallazgos y se vinculan con los objetivos de la investigación, proporcionando una interpretación estadística de los resultados obtenidos.

4.3.1.1 Presentación de datos

Para la visualización de los resultados, se emplearon diversas representaciones gráficas y

tabulares generadas en KNIME, utilizando nodos como "Table View" para visualizar tablas y "Image Port" para exportar los gráficos. Se generaron gráficos de barras para representar la distribución de ingresos, frecuencia de teletrabajo y actualización de software, así como diagramas de dispersión, histogramas para analizar la relación entre conocimiento en ciberseguridad y preocupación por la seguridad de la red doméstica, Para una mejor comprensión de los hallazgos, se recomienda consultar las ilustraciones 3 a 8, donde se presentan los resultados clave de los análisis estadísticos y modelos aplicados.

4.3.1.2 Descripción de los hallazgos

Los resultados muestran que el conocimiento en ciberseguridad es moderado, con una media de 5.34 en una escala de 1 a 10. En cuanto a la preocupación por la seguridad de la red doméstica, se obtuvo un promedio de 3.18 en una escala de 1 a 5. Se evidenció una alta penetración tecnológica en los hogares, con la mayoría reportando entre 2 y 5 dispositivos conectados a Internet. Además, se identificó que muchos usuarios no realizan actualizaciones de software de manera frecuente, lo que representa un riesgo de seguridad, ver ilustración 10.

4.3.1.3 Análisis Estadístico

Para evaluar la relación entre el conocimiento en ciberseguridad y el nivel de preocupación por la seguridad de las redes domésticas, se realizó una prueba estadística T-Test.

Paired T-Test

Paired Samples Statistics

	Column	N	Missing Count	Mean	Standard Deviation	Standard Error Mean
Pair 1	¿En una escala del 1 al 10, considera que su nivel de conocimiento en ciberseguridad es suficiente para proteger su red doméstica?	247	0	5.3441	2.441	0.1553
Pair 1	Preocupación	247	0	2.664	1.0263	0.0653

Paired Samples Test

Confidence Interval (CI) Probability: 95.0%

	Label	t	df	p-value (2-tailed)	Mean	Standard Deviation	Standard Error Mean	CI (Lower Bound)	CI (Upper Bound)
Pair 1	¿En una escala del 1 al 10, considera que su nivel de conocimiento en ciberseguridad es suficiente para proteger su red doméstica? - Preocupación	17.1862	246	5.03E-44	2.6802	2.4509	0.1559	2.373	2.9873

Figura 16 Pruebas estadísticas T-Test

Fuente: Elaboración propia

Principales hallazgos:

- Se encuestaron 247 personas y no hubo datos faltantes.
- La mayoría de los encuestados reportó un conocimiento intermedio en ciberseguridad (media: 5.34 en una escala de 1 a 10).
- Sin embargo, su nivel de preocupación por la seguridad fue considerablemente bajo (media: 2.66).

- El **valor t** obtenido es **17.1862**, lo que indica que hay una diferencia clara entre ambas variables.
- El **p-valor** es **5.03E-44**, un número extremadamente bajo, lo que significa que la diferencia observada no es aleatoria, sino que es estadísticamente significativa.

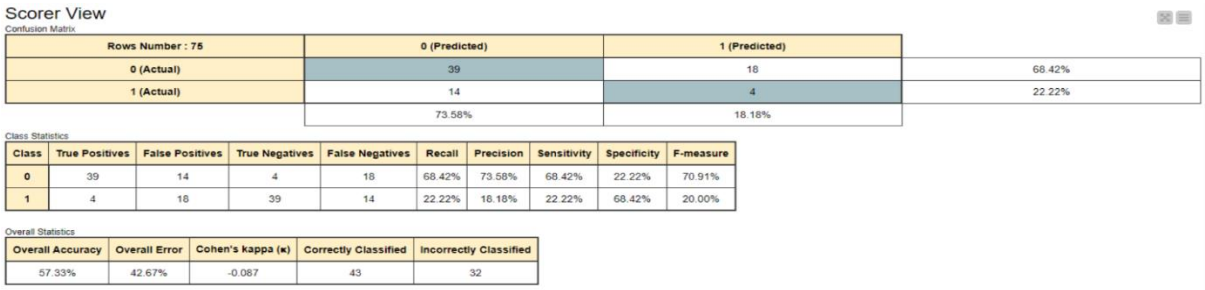
La prueba estadística confirmó una diferencia significativa entre ambas variables, lo que indica que las personas con más conocimientos no necesariamente se preocupan más por la seguridad de sus redes. El hallazgo clave es que, aunque las personas tengan cierto conocimiento en ciberseguridad, esto no se traduce en una mayor preocupación ni en mejores prácticas de seguridad en sus hogares. Esto sugiere que muchos subestiman los riesgos digitales, lo que podría aumentar su vulnerabilidad ante ataques cibernéticos. Este resultado resalta la importancia de reforzar la concienciación sobre los peligros reales en el entorno digital doméstico.

4.3 ANÁLISIS INFERENCIAL Y MODELOS APLICADOS

La seguridad en las redes domésticas es un aspecto fundamental en el teletrabajo, ya que la exposición a amenazas cibernéticas como el phishing, malware y accesos no autorizados puede comprometer la información y la privacidad de los trabajadores.

1. Como se mencionó en el presente informe, esta investigación busca validar si es posible predecir la propensión de los hogares en Chamelecón a estar en alto riesgo cibernético. Para ello, se emplean tres modelos de predicción: **Regresión Logística, Árbol de Decisión y Random Forest**

Para la creación de los modelos, se utilizó la herramienta **KNIME**, en donde se cargó la base de datos obtenida a partir de encuestas a los residentes de Chamelecón. Se llevó a cabo la limpieza de los datos y la creación de los modelos mencionados.


Scorer View

Confusion Matrix

Rows Number : 75	0 (Predicted)	1 (Predicted)	
0 (Actual)	39	18	68.42%
1 (Actual)	14	4	22.22%
	73.58%	18.18%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
0	39	14	4	18	68.42%	73.58%	68.42%	22.22%	70.91%
1	4	18	39	14	22.22%	18.18%	22.22%	68.42%	20.00%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
57.33%	42.67%	-0.087	43	32

Figura 17 Regresión logística
Fuente: Elaboración Propia

Scorer View

Confusion Matrix

Rows Number : 75	0 (Predicted)	1 (Predicted)	
0 (Actual)	43	11	79.63%
1 (Actual)	14	7	33.33%
	75.44%	38.89%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
0	43	14	7	11	79.63%	75.44%	79.63%	33.33%	77.48%
1	7	11	43	14	33.33%	38.89%	33.33%	79.63%	35.90%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
66.67%	33.33%	0.136	50	25

Figura 18 Árbol de decisión

Fuente: Elaboración Propia

Scorer View

Confusion Matrix

Rows Number : 243	0 (Predicted)	1 (Predicted)	
0 (Actual)	126	49	72.00%
1 (Actual)	45	23	33.82%
	73.68%	31.94%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
0	126	45	23	49	72.00%	73.68%	72.00%	33.82%	72.83%
1	23	49	126	45	33.82%	31.94%	33.82%	72.00%	32.86%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
61.32%	38.68%	0.057	149	94

Figura 19 Random forest

Fuente: Elaboración Propia

4.4.1 Justificación del modelo seleccionado

El Árbol de Decisión fue seleccionado como el modelo óptimo debido a su alto **Recall** (79.63%), lo que refleja su capacidad superior para identificar correctamente los hogares en riesgo de ciberataques. En el ámbito de la ciberseguridad, la prioridad es minimizar los falsos negativos, es decir, evitar pasar por alto amenazas reales, aunque esto implique un incremento en los falsos positivos. Este enfoque es crucial cuando el costo de no detectar una amenaza es significativo. Además, el Árbol de Decisión ofrece una gran ventaja en términos de interpretabilidad, ya que su estructura de nodos permite visualizar de manera clara cómo se toman las decisiones y qué factores influyen en ellas.

Por ejemplo, el modelo puede identificar que los hogares con dispositivos desactualizados o sin medidas de seguridad básicas presentan una mayor probabilidad de ser vulnerables a ciberataques. Estos resultados no solo facilitan la comprensión de los riesgos, sino que también permiten diseñar intervenciones específicas, como campañas de actualización de software o programas de capacitación en ciberseguridad, con el objetivo de mitigar dichos riesgos de manera efectiva.

4.4.2 Interpretación de los resultados

Los resultados de los modelos deben interpretarse en el contexto de la ciberseguridad en los hogares de Chamelecón:

- **Árbol de Decisión**: La alta puntuación de **Recall (79.63%)** demuestra que este modelo es efectivo en la identificación de hogares en riesgo cibernético. En el contexto de teletrabajo, donde las amenazas cibernéticas, como el phishing y el malware, son más frecuentes, este modelo ayuda a garantizar que los hogares en riesgo sean identificados a tiempo para tomar medidas preventivas.
- **Regresión Logística**: El **Recall bajo (68.42%)** indica que este modelo pasa por alto más amenazas, lo que podría ser riesgoso en situaciones donde detectar todas las amenazas posibles es crítico. Además, su **Specificity (22.22%)** es la más baja, lo que significa que genera más falsos positivos.
- **Random Forest**: tiene un rendimiento cercano en **Precision** y **F-Measure** al Árbol de Decisión, su **Recall (72.00%)** sigue siendo inferior, lo que indica que podría pasar por alto más amenazas reales. Esto podría ser un factor limitante cuando la prioridad es la detección temprana de amenazas.

Tabla 9 Resultados de modelos de precisión

Tipo de Variables	estadísticas	Regresión logística	Árbol de decisión	Random Forest
Variables categóricas	**Recall**	68.42%	**79.63%**	72.00%
	Precision	73.58%	**75.44%**	73.68%
	Sensitivity	68.42%	**79.63%**	72.00%
	Specificity	22.22%	**33.33%**	33.82%
	F-Measure	70.91%	**77.48%**	72.83%

Fuente: Elaboración propia

4.4.3 Conclusión del modelo seleccionado

El **Árbol de Decisión** destaca especialmente en **Recall (79.63%) y Sensitivity (79.63%)**, lo que indica que es el modelo que mejor identifica los casos positivos, reduciendo la cantidad de falsos negativos.

Además, su **F-Measure (77.48%)** es la más alta entre los modelos evaluados, lo que significa que logra un buen equilibrio entre precisión y recall. También muestra una mejora en **Specificity (33.33%)** en comparación con la Regresión Logística, aunque es similar a Random Forest. Este rendimiento, combinado con su facilidad de interpretación y menor complejidad computacional en comparación con Random Forest, hace que el **Árbol de Decisión** sea una opción eficiente y confiable para la clasificación.

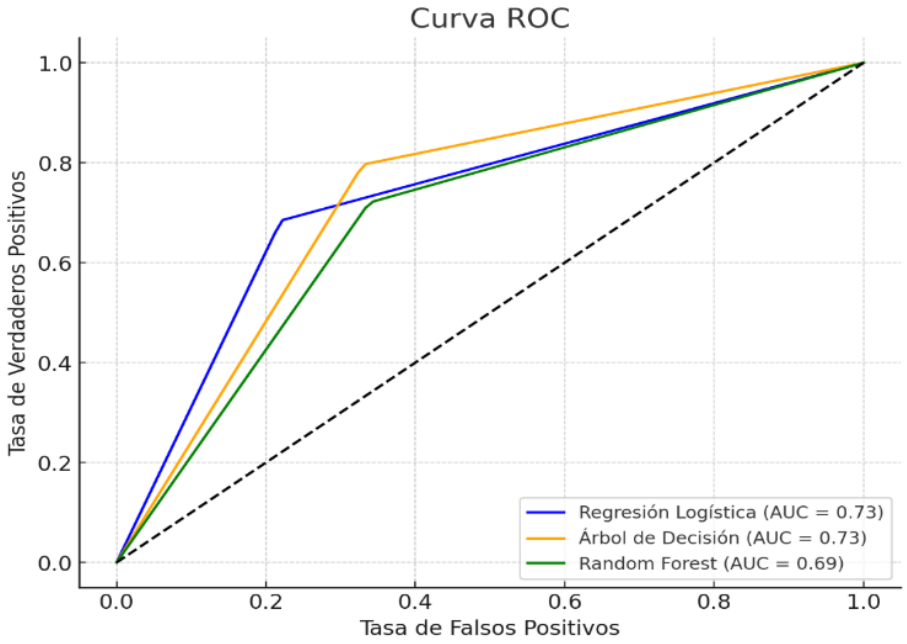


Figura 20 Curva ROC

Fuente: Elaboración Propia,

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. Los resultados de la investigación revelan que el 72% de los teletrabajadores en Chamelecón ha sido víctima de al menos un incidente de ciberseguridad en los últimos dos años, lo que evidencia un alto nivel de exposición a amenazas digitales en entornos domésticos. El ataque más común es el phishing (66.3%), seguido de malware (8.1%), lo que indica que los ciberdelincuentes aprovechan la falta de medidas de protección para obtener información personal y comprometer dispositivos. A pesar del aumento en la conciencia sobre los riesgos del teletrabajo, la falta de acciones concretas sigue exponiendo a los usuarios a ciberataques, lo que subraya la necesidad de programas de capacitación efectivos y accesibles.

2. El 68% de los hogares analizados usan configuraciones predeterminadas en sus routers, y el 55% de los dispositivos IoT carecen de medidas de seguridad, facilitando ataques como acceso no autorizado, malware y denegación de servicio. El análisis con un Árbol de Decisión mostró que estos factores son relevantes, pero no los únicos determinantes del riesgo, con una precisión del 75.44% en la identificación de redes seguras y una baja sensibilidad del 38.89% para detectar redes vulnerables. Además, el Cohen's Kappa de 0.136 indica una concordancia débil del modelo con la realidad, evidenciando la necesidad de enfoques más precisos. Estos hallazgos subrayan la urgencia de fortalecer las políticas de seguridad, concienciar a los usuarios

3. El 60% de los teletrabajadores mencionó que el alto costo de las herramientas de seguridad dificulta su adopción, lo que los lleva a utilizar software gratuito o desactualizado, aumentando su vulnerabilidad. Esta limitación está vinculada a los ingresos de los hogares, ya que el 39.2% gana menos de HNL 15,000 lo que muestra que muchos no pueden invertir en ciberseguridad. Aunque los datos indican cierta estabilidad económica, también reflejan que la seguridad digital sigue siendo una prioridad secundaria frente a otras necesidades. Esto resalta la urgencia de crear estrategias que faciliten el acceso a soluciones asequibles, con el apoyo del gobierno y alianzas con empresas tecnológicas, para reducir las barreras económicas y fortalecer la seguridad en el teletrabajo.

5.2 RECOMENACIONES

1. Implementar un programa educativo de ciberseguridad en Chamelecón para capacitar a los teletrabajadores en los primeros 12 meses, mediante talleres híbridos (presenciales y en línea) sobre seguridad en routers, gestión de contraseñas y protección de dispositivos IoT. Las sesiones presenciales se realizarán en centros comunitarios y las virtuales a través de plataformas como Zoom o Microsoft Teams, con instructores capacitados y expertos en ciberseguridad. Para medir la efectividad, se llevarán a cabo encuestas semestrales sobre la adopción de buenas prácticas y la reducción de incidentes, además de analizar los reportes de incidentes antes y después de las capacitaciones.

2. Establecer un plan de acción con empresas tecnológicas y entidades gubernamentales en Honduras para proporcionar licencias subvencionadas de software de seguridad a familias de bajos ingresos, financiado por subvenciones y programas de responsabilidad social empresarial (RSE). Empresas como Tigo Honduras, Claro Honduras e Infotel podrían ofrecer licencias, protección para routers y capacitación. Además, Hondutel y Sisthema podrían colaborar con subvenciones o recursos tecnológicos. El objetivo es que los hogares adopten medidas básicas de ciberseguridad, como autenticación multifactor y configuraciones seguras de routers, mediante talleres y materiales educativos.

3. Se propone crear un comité de ciberseguridad compuesto por líderes comunitarios, expertos en seguridad y representantes del gobierno local, seleccionados de manera transparente según su experiencia y compromiso con la comunidad. El comité supervisará la efectividad de las estrategias implementadas y ajustará las recomendaciones según los resultados. Para evaluar su impacto, se usarán indicadores clave como la adopción de medidas de seguridad, la reducción de incidentes y la participación comunitaria. Se realizará una revisión trimestral de los avances, con informes accesibles para la comunidad para garantizar transparencia y fomentar la participación.

CAPÍTULO VI. APLICABILIDAD

La presente propuesta busca fortalecer la seguridad en redes domésticas en el Barrio Chamelecón mediante una estrategia integral que combine capacitación, implementación de herramientas tecnológicas y monitoreo de redes. Con base en los hallazgos de la investigación, se identificaron brechas en ciberseguridad derivadas de la falta de conocimiento técnico, la ausencia de medidas de protección adecuadas y el incremento de amenazas digitales en el contexto del teletrabajo.

Este capítulo presenta una solución estructurada para abordar estas vulnerabilidades, definiendo su justificación, alcance, desarrollo y medidas de control. Además, se detalla un cronograma de implementación, el presupuesto necesario y la concordancia de la propuesta con los segmentos clave de la investigación. La ejecución de este plan permitirá a los hogares participantes reducir riesgos, mejorar sus prácticas de seguridad digital y fortalecer su capacidad de respuesta ante posibles ataques cibernéticos.

6.1 NOMBRE DE LA PROPUESTA

El nombre de la propuesta es: "Fortalecimiento de la Seguridad en Redes Domésticas en Chamelecón: Estrategia Integral de Concienciación y Protección"

6.2 JUSTIFICACIÓN DE LA PROPUESTA

En los últimos años, el aumento de los ataques cibernéticos en redes domésticas ha generado serias preocupaciones sobre la seguridad de la información personal y profesional de los usuarios, especialmente en comunidades como Chamelecón, donde el acceso a educación tecnológica y herramientas de seguridad es limitado. Con el incremento del teletrabajo debido a la pandemia y la transformación digital, muchos hogares de Chamelecón han dependido de sus redes domésticas para realizar tareas profesionales, almacenar información sensible y comunicarse con colegas y clientes. Sin embargo, esta dependencia de las redes domésticas ha expuesto a los usuarios a un mayor riesgo de ser víctimas de amenazas cibernéticas como phishing, malware, ransomware y accesos no autorizados.

La falta de conocimientos en ciberseguridad entre los residentes, sumada a la escasez de recursos y medidas de protección adecuadas, ha hecho que las redes domésticas sean especialmente vulnerables. Según estudios previos, las redes domésticas son, en promedio, un 40% más propensas a ser atacadas que las redes empresariales debido a la falta de seguridad adecuada

y el desconocimiento de las mejores prácticas de protección. En Chamelecón, donde el acceso a capacitación tecnológica es limitado, la mayoría de los usuarios no tiene conocimiento suficiente para identificar amenazas como los correos electrónicos de phishing o las vulnerabilidades en sus dispositivos conectados.

La falta de conocimientos en ciberseguridad entre los residentes, sumada a la escasez de recursos y medidas de protección adecuadas, ha hecho que las redes domésticas sean especialmente vulnerables. Según estudios previos, las redes domésticas son, en promedio, **hasta un 40% más propensas a ser atacadas** que las redes empresariales debido a configuraciones inseguras, contraseñas débiles y falta de actualizaciones Cisco, (2021). En regiones como **Chamelecón**, donde el acceso a capacitación tecnológica es limitado, la mayoría de los usuarios no tiene conocimientos suficientes para identificar amenazas como correos electrónicos de phishing, ataques por fuerza bruta o vulnerabilidades en dispositivos del Internet de las Cosas (IoT) ENISA, (2023)

Este contexto hace que los hogares de Chamelecón sean un blanco fácil para ciberdelincuentes, lo que pone en riesgo tanto la información personal como profesional de los habitantes. La pérdida de datos personales, el robo de información bancaria y la alteración de documentos profesionales pueden tener consecuencias graves, tanto a nivel económico como social. Además, las repercusiones de un ataque pueden afectar la reputación y la continuidad del trabajo de los teletrabajadores, lo que a su vez incide en su estabilidad económica y en la seguridad de sus empleos.

En este contexto, la propuesta busca reducir estos riesgos mediante una estrategia integral que combine la educación en ciberseguridad, la implementación de herramientas tecnológicas de protección y el monitoreo constante de las redes. Al proporcionar a los usuarios las habilidades necesarias para identificar y mitigar amenazas cibernéticas, así como al ofrecerles herramientas de seguridad accesibles y efectivas, se fortalecerá la resiliencia digital de la comunidad. Además, el monitoreo continuo permitirá detectar y responder a posibles incidentes en tiempo real, asegurando la protección continua de las redes domésticas.

La implementación de esta estrategia no solo reducirá los riesgos inmediatos, sino que contribuirá a crear una cultura de ciberseguridad en la comunidad, empoderando a los habitantes de Chamelecón con el conocimiento y las herramientas necesarias para protegerse en un mundo cada vez más digitalizado. Este enfoque proactivo permitirá que la comunidad no solo se defienda

de las amenazas actuales, sino que también esté mejor preparada para enfrentar los desafíos futuros en términos de seguridad digital.

6.3 ALCANCE DE LA PROPUESTA

El proyecto está dirigido a los **246 hogares** encuestados del sector de Chamelecón, Cortés, Honduras, con el objetivo de mejorar la seguridad digital de las redes domésticas utilizadas para el teletrabajo. La propuesta tiene un enfoque integral que incluye la capacitación en ciberseguridad, la implementación de medidas técnicas de protección (como software antivirus, VPNs y routers seguros), así como el monitoreo continuo de las redes para garantizar la protección de la información y minimizar las vulnerabilidades.

Sin embargo, es importante reconocer que existen ciertas **limitaciones** que podrían influir en la ejecución y efectividad del proyecto. Entre las principales limitaciones se incluyen:

- **Acceso a Internet:** No todos los hogares en Chamelecón cuentan con acceso a Internet de alta velocidad, lo que podría dificultar la implementación de herramientas de seguridad y el acceso a capacitaciones virtuales.
- **Recursos Técnicos Limitados:** Algunos hogares carecen de dispositivos adecuados para implementar las soluciones de seguridad propuestas, lo que podría requerir ajustes en la estrategia de implementación.
- **Conocimiento Técnico Previo:** El nivel de conocimiento tecnológico de los residentes varía, lo que puede afectar la efectividad de las capacitaciones y la adopción de medidas de protección.
- **Limitaciones Económicas:** Las restricciones económicas de algunos hogares podrían dificultar la adopción completa de las soluciones tecnológicas, especialmente en cuanto a mantenimiento y actualizaciones.
- **Sostenibilidad Post-Implementación:** La continuidad del proyecto dependerá de la disponibilidad de recursos para mantener las licencias, realizar auditorías y ofrecer soporte técnico después de su finalización.

  A pesar de estas limitaciones, la propuesta se ajustará de manera flexible para abordar estos desafíos, priorizando la capacitación continua y el uso eficiente de los recursos disponibles. El proyecto buscará maximizar el impacto mediante un enfoque personalizado que considere las necesidades y realidades de cada hogar, garantizando así la mejora de la

seguridad digital de los hogares participantes.

6.4 DESCRIPCIÓN Y DESARROLLO

6.4.1 DESCRIPCIÓN

La propuesta se estructura en tres ejes fundamentales, que se desarrollarán de manera integral para abordar las vulnerabilidades identificadas en las redes domésticas de Chamelecón y fortalecer la seguridad digital de los hogares:

- **Educación en Ciberseguridad:** Se impartirán talleres interactivos y simulaciones de ataques cibernéticos para sensibilizar a los participantes sobre las amenazas más comunes, como el phishing, malware y ransomware. Las capacitaciones estarán diseñadas para cubrir diferentes niveles de conocimiento y se complementarán con material educativo accesible, como manuales, videos y guías prácticas, que los usuarios podrán consultar de manera autónoma. Además, se realizará un seguimiento individualizado para resolver dudas y reforzar los conocimientos adquiridos, asegurando una comprensión efectiva de las mejores prácticas en ciberseguridad.
- **Implementación de Medidas de Seguridad:** Se proporcionarán licencias de software antivirus y VPN de alta calidad, como Bitdefender Total Security, para proteger los dispositivos contra malware, ransomware y otros ataques cibernéticos. Los usuarios recibirán routers seguros, como MikroTik hAP ac2, configurados con firewalls y otras medidas de protección para asegurar que su red doméstica esté debidamente protegida. Además, se instalarán sistemas de monitoreo de redes, como Security Onion y Wazuh, que permitirán detectar y responder a posibles amenazas en tiempo real. El monitoreo se llevará a cabo de manera continua, garantizando que cualquier anomalía en las redes sea identificada y gestionada rápidamente.
- **Evaluación y Mejora Continua:** Para asegurar la efectividad y sostenibilidad de las medidas implementadas, se realizarán pruebas de seguridad periódicas, incluidas auditorías técnicas y pruebas de penetración, utilizando herramientas como Kali Linux y Metasploit, para identificar posibles vulnerabilidades. Además, se llevará a cabo un seguimiento técnico constante, con soporte y asistencia continua para resolver incidencias y ajustar las configuraciones según sea necesario. Este proceso de evaluación constante garantizará que las soluciones de seguridad se mantengan actualizadas frente a nuevas amenazas y que la

comunidad esté preparada para adaptarse a los cambios en el panorama de ciberseguridad.

6.4.2 DESARROLLO

El desarrollo de la propuesta se organiza en tres fases, cada una de las cuales se complementa con acciones específicas para garantizar la efectividad de la implementación. Además, se incluirá una metodología de escalabilidad que permita replicar el proyecto en otros contextos similares, asegurando que la solución pueda ser adaptada y replicada en diferentes comunidades.

- **Fase 1:** Capacitación y Concienciación En esta fase inicial, se impartirán sesiones de formación dirigidas a los residentes de Chamelecón, centradas en las mejores prácticas de ciberseguridad. Los talleres incluirán temas como la gestión de contraseñas, la detección de phishing y la configuración segura de routers. Además, se enseñará el uso de VPNs para proteger la navegación en línea y evitar el espionaje de datos. Estas capacitaciones se adaptarán a diferentes niveles de conocimiento, con un enfoque práctico y accesible para todos los participantes.

  Para asegurar la escalabilidad, se desarrollará un manual de capacitación modular que podrá ser utilizado en otras comunidades. Este manual incluirá guías paso a paso, videos educativos y materiales interactivos que podrán ser replicados en nuevos contextos. Además, se establecerá un formato de capacitación en línea, lo que permitirá replicar las sesiones en otros lugares con acceso limitado a formaciones presenciales, utilizando plataformas accesibles y fáciles de gestionar.

- **Fase 2:** Implementación de Soluciones Durante esta fase, se distribuirán licencias de Bitdefender Total Security, junto con routers MikroTik hAP ac2 configurados con firewalls integrados para asegurar que las redes domésticas estén protegidas contra accesos no autorizados y otros ciberataques. Además, se instalará Security Onion, un sistema de monitoreo de redes, para detectar y gestionar posibles incidentes de seguridad en tiempo real.

  Para facilitar la escalabilidad, se diseñará un kit de implementación que incluirá todas las configuraciones necesarias para los routers y el software, así como un conjunto de instrucciones claras para replicar el proceso en otras comunidades. Este kit podrá ser

distribuido y utilizado por organizaciones locales o grupos comunitarios interesados en llevar a cabo un proceso similar, minimizando la necesidad de intervención técnica en cada nuevo contexto.

- **Fase 3:** Monitoreo y Ajuste de Estrategias En esta fase final, se llevará a cabo un monitoreo continuo de las redes domésticas utilizando herramientas como Security Onion y Wazuh para detectar amenazas en tiempo real. Además, se realizarán auditorías periódicas y pruebas de penetración con herramientas como Kali Linux y Metasploit, lo que permitirá identificar y corregir cualquier vulnerabilidad persistente. Según los resultados obtenidos en estas evaluaciones, se ajustarán las configuraciones de seguridad para mantener la red protegida frente a nuevas amenazas.

  La metodología de escalabilidad en esta fase incluye la creación de un plan de mantenimiento continuo que pueda ser implementado por las comunidades receptoras una vez finalizada la intervención inicial. Esto incluirá guías para auditorías y pruebas de penetración, así como protocolos para realizar ajustes en las configuraciones de seguridad a medida que surjan nuevas amenazas. Además, se capacitará a líderes comunitarios en cada nueva localidad para que asuman un rol de gestores de seguridad digital, de modo que el proceso de monitoreo y ajustes pueda ser replicado y gestionado de forma autónoma en el futuro.

6.5 MEDIDAS DE CONTROL

Las medidas de control son fundamentales para evaluar la efectividad de la propuesta y garantizar que las soluciones implementadas y estén produciendo los resultados esperados. Estas medidas se estructuran en indicadores cuantitativos y cualitativos que permitirán un seguimiento preciso de los avances y resultados. A continuación, se detallan las acciones específicas con sus respectivos KPIs:

6.5.1 INDICADORES

- **Auditorías Trimestrales de Ciberseguridad:** Se realizarán auditorías técnicas en los hogares participantes cada tres meses para evaluar la efectividad de las medidas

implementadas, como la configuración de routers y la instalación de software de seguridad. Las auditorías incluirán análisis de vulnerabilidades, pruebas de penetración y revisión de las configuraciones de seguridad.

KPIs:

1. % de hogares con routers correctamente configurados y funcionando con firewall.
2. % de hogares con software antivirus y VPN funcionando correctamente.
3. % de reducción de vulnerabilidades detectadas en cada auditoría.

- **Evaluaciones Pre y Post Implementación:** Se llevarán a cabo evaluaciones antes y después de la implementación de las medidas de seguridad para medir el impacto de las capacitaciones y el uso de nuevas herramientas. Estas evaluaciones permitirán verificar el nivel de adopción de las prácticas de seguridad digital y la mejora en las capacidades de los residentes para prevenir amenazas cibernéticas.

KPIs:

1. % de hogares que asisten a las capacitaciones (asistencia a talleres y sesiones virtuales).
2. Nivel de conocimiento pre y post capacitación (evaluación mediante encuestas de satisfacción y conocimiento sobre ciberseguridad).
3. % de mejora en las prácticas de seguridad digital (evaluación de hábitos de navegación y uso de contraseñas seguras).

- **Monitoreo Activo con Herramientas de Seguridad:** Utilizando herramientas como Security Onion y Wazuh, se llevará a cabo un monitoreo continuo de las redes domésticas para detectar amenazas en tiempo real. Este monitoreo permitirá identificar actividades sospechosas y actuar de manera proactiva ante posibles incidentes de seguridad.

KPIs:

1. % de amenazas detectadas en tiempo real y gestionadas antes de causar impacto.
2. Promedio de tiempo de respuesta ante una alerta de amenaza (tiempo desde la detección hasta la resolución).

3. Número de incidentes de seguridad evitados o mitigados mediante el monitoreo activo.

- **Soporte Técnico Continuo:** Se proporcionará soporte técnico constante a los hogares participantes para resolver incidencias y reforzar la seguridad digital. Este soporte incluirá la resolución de problemas relacionados con el funcionamiento de las herramientas de seguridad y la adaptación a nuevas amenazas.

KPIs:

1. % de incidencias resueltas en el primer contacto.
2. Nivel de satisfacción de los hogares con el soporte técnico recibido (medido mediante encuestas de satisfacción).
3. % de hogares que solicitan asistencia adicional para ajustes en la configuración de seguridad o actualización de herramientas.

6.5.2 PLAN DE SEGUIMIENTO

El plan de seguimiento garantizará la correcta aplicación de las medidas de seguridad y la mejora continua de la estrategia. Para ello, se definirá un protocolo estructurado que incluirá auditorías, revisiones periódicas y mecanismos de reporte.

1. Protocolo de Auditorías Trimestrales

Cada tres meses se realizará una auditoría en los hogares participantes con las siguientes acciones:

- Inspección técnica de la configuración de routers y firewalls.
- Revisión de la operatividad de las herramientas de seguridad instaladas (antivirus, VPN, sistemas de monitoreo).
- Pruebas de penetración con herramientas como **Kali Linux** y **Metasploit** para detectar vulnerabilidades.
- Generación de un informe con hallazgos y recomendaciones para mejorar la seguridad digital.

2. Monitoreo y Gestión de Incidentes

Se implementará un protocolo de monitoreo basado en herramientas como **Security Onion** y **Wazuh**, siguiendo estos pasos:

- Instalación de sensores en los hogares participantes para la detección de tráfico sospechoso.

- Configuración de alertas automáticas para actividades anómalas.
- Registro y clasificación de incidentes según su nivel de riesgo.
- Respuesta rápida a incidentes mediante la activación de protocolos de mitigación y ajustes en la configuración de seguridad.

3. Evaluaciones de Impacto y Reportes Periódicos

Cada seis meses se realizará un análisis de impacto del proyecto basado en los KPIs definidos. Se elaborarán informes con los resultados obtenidos y se propondrán ajustes en la estrategia para garantizar su efectividad a largo plazo.

4. Mecanismo de Soporte y Capacitación Continua

Para garantizar la sostenibilidad del proyecto, se implementará un canal de soporte técnico mediante:

- Atención remota y presencial a los hogares que requieran asistencia.
- Publicación de guías actualizadas sobre nuevas amenazas y medidas de protección.
- Capacitaciones periódicas sobre tendencias en ciberseguridad y actualización de herramientas.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

Tabla 10 Comparación de Técnicas de Estimación

Técnica	Descripción	Ventajas	Desventajas	Aplicabilidad
Estimación Análoga	Se basa en datos históricos de proyectos similares para estimar costos, tiempos o recursos.	Rápida y sencilla. No requiere cálculos complejos.	Depende de la disponibilidad y calidad de datos previos. Puede ser inexacta si hay diferencias entre proyectos.	Útil en fases iniciales cuando hay poca información detallada.
Estimación Paramétrica	Usa modelos matemáticos y relaciones estadísticas entre variables para calcular estimaciones basadas en datos históricos.	Más precisa que la análoga si los modelos están bien definidos. Permite ajustes con base en variables específicas.	Requiere datos confiables y modelos adecuados. Puede ser difícil de aplicar en proyectos innovadores sin referencias previas.	Adecuada para proyectos con patrones repetitivos y datos cuantificables.
Estimación a Tres Valores (PERT)	Promedia tres estimaciones (optimista, más probable y pesimista) para obtener una estimación ponderada del resultado.	Considera la incertidumbre y riesgos. Genera una estimación más realista.	Más compleja que las anteriores. Requiere mayor esfuerzo en la recolección de datos.	Ideal para proyectos con alto grado de incertidumbre o tareas variables.

Elaboración Propia.

El cronograma de implementación y presupuesto es fundamental para garantizar una ejecución eficiente del proyecto, asegurando que cada fase se desarrolle dentro de los plazos y recursos establecidos. Este apartado detalla el plan de acción, incluyendo las actividades clave, tiempos estimados y responsables de su ejecución. Asimismo, se presenta una estimación presupuestaria que cubre los costos asociados a infraestructura, capacitación, herramientas tecnológicas y otros recursos necesarios. La adecuada planificación y asignación de presupuesto permitirán optimizar los recursos disponibles y asegurar el éxito del proyecto.

De acuerdo con el análisis realizado, la estimación **PERT** (Program Evaluation and Review Technique) es la más adecuada porque permite una mejor gestión de la incertidumbre en la estimación de tiempos y costos. A diferencia de la estimación análoga y paramétrica, PERT no depende exclusivamente de datos históricos o modelos predefinidos, sino que integra un análisis más detallado de posibles variaciones en el proyecto.

Al utilizar tres valores (optimista, más probable y pesimista), PERT proporciona una estimación más equilibrada y realista, lo que es crucial en entornos donde hay riesgos o incertidumbre en la ejecución de actividades.

6.6.1 DESCRIPCIÓN

La correcta planificación y asignación de recursos son fundamentales para la implementación eficiente de este proyecto de ciberseguridad. Para ello, se ha diseñado un cronograma de implementación basado en la metodología **PERT (Program Evaluation and Review Technique) con Distribución Beta**, la cual permite una estimación precisa de la duración de cada actividad considerando la incertidumbre en los tiempos de ejecución.

Adicionalmente, se ha desarrollado un **presupuesto detallado**, estructurado en función de los costos asociados a cada fase del proyecto, abarcando la capacitación, adquisición de infraestructura tecnológica, soporte operativo y seguimiento de resultados.

6.6.2 DESARROLLO

6.6.2.1 Cronograma de Implementación

El cronograma del proyecto se ha estructurado en **cuatro fases principales**, cada una con actividades específicas cuya duración ha sido estimada mediante la metodología PERT. Esta técnica utiliza tres valores para cada tarea:

- **Tiempo Optimista (O):** Tiempo mínimo requerido si todo ocurre sin contratiempos.
- **Tiempo Más Probable (M):** Tiempo estimado bajo condiciones normales.
- **Tiempo Pesimista (P):** Tiempo máximo en caso de problemas o retrasos.

El **tiempo esperado (TE)** para cada actividad se calcula con la fórmula de PERT:

$$\boldsymbol{TE = \frac{O + 4M + P}{6}}$$

Para evaluar la incertidumbre en la planificación, se calcula la **varianza (V)** con la siguiente ecuación:

$$\boldsymbol{V = \left(\frac{P-O}{6}\right)^2}$$

A continuación, se presenta la planificación detallada con sus respectivos cálculos:

Tabla 11 Cronograma de Implementación

Fase	Actividad	O (días)	M (días)	P (días)	TE (días)	Varianza (V)
Fase 1: Planificación	Selección de equipo y recursos	5	7	10	$\frac{5+4(7)+10}{6} = 7.33$	$\left(\frac{10-5}{6}\right)^2 = 0.69$
	Diseño del programa educativo	7	10	15	$\frac{7+4(10)+15}{6} = 10.33$	$\left(\frac{15-7}{6}\right)^2 = 1.78$
Fase 2: Capacitación	Formación de instructores	10	15	20	$\frac{10+4(15)+20}{6} = 15$	$\left(\frac{20-10}{6}\right)^2 = 2.78$
	Desarrollo de materiales	8	12	18	$\frac{8+4(12)+18}{6} = 12.67$	$\left(\frac{18-8}{6}\right)^2 = 2.78$
Fase 3: Implementación	Ejecución de talleres	15	20	30	$\frac{15+4(20)+30}{6} = 21.67$	$\left(\frac{30-15}{6}\right)^2 = 6.25$
	Implementación de herramientas de seguridad	12	18	25	$\frac{12+4(18)+25}{6} = 18.17$	$\left(\frac{25-12}{6}\right)^2 = 4.69$
Fase 4: Monitoreo y Evaluación	Encuestas y análisis de impacto	10	12	18	$\frac{10+4(12)+18}{6} = 12.67$	$\left(\frac{18-10}{6}\right)^2 = 1.78$
	Ajustes y optimización	8	10	15	$\frac{8+4(10)+15}{6} = 10.33$	$\left(\frac{15-8}{6}\right)^2 = 1.36$

Fuente: Elaboración Propia

Cálculo del Tiempo Total y la Variabilidad

El **tiempo total estimado (T_Total)** se obtiene sumando los valores TE:

T_Total=7.33+10.33+15+12.67+21.67+18.17+12.67+10.33= **108.17 días**

La **varianza total (V_Total)** es la suma de todas las varianzas individuales:

V_Total=0.69+1.78+2.78+2.78+6.25+4.69+1.78+1.36= **22.11**

La **desviación estándar total (σ_Total)** es la raíz cuadrada de la varianza total:
σTotal= $\sqrt{22.11}$ = **4.70 días.**

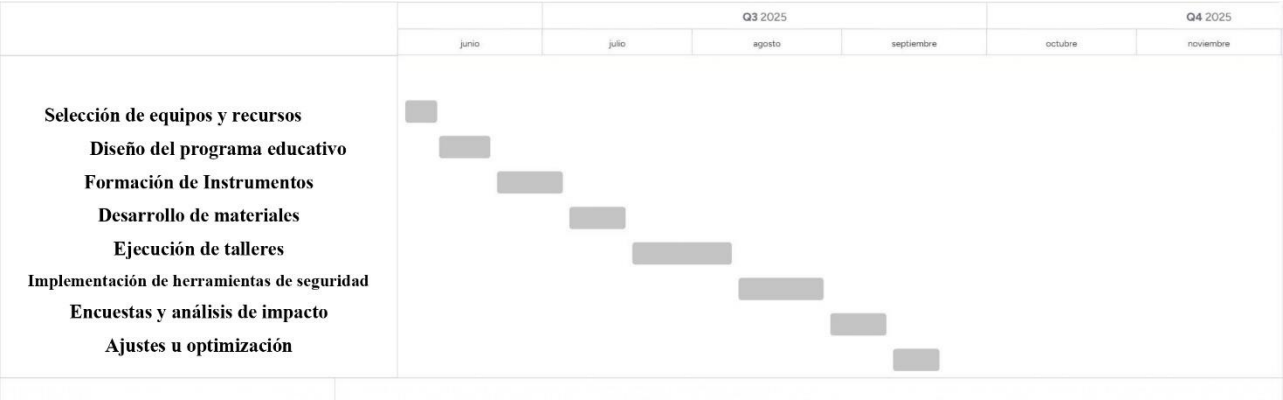


Figura 21 Diagrama de Gantt

Fuente: Elaboración propia

Tabla 12 Presupuesto

Concepto	Descripción	Costo Unitario (USD)	Cantidad/Periodicidad	Total (USD)	Observaciones
Capacitación y Sensibilización	Talleres interactivos, manuales, videos y guías didácticas	100 por sesión	10 sesiones	USD 1,000.00	Incluye honorarios de instructores y materiales educativos
Licencias de Software de Seguridad	Bitdefender Total Security (incluye funciones VPN)	50 por hogar	247 hogares	USD 12,300.00	Precio referencial anual; posibilidad de descuentos por compra en volumen
Infraestructura de Redes	Routers MikroTik hAP ac2 configurados con firewalls integrados	80 por unidad	246 unidades	USD 19,680.00	Costo aproximado e incluye la configuración inicial
Sistemas de Monitoreo y Gestión	Implementación y configuración de Security Onion	0 (open-source)*	1 implementación	USD 2,000.00	Inversión en instalación, personalización y soporte técnico
	Implementación y configuración de Wazuh	0 (open-source)*	1 implementación	USD 1,500.00	Costos asociados a soporte técnico y personalización adicional

Concepto	Descripción	Costo Unitario (USD)	Cantidad/Periodicidad	Total (USD)	Observaciones
Auditorías y Pruebas de Seguridad	Pruebas de penetración y auditorías técnicas (uso de Kali Linux y Metasploit)	500 por auditoría	4 auditorías anuales	USD 2,000.00	Incluye contratación de expertos para análisis y detección de vulnerabilidades
Soporte Técnico y Mantenimiento	Atención remota y presencial para resolución de incidencias	200 mensuales	12 meses	USD 2,400.00	Servicio de soporte continuo y mantenimiento preventivo
Gastos Administrativos y Logística	Materiales, coordinación administrativa, imprevistos y logística	-	Proyecto completo	USD 1,000.00	Fondo de contingencia para gastos operativos adicionales
Total Estimado				**USD 41,880.00**	

Fuente: Elaboración Propia

6.7 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

La propuesta está directamente alineada con los hallazgos de la investigación, respondiendo a las vulnerabilidades identificadas en las redes domésticas de teletrabajadores en Chamelecón. Se evidenció que la falta de conocimientos en ciberseguridad, la escasez de medidas de protección adecuadas y la baja inversión en herramientas de seguridad han incrementado la exposición de los hogares a ataques cibernéticos. Las acciones propuestas, como la capacitación en seguridad digital, la implementación de routers seguros y el monitoreo de redes, abordan los problemas detectados en el estudio y ofrecen soluciones realistas y adaptadas a la comunidad. El uso de herramientas como Bitdefender, MikroTik y Security Onion permitirá mejorar la seguridad digital con soluciones accesibles y efectivas.

Además, el modelo de evaluación y mejora continua garantizará que las estrategias implementadas se adapten a los cambios en el panorama de amenazas, asegurando la sostenibilidad de la seguridad digital en los hogares de la comunidad. Esta propuesta no solo mitigará las vulnerabilidades existentes, sino que también fomentará una **cultura de ciberseguridad** entre los teletrabajadores de Chamelecón, promoviendo un entorno digital más seguro.

Anexos

Estructura de cuestionario

Cuestionario sobre Ciberseguridad en Redes Domésticas para Teletrabajo en Chamelecón departamento de Cortés, Honduras

Ciberseguridad en Redes Domésticas para Teletrabajo en Chamelecón dpto. de Cortés, Honduras

Introducción: Estimado(a) participante, Le agradecemos su disposición para participar en esta investigación. Este cuestionario tiene como objetivo recopilar información sobre las amenazas cibernéticas, las prácticas de seguridad y el nivel de capacitación en ciberseguridad en hogares del Barrio Chamelecón que realizan teletrabajo. Sus respuestas serán fundamentales para comprender los retos de ciberseguridad en el contexto local y diseñar estrategias efectivas de mitigación.
Tiempo estimado: El tiempo estimado para completar este cuestionario es de 10 a 15 minutos.

Confidencialidad: Toda la información proporcionada será tratada de forma confidencial y anónima. Los datos recolectados se utilizarán únicamente con fines académicos. En ningún caso, sus respuestas estarán vinculadas a su identidad personal.

Consentimiento: Al responder este cuestionario, usted acepta participar de manera voluntaria en esta investigación. Puede abandonar el cuestionario en cualquier momento si lo desea, sin que ello implique ningún perjuicio.

Instrucciones: Por favor, lea cada pregunta con atención y marque la opción que mejor refleje su situación o percepción. Si tiene dudas, no dude en contactarme a través del correo institucional oscar.benites@unitec.edu

Fase I: Información General y Socioeconómica

¿Cuál es el ingreso mensual aproximado de su hogar? *

Marca solo un óvalo.

- Menos de 10,000 Lempiras
- 10,001 - 15,000 Lempiras
- 15,001 - 20,000 Lempiras
- Más de 20,000 Lempiras

¿Cuántas personas en su hogar realizan teletrabajo actualmente? *

Marca solo un óvalo.

- Ninguna
- 1 Persona
- 2 Personas
- 3 o más personas

¿Cuántos dispositivos con acceso a Internet tiene su hogar? *

Marca solo un óvalo.

- 1 dispositivo
- 2-3 dispositivos
- 4-5 dispositivos
- Más de 5 dispositivos

Fase II: Prácticas de Seguridad Digital

¿Con qué frecuencia realiza actualizaciones de software en los dispositivos de su hogar? *

Marca solo un óvalo.

- Nunca
- Rara vez
- De vez en cuando
- Siempre

¿Utiliza alguna de las siguientes medidas de seguridad en los dispositivos de su hogar? (Seleccione todas las que apliquen) *

Selecciona todos los que correspondan.

- [ ] Antivirus
- [ ] Firewall
- [ ] VPN
- [ ] Autenticación Multifactor
- [ ] Ninguna

¿Cuántas veces ha experimentado su hogar un ataque cibernético en los últimos 12 meses? *

Marca solo un óvalo.

- Ninguna
- 1 vez
- 2-3 veces
- Más de 3 veces

¿Cuál de los siguientes ciberataques ha experimentado en su hogar? (Seleccione todas las que apliquen) *

Marca solo un óvalo.

- Phishing
- Ransimware
- Malware
- Ataques de denegación de servicios (DDoS)
- Ninguno

Fase III: Capacitación en Ciberseguridad

¿Ha recibido alguna capacitación en ciberseguridad en los últimos 12 meses?

Marca solo un óvalo.

- Sí
- No

Si respondió "Sí" a la pregunta anterior, ¿qué tipo de capacitación recibió? (Seleccione todas las que apliquen) *

Selecciona todos los que correspondan.

- Curso en línea
- Taller presencial
- Capacitación autodidacta (Artículos, videos, etc.)
- Ninguna

¿Considera que su nivel de conocimiento en ciberseguridad es suficiente para proteger su red doméstica? *

Marca solo un óvalo.

- Sí
- No
- No estoy seguro

¿Cuáles de las siguientes acciones de seguridad realiza regularmente para proteger su red doméstica? (Seleccione todas las que apliquen) *

Selecciona todos los que correspondan.

- [ ] Cambio regular de contraseñas
- [ ] Uso de contraseñas seguras
- [ ] Supervisión de la actividad de la red
- [ ] Ninguna

Fase IV: Percepción del Riesgo Cibernético

En una escala de 1 a 5, ¿qué tan preocupado está por la seguridad de su red doméstica y los dispositivos utilizados para teletrabajo? *

Marca solo un óvalo.

- ◯ 1 (Nada preocupado)
- ◯ 2 (Poco preocupado)
- ◯ 3 (Moderadamente preocupado)
- ◯ 4 (Bastante preocupado)
- ◯ 5 (Muy preocupado)

¿Cree que las medidas de seguridad implementadas en su hogar son suficientes para prevenir los ciberataques? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No estoy seguro

Fase V: Opiniones Generales

¿Qué tanto cree que el teletrabajo ha incrementado el riesgo de sufrir un ciberataque en su hogar? *

Marca solo un óvalo.

- ◯ Ha incrementado significativamente el riesgo
- ◯ Ha incrementado ligeramente el riesgo
- ◯ No ha tenido impacto
- ◯ Ha reducido el riesgo

En su opinión, ¿qué tan importante es que las empresas proporcionen capacitación en ciberseguridad a sus empleados que trabajan desde casa?

Marca solo un óvalo.

- ◯ Muy importante
- ◯ Algo importante
- ◯ Poco importante
- ◯ No es importante

Estructura de guía de entrevista

Guía de entrevista a los expertos sobre Ciberseguridad

Guía de Entrevista a Expertos en Ciberseguridad

Introducción: Estimado(a) experto(a), Le agradecemos por participar en esta entrevista, que forma parte de una investigación orientada a comprender las amenazas cibernéticas en redes domésticas utilizadas para teletrabajo en el Barrio Chamelecón, Cortés, Honduras. Su experiencia y conocimientos serán esenciales para identificar vulnerabilidades, diseñar estrategias de mitigación y proponer soluciones prácticas adaptadas al contexto local.
Tiempo estimado: La duración aproximada de esta entrevista será de **30 a 40 minutos**.
Confidencialidad: Toda la información compartida será tratada de forma **confidencial y anónima**. Los datos obtenidos se utilizarán exclusivamente para fines académicos. En ningún caso, sus respuestas estarán vinculadas a su identidad personal o profesional sin su consentimiento explícito.
Consentimiento: Al participar en esta entrevista, usted acepta hacerlo de manera voluntaria. La sesión será grabada con su consentimiento para garantizar la precisión en el análisis, y podrá solicitar la interrupción de la grabación o la entrevista en cualquier momento.
Instrucciones: La entrevista constará de preguntas abiertas que buscan explorar su percepción y experiencia en temas relacionados con ciberseguridad en redes domésticas. No hay respuestas correctas o incorrectas; lo importante es su perspectiva profesional.

¿Podría compartir un poco sobre su experiencia en ciberseguridad, especialmente en el contexto de redes domésticas y teletrabajo? *

¿Cuáles son las principales amenazas cibernéticas que afectan a los trabajadores remotos en redes domésticas? ¿Ha notado un incremento en ciertos tipos de ciberataques desde la adopción del teletrabajo? *

¿Qué diferencias observa entre las amenazas cibernéticas que enfrentan las redes corporativas y las redes domésticas utilizadas para teletrabajo? *

Desde su perspectiva, ¿cuáles son las vulnerabilidades más comunes en las redes domésticas utilizadas para teletrabajo, especialmente en zonas como el Barrio Chamelecón, donde los recursos tecnológicos pueden ser limitados? *

¿Qué tipos de dispositivos (como routers, computadoras, IoT, etc.) son los más propensos a ser atacados por cibercriminales en entornos de teletrabajo? *

¿Qué estrategias o medidas de seguridad considera más efectivas para proteger las redes domésticas de los teletrabajadores? ¿Qué herramientas de protección digital recomendaría? *

¿Cuál considera que es el nivel actual de capacitación en ciberseguridad entre los teletrabajadores en Honduras, y cómo cree que esto afecta la seguridad de las redes domésticas? *

¿Cuáles son las principales recomendaciones que le daría a las empresas y organismos gubernamentales para mejorar la seguridad de las redes domésticas en Honduras? *

REFERENCIAS BIBLIOGRÁFICAS

Atlantic Council. (2023). *The State of Cybersecurity in Latin America.*

Banco Interamericano de Desarrollo. (2023). *Informe sobre Ciberseguridad en América Latina: Desafíos y Oportunidades*.

Barney, J. B., & Hesterly, W. S. (2022). *Strategic Management and Competitive Advantage: Concepts and Cases*. Pearson.

Cisco. (2021). *Understanding Home Networks*.

CNBS. (2021). *Normas para la Administración de Información y Tecnología.*

Combs, G. (2022). *Wireshark User's Guide. The Wireshark Foundation.*

Comisión Federal de Comercio (FTC). (2023). *Consumer Sentinel Network Data Book 2023*.

CONATEL. (2023). *Normativas y directrices sobre ciberseguridad en Honduras.*

Conrrado E., Pizarro G. & Gonzalez M. (2021). *Seguridad y Protección de la Información en la Era Digital*.

Consejo de Europa. (2001). *Convenio de Budapest sobre Ciberdelincuencia*.

Consejo de Protección de Datos de California. (2022). *CCPA Compliance Report.*

Criterio HN. (2019). *Propuesta de ley de ciberseguridad*.

CSIS. (2022). *Centro de Estudios Estratégicos e Internacionales (Informe sobre el costo global del delito cibernético)*.

Cybersecurity Ventures 2024. (2023). *Cybersecurity Ventures*. Cybersecurity Ventures.

Deloitte. (2023). *Data Center Sustainability*.

Diario Oficial La Gaceta. (2014). *Ley de Comercio Electrónico (Decreto No. 149-2014).*

Diario Oficial La Gaceta. (2017). *Código Penal de Honduras (Decreto No. 130-2017).*

ENISA. (2023). *ENISA threat landscape 2021: April 2020 to mid July 2021*. Publications Office.

https://data.europa.eu/doi/10.2824/324797

ESET. (2023). *Informe de Ciberseguridad en América Latina.*

Foro Económico Mundial. (2023). *Growing Threat to Fragile Global Economy*.

Forrester. (2023). *Third-Party Risk Management in the Age of Remote Work*.

FortiGuard Lab. (2024). *Ciberseguridad, las cifras que evidencian el riesgo: Tendencias. DATA Y CIBERSEGURIDAD*. Editora El Sol, S.A. de C.V.

Gartner. (2023). *Gartner 2023*.

Gómez, R.; Ruiz, D. (2022). *Ciberseguridad y teletrabajo: Riesgos y medidas preventivas*.

Google Maps. (2024). *Google [Mapa de Chamelecon, Cortés, Honduras]* [Map].

Hernández Sampieri, R., & Fernandez-Collado, C. F. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education.

IBM. (2023). *Cost of a Data Breach Report.*

IEEE. (2022). *Internet of Things: Concepts and Applications.*

IIES-UNAH. (2022). *Perfil Sociodemográfico de San Pedro Sula, Cortés*.

ISACA. (2023). *State of Cybersecurity 2023*.

ISO. (2022). *ISO/IEC 27001: Information Security Management*. International Organization for Standardization.

ISO/IEC 27001:2022. (2022). *Security Techniques—Information Security Management Systems—Requirements*.

Kaspersky Lab. (2023). *Top Cybersecurity Threats for Remote Work.*

Lyon. (2009). *The Official Nmap Project Guide to Network Discovery and Security Scanning.*

National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Information Systems and Organizations*.

Oostendorp, S. (2021). *The Penetration Tester's Guide. No Starch Press*.

Organización Internacional del Trabajo. (2020). *El Futuro del Trabajo: Teletrabajo y sus Desafíos*.

Parlamento Europeo. (2016). *Reglamento General de Protección de Datos (GDPR)*.

Statista. (2023). *Economic Impact of Cybercrime Worldwide*.

UNAH. (2022). *Equipo de Respuesta ante Incidentes de Seguridad Informática*.

Verizon. (2023). *Data Breach Investigations Report*. Verizon.

Weber, R. H. (2021). *Weber*.

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*.