

**UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO**



FACULTAD DE CIENCIAS DE LA INGENIERÍA

SOFTWARE (REDISEÑO)

**Virus Informáticos:**

**Análisis de Vulnerabilidades y**

**Técnicas de Detección**

**PROYECTO DE INVESTIGACIÓN**

**AUTOR:**

FREDDY VLADIMIR FARINANGO GUANDINANGO

**QUEVEDO LOS RIOS**

MARZO, 2024

**RESUMEN EJECUTIVO PALABRAS CLAVES**

Este proyecto de investigación se centra en el análisis de las vulnerabilidades en sistemas informáticos y en la exploración de técnicas de detección de virus informáticos. Con el aumento de la dependencia de la tecnología digital en la sociedad actual, los virus informáticos representan una amenaza significativa para la seguridad cibernética.

El objetivo principal es identificar las vulnerabilidades más comunes que permiten la propagación de virus informáticos y evaluar las técnicas de detección más efectivas disponibles. Esto se logrará mediante un análisis teórico y práctico de las vulnerabilidades y técnicas de detección existentes.

La metodología de investigación incluirá el uso de bases de datos de vulnerabilidades, muestras de malware y herramientas de análisis de seguridad. Además, se llevarán a cabo estudios de casos y encuestas para comprender mejor las necesidades y desafíos reales en términos de seguridad cibernética.

Se espera que los resultados de esta investigación proporcionen una mejor comprensión de las vulnerabilidades en sistemas informáticos y contribuyan al desarrollo de estrategias más efectivas para detectar y prevenir la propagación de virus informáticos. Esto ayudará a promover un entorno en línea más seguro y confiable para individuos y organizaciones. Además, se espera que los hallazgos de este estudio no solo beneficien a la comunidad académica y técnica, sino que también sean útiles para profesionales de la seguridad cibernética, responsables de políticas públicas y cualquier persona interesada en proteger su información en línea.

**Palabras claves:** Virus informático, Análisis, detención, vulnerabilidades, seguridad cibernética

**ABSTRAC AND KEYWORDS**

This research project focuses on analyzing vulnerabilities in computer systems and exploring techniques for detecting computer viruses. With the increasing reliance on digital technology in today's society, computer viruses pose a significant threat to cybersecurity.

The main objective is to identify the most common vulnerabilities that allow computer viruses to spread and evaluate the most effective detection techniques available. This will be achieved through both theoretical and practical analysis of existing vulnerabilities and detection techniques.

The research methodology will involve using vulnerability databases, malware samples, and security analysis tools. Additionally, case studies and surveys will be conducted to better understand the real needs and challenges in terms of cybersecurity.

It is expected that the results of this research will provide a better understanding of vulnerabilities in computer systems and contribute to the development of more effective strategies for detecting and preventing the spread of computer viruses. This will help promote a safer and more reliable online environment for individuals and organizations. Furthermore, it is anticipated that the findings of this study will not only benefit the academic and technical community but also be useful for cybersecurity professionals, policymakers, and anyone interested in protecting their information online.

Keywords: Computer virus, Analysis, detection, vulnerabilities, cybersecurity

Tabla de contenido

[INTRODUCCIÓN 6](#_Toc161422855)

[**CAPITULO I** 7](#_Toc161422856)

[**CONTEXTO ESPECÍFICO DE LA INVESTIGACIÓN** 7](#_Toc161422857)

[**1.1.** **PROBLEMATIZACIÓN DE LA INVESTIGACIÓN** 8](#_Toc161422858)

[**1.1.1.** **Planteamiento del problema** 8](#_Toc161422859)

[**1.1.2.** **DIAGNÓSTICO** 8](#_Toc161422860)

[**1.1.2.1.** **Causas principales** 9](#_Toc161422861)

[**1.1.2.2.** **Efectos principales** 9](#_Toc161422862)

[**1.1.3.** **PRONÓSTICO** 10](#_Toc161422863)

[**1.1.4.** **SISTEMATIZACIÓN DEL PROBLEMA** 10](#_Toc161422864)

[**1.1.4.1.** **Pregunta general** 10](#_Toc161422865)

[**1.1.4.2.** **Preguntas específicas** 10](#_Toc161422866)

[**1.1.5. OBJETIVOS** 11](#_Toc161422867)

[**1.1.5.1. Objetivo general** 11](#_Toc161422868)

[**1.1.5.2. Objetivos específicos** 11](#_Toc161422869)

[**1.1.6.** **HIPOTESIS.** 12](#_Toc161422870)

[**1.1.6.1.** **Planteamiento** 12](#_Toc161422871)

[**1.1.6.2.** **Matriz de operacionalización de la hipótesis** 12](#_Toc161422872)

[**CAPÍTULO II** 14](#_Toc161422873)

[**FUNDAMENTACIÓN TEÓRICA DE LA** 14](#_Toc161422874)

[**INVESTIGACIÓN** 14](#_Toc161422875)

[**2.1. MARCO TEÓRICO** 15](#_Toc161422876)

[**2.1.1. MARCO CONCEPTUAL** 15](#_Toc161422877)

[**2.1.2. MARCO REFERENCIAL** 16](#_Toc161422878)

[**CAPÍTULO III** 17](#_Toc161422879)

[**METODOLOGÍA DE LA INVESTIGACIÓN** 17](#_Toc161422880)

[**3.1. LOCALIZACIÓN** 18](#_Toc161422881)

[Tabla 1 Población y muestra 18](#_Toc161422882)

[ 18](#_Toc161422883)

[**3.2.** **MÉTODO DE INVESTIGACIÓN** 18](#_Toc161422884)

[**3.2.1.** **Metodología Cuantitativa** 18](#_Toc161422885)

[**3.2.2.** **Comprobación de la hipótesis** 19](#_Toc161422886)

[**3.2.2.1.** **Manipulación de la variable independiente:** 19](#_Toc161422887)

[**3.2.2.2.** **Efecto en la variable dependiente:** 19](#_Toc161422888)

[**3.2.2.3.** **Análisis de los resultados:** 20](#_Toc161422889)

[**3.3.** **METODOLOGÍA CUALITATIVA** 20](#_Toc161422890)

[**3.4.** **FUENTES DE RECOPILACIÓN** 20](#_Toc161422891)

[**3.4.1.** **Fuentes Primarias:** 21](#_Toc161422892)

[**3.4.2.** **Fuentes Secundarias:** 21](#_Toc161422893)

[**3.5.** **DISEÑO DE LA INVESTIGACIÓN** 21](#_Toc161422894)

[**3.6.** **INSTRUMENTOS DE INVESTIGACIÓN** 22](#_Toc161422895)

[**3.6.1.** **Encuesta sobre Conocimientos y Experiencias con Virus Informáticos:** 22](#_Toc161422896)

[**3.6.2.** **Cuestionario de Evaluación de Software Antivirus:** 23](#_Toc161422897)

[**3.6.3.** **Entrevistas en Profundidad con Expertos en Seguridad Informática:** 23](#_Toc161422898)

[**3.6.4.** **Ejemplo de entrevista que se llevó a cabo** 23](#_Toc161422899)

[**3.7.** **TRATAMIENTO DE LOS DATOS** 25](#_Toc161422900)

[**3.7.1.** **Datos obtenidos** 25](#_Toc161422901)

[**3.8.** **Recursos Humanos y Materiales** 26](#_Toc161422902)

[**3.8.1.** Materiales para utilizar 27](#_Toc161422903)

[**3.9.** **Cronograma de Actividades** 28](#_Toc161422904)

[**CAPÍTULO IV** 29](#_Toc161422905)

[**BIBLIOGRAFIA Y ANEXOS** 29](#_Toc161422906)

[**4.1. REFERENCIAS** 30](#_Toc161422907)

[**4.2. ANEXOS** 32](#_Toc161422908)

[**4.2.1. CUESTIONARIO DE PREGUNTAS-ENCUESTA** 32](#_Toc161422909)

[**4.3. ENCUESTA Y RESULTADOS DE SIMULACIÓN** 33](#_Toc161422910)

[**4.4. ÁRBOL DE PROBLEMA** 36](#_Toc161422911)

# INTRODUCCIÓN

En el trasfondo de la era digital, donde la tecnología se ha vuelto inseparable de nuestra vida cotidiana, surge una amenaza persistente que compromete la seguridad y estabilidad de nuestros sistemas informáticos: los virus informáticos. Este proyecto se sumerge en la exploración exhaustiva de esta problemática, ofreciendo una retrospectiva crítica de los desafíos enfrentados y propiciando una perspectiva prospectiva para construir un entorno digital más seguro.

A lo largo del tiempo, hemos sido testigos de la evolución constante de los virus informáticos, transformándose de simples códigos maliciosos a sofisticadas herramientas que amenazan la integridad de datos y la privacidad de usuarios en todo el mundo. Esta investigación, al abordar los acontecimientos pasados y actuales, pretende dotar al lector de una comprensión profunda de la importancia y gravedad de esta amenaza.

La motivación subyacente en este trabajo no se limita a la mera exposición de hechos históricos. Más allá, busca inspirar el interés del lector al ofrecer una visión clara y convincente sobre la magnitud del problema. La relevancia de esta investigación se manifiesta en la necesidad apremiante de comprender y enfrentar estos desafíos de manera proactiva, antes de que evolucionen hacia formas aún más perniciosas.

Esta centrado en la problemática de los virus informáticos, se revela como un área de estudio crítica en el contexto actual. La dependencia creciente de la sociedad en la tecnología hace que la seguridad digital sea una prioridad ineludible. En este sentido, la presente investigación no solo reflexiona sobre los riesgos pasados y presentes, sino que también señala la importancia de adoptar medidas preventivas y soluciones innovadoras.

# **CAPITULO I**

# **CONTEXTO ESPECÍFICO DE LA INVESTIGACIÓN**

## **PROBLEMATIZACIÓN DE LA INVESTIGACIÓN**

### **Planteamiento del problema**

Una imagen de un videojuego

Descripción generada automáticamente con confianza bajaCon el rápido avance de la tecnología y la presencia constante de la internet en nuestras vidas, hemos obtenido muchos beneficios. Pero, al mismo tiempo, nos enfrentamos a un problema serio: los virus informáticos. Estos "bichos" afectan la ciberseguridad[1], [2]. En la actualidad enfrenta desafíos constantes debido a la proliferación de virus informáticos y programa maligno. Estos agentes maliciosos pueden comprometer la integridad, confidencialidad y disponibilidad de datos y sistemas. Por lo tanto, es crucial analizar y comprender sus técnicas de evasión y propagación. [1], [3]

La falta de un análisis profundo de estas vulnerabilidades y de la eficacia de las técnicas de detección disponibles crea una brecha significativa en nuestra capacidad para proteger adecuadamente los sistemas informáticos contra esta amenaza creciente.[4]

Además, la detección de vulnerabilidades es fundamental para prevenir ataques. Mediante un minucioso análisis de software, hardware y configuraciones, se pueden identificar debilidades que podrían ser explotadas por atacantes. La detección temprana de estas vulnerabilidades permite tomar medidas preventivas y proteger activos digitales. [3], [5], [6]

Este es un problema grande que afecta a personas, negocios e instituciones en todo el mundo.

### **DIAGNÓSTICO**

Mucho es lo que se habla de los Virus Informáticos pero la realidad es que cada día que pasa nos llegan nuevos comentarios y nos preguntamos cuales son las causas del origen y de recientes apariciones que hoy en día producen daños y efectos maliciosos, lo que en últimas ha propiciado desconcierto y malestar general en los usuarios; por eso es conveniente conocer un poco más acerca de ellos, como su forma de actuar, para así poderlos prevenir y en el peor de los casos combatirlos con eficacia. [6]

### **Causas principales**

* Programadores interesados en rebasar los límites de las más reciente tecnologías. [6]
* Por varias empresas interesadas en la piratería de software. [3], [6]
* personas lo hacían con la necesidad de demostrar su creatividad y su dominio de las computadoras, por diversión o como una forma de manifestar su repudio a la sociedad que los oprimía. [3]
* la producción inicial de los virus informáticos fue obra de expertos inescrupulosas con ansias de hacer dineros con posteriores curas.[1]
* estudiantes ele informática deseosos de probar su destreza. Demostrar su valía como programadores. Cuantos mayores sean sus daños, mayor el reconocimiento entre los miembros ele la escena. [4], [5]

### **Efectos principales**

* crea sectores malos en áreas no usadas del disco, disminuyendo paulatinamente su capacidad,[3], [7]
* Interfieren con la operación de programas residentes en memoria RAM, [8]
* Bloquear buffers de manera que no permite la entrada o salida de los discos, pareciendo una falla de software [9]
* Destrozar discos duros, alterar el buen funcionamiento ele las redes, provocar pérdidas, molestar.[10]
* Pérdida de datos o parte de su información, evitando el intercambio de información importante que antes era fomentada, ocasionando con esto pérdida de tiempo y dinero. [11]
* Aumento de labor y economía de las empresas de servicios y desarrollos de sistemas de seguridad informática ya que en la actualidad están viviendo en un tiempo de oro por elaborar proyectos para prevenir el virus. [8], [12]

### **PRONÓSTICO**

La evolución futura de los virus informáticos es un aspecto crucial en el ámbito de la seguridad cibernética. A medida que avanzamos en nuestro proyecto, debemos considerar las implicaciones de esta evolución constante. Se espera que los virus se vuelvan cada vez más complejos y evasivos, dificultando su detección y comprensión.[12]

Este aumento en la sofisticación podría traducirse en una mayor frecuencia y gravedad de los ataques cibernéticos. Las consecuencias podrían ser pérdidas económicas significativas y la exposición de información confidencial tanto para individuos como para organizaciones. Además, responder a estos ataques requerirá más tiempo y recursos, lo que podría afectar el funcionamiento habitual de los sistemas informáticos.[8], [10], [12], [13]

Por lo tanto, es vital adoptar un enfoque proactivo y adaptable para afrontar estos desafíos emergentes y garantizar la seguridad continua de los sistemas digitales. Reconocer estas proyecciones nos permitirá estar mejor preparados y desarrollar estrategias eficaces de defensa cibernética que preserven la integridad de la información y la seguridad de nuestros sistemas.[10], [11]

### **SISTEMATIZACIÓN DEL PROBLEMA**

### **Pregunta general**

¿se puede desarrollar un programa de alto rendimiento de manera muy inteligente para la detección y prevención del virus informático?

### **Preguntas específicas**

* ¿Cuáles son las técnicas más efectivas para detectar la presencia de virus informáticos en un sistema?
* ¿Cómo se puede reconocer la presencia de un virus informático en una computadora?
* ¿Cuál es la herramienta apropiada para realizar el programa de detección y prevención del virus?
* ¿Qué nivel de conocimiento académico de programación debo tener para llevar a cabo el proyecto?
* ¿Cuáles son las vulnerabilidades más críticas en los sistemas operativos modernos que pueden ser explotadas por virus informáticos?
* ¿Cómo influye el desarrollo de software seguro en la prevención de vulnerabilidades que podrían ser explotadas por virus informáticos?

### **1.1.5. OBJETIVOS**

### **1.1.5.1. Objetivo general**

Desarrollar un software de sistema basado en seguridad de detección y prevención del virus informático en la sociedad.

### **1.1.5.2. Objetivos específicos**

* Desarrollar una aplicación antivirus avanzado que abarque la, prevención y respuesta efectiva para computadoras y dispositivos en el transcurso de tres años académicos.
* Establecer alianzas con instituciones educativas y empresas de tecnología para promover el acceso a recursos y oportunidades de aprendizaje en el desarrollo de antivirus para estudiantes a nivel internacional.
* Desarrollar una plataforma web internacional que ofrezca orientación y recursos para principiantes interesados en el desarrollo efectivo de antivirus, facilitando así su formación en seguridad informática.
* Diseñar un software de análisis forense que utilice inteligencia artificial para identificar la firma digital y el comportamiento de malware en sistemas informáticos comprometidos, con el objetivo de mejorar las investigaciones de ciberdelitos.
* Desarrollar una herramienta de detección de malware basada en la nube, con algoritmos avanzados para proteger la información sensible de usuarios y organizaciones.
* Crear una aplicación web como parte del proyecto de titulación académica, utilizando algoritmos de inteligencia artificial y aprendizaje automático para detectar y analizar características específicas de malware

### **HIPOTESIS.**

### **Planteamiento**

Un software inteligente basado en la detección y prevención en seguridad informática es clave para la erradicación sostenida de infecciones provocadas por virus informáticos

### **Matriz de operacionalización de la hipótesis**

|  |  |  |
| --- | --- | --- |
| **VARIABLE** | **DEFINICIÓN** | **INDICADOR** |
| **VARIABLE INDEPENDIENTE**  Un software inteligente basado en la detección y prevención en seguridad informática | Desarrollar un software antivirus implica crear defensas contra amenazas informáticas . Además, se define como una aplicación informática diseñada para identificar y mitigar amenazas y vulnerabilidades en sistemas informáticos.[6], [14], [15] | * Licencia adquirida (porcentaje de licencias disponibles). * Porcentaje de sistemas en los que está instalado el software * Porcentaje de dispositivos con configuración de protección activa. * Porcentaje de sistemas actualizados automáticamente. |
| **VARIABLE DEPENDIENTE**    Erradicación sostenida de infecciones provocadas por virus informáticos | Son programas desconocido os y con intenciones maliciosas que se ejecutan en un ordenador o dispositivo sin el permiso del usuario, generando problemas de software y hardware[1], [5], [11] | * Porcentaje de disminución en el número de incidentes reportados * Reducción en el tiempo promedio entre infecciones antes y después de la implementación del software. * Aumento porcentual en la confianza del usuario en la seguridad del sistema. |

**Tabla de Operacionalización**

# **CAPÍTULO II**

# **FUNDAMENTACIÓN TEÓRICA DE LA**

# **INVESTIGACIÓN**

# **2.1. MARCO TEÓRICO**

A continuación, esta presentado fuentes confiables que respaldan la hipótesis planteada de que la creación y el uso del software antivirus han aumentado la seguridad cibernética y han contribuido a reducir la delincuencia informática. Sus hallazgos proporcionan una base sólida para comprender el impacto positivo del software antivirus en la protección de datos y la seguridad en línea

### **2.1.1. MARCO CONCEPTUAL**

Seguridad del software Protege al software de amenazas que pueden ser producidas por un cracker u otras potenciales vulnerabilidades que ponen en peligro a los principios de La seguridad de la información como la confidencialidad, integridad y disponibilidad de los datos.[9]

Uno de los problemas que surgen al implementar sistemas de alta seguridad es definir una arquitectura que minimice el código necesario para implementar la seguridad del sistema[6], [15].

Un concepto que ayuda a abordar este problema es la TCB que es el conjunto de componentes de hardware y software responsables de implementar la política de seguridad.[10]

La seguridad informática se ha convertido en un factor de gran importancia principalmente en las organizaciones, derivado de la necesidad de mantener protegida la información que se encuentra en los dispositivos electrónicos, así como de los usuarios que la manejan.[16]

El desarrollo de software de seguridad actúa como un guardián contra estos invasores digitales.

Los antivirus son la mejor herramienta para combatir este tipo de problemas de virus expuestos, de ahí su eficacia para mitigar y controlar la seguridad en su organización y supervisar los archivos maliciosos con el fin de eliminarlos del sistema [6], [14]

Actualmente se considera que la criptografía es una disciplina que combina la matemática y la informática con el fin de crear y estudiar métodos para transmitir datos de forma segura a través de canales de comunicación públicos. La seguridad se logra por medio de métodos que cambian la apariencia de un mensaje sin cambiar su significado[6], [9], [13]

### **2.1.2. MARCO REFERENCIAL**

Investigaciones realizadas por el Instituto de Seguridad Cibernética han documentado casos de organizaciones que experimentaron una disminución significativa en incidentes de seguridad relacionados con malware después de implementar soluciones avanzadas de seguridad informática.[15]

Un estudio de García et al. (2019) encontró que las organizaciones que implementaron software de seguridad avanzado experimentaron una reducción sustancial en incidentes de seguridad relacionados con malware, respaldando así la efectividad de las soluciones de seguridad inteligente en la erradicación de infecciones por virus informáticos.[17]

Además, según múltiples fuentes confiables, incluyendo informes de instituciones de investigación líderes en seguridad informática y expertos reconocidos en el campo, la creación y el uso extendido de software antivirus han demostrado aumentar la seguridad cibernética al reducir las tasas de robo de información y delincuencia informática. Por ejemplo, estudios recientes han indicado una disminución del 70% en los casos de robo de información y del 75% en la delincuencia informática desde la implementación generalizada de software antivirus. Estos hallazgos subrayan el papel crucial del software antivirus en la protección de datos y la seguridad en línea[6], [14], [15], [16]

Algo relevante también es el informe de la Europol sobre la Evaluación de la Amenaza de la Delincuencia Cibernética (TESA), que identifica el desarrollo y la implementación de software antivirus como una de las estrategias clave para combatir la delincuencia informática a nivel internacional. El informe destaca los avances tecnológicos en la detección y prevención de amenazas cibernéticas y enfatiza la importancia de la cooperación entre los sectores público y privado en la lucha contra la delincuencia informática.[18]

**Bruce Schneier** Su condición de gurú de la seguridad se ve confirmada por haber testificado ante el Congreso de los Estados Unidos en materia de seguridad. Él es un maestro en ilustrar el mundo oculto de la encriptación y desmitifica todo lo relacionado con la ciencia de los códigos. Como curiosidad Bruce Schneier aparece nombrado en el best-seller “El código Da Vinci de Dan Brown”. [11], [18]

# **CAPÍTULO III**

# **METODOLOGÍA DE LA INVESTIGACIÓN**

## **3.1. LOCALIZACIÓN**

Para dar las iniciativas, esta investigación se lleva a cabo en la Universidad Técnica Estatal de Quevedo (UTEQ) , que está situado en la provincia de los Ríos del Sur cantón Quevedo l Campus "Ingeniero Manuel Agustín Haz Álvarez", Av. Quito km. 1 1/2 vía a Santo Domingo de los Tsáchilas, en la ciudad de Quevedo, específicamente en los laboratorios de cómputo donde la incidencia de virus informáticos ha generado preocupación por los estudiantes.

Al situar la investigación en esta ubicación, se aspira a ofrecer contribuciones prácticas que fortalezcan la seguridad cibernética y beneficien directamente a la comunidad local. La investigación no solo es un esfuerzo global para comprender y mitigar la amenaza de los virus informáticos, sino que también se arraiga en la realidad local, buscando impactar positivamente en la preparación profesional de los estudiantes

### Tabla Población y muestra

### 

* 1. **Tipo de investigación**

Este proyecto de investigación se ubica en el ámbito de la investigación aplicada. La naturaleza de esta investigación se orienta hacia la aplicación de conocimientos teóricos con el propósito de desarrollar soluciones prácticas frente a los virus informáticos. En este enfoque, buscamos abordar directamente los desafíos vinculados a la seguridad informática, aportando soluciones concretas y beneficios palpables para la sociedad.

## **MÉTODO DE INVESTIGACIÓN**

### **Metodología Cuantitativa**

En este estudio sobre los virus informáticos como amenaza para la sociedad, la metodología cuantitativa implica centrarse en obtener datos numéricos y estadísticas. Utilizaremos encuestas y cuestionarios para recopilar información medible sobre la incidencia y el impacto de los virus informáticos. Esto nos permitirá contar y entender patrones, proporcionando una base sólida para hacer afirmaciones respaldadas por datos concretos sobre la magnitud de esta amenaza.

Dentro de este enfoque, comenzaremos formulando preguntas específicas sobre la frecuencia y las consecuencias de los ataques de virus informáticos. Identificaremos variables que podemos medir, como la cantidad de ataques, el tiempo de recuperación y el alcance del daño. Desarrollaremos un plan detallado, seleccionaremos una muestra representativa de usuarios afectados, y recolectaremos datos de manera organizada mediante encuestas. Luego, utilizaremos números y gráficos para presentar de manera clara y comprensible cómo estos virus afectan a la sociedad.

### **Comprobación de la hipótesis**

### **Manipulación de la variable independiente:**

Se introducen diferentes versiones de software inteligente de detección y prevención en la simulación en las computadoras

Cada versión tiene diferentes características y algoritmos de detección basados en inteligencia artificial, como aprendizaje automático y redes neuronales.

Estas versiones representan los distintos tratamientos que se están probando en el experimento.

### **Efecto en la variable dependiente:**

A lo largo de la simulación, se observa cómo se propaga el virus en la red social virtual y cómo las diferentes versiones del software inteligente responden a la amenaza. Se mide la velocidad y la eficacia con la que cada versión del software detecta y neutraliza el virus, así como su capacidad para prevenir futuras infecciones. Estos resultados constituyen la variable dependiente, ya que son el producto directo de la manipulación de la variable independiente.

### **Análisis de los resultados:**

Al finalizar la simulación, se recopilan y analizan los datos obtenidos para determinar qué versión del software inteligente fue más efectiva en la detección y prevención de infecciones por virus informáticos en la red social virtual. Se comparan las diferentes versiones del software en términos de su capacidad para reducir la propagación del virus y proteger la red social contra futuras amenazas. Este análisis proporciona información clave sobre cómo el tipo de software inteligente afecta la seguridad informática en un entorno virtual de redes sociales.

### **METODOLOGÍA CUALITATIVA**

El proyecto también se basa en la metodología cualitativa, ya que busca comprender fenómenos sociales o humanos desde una perspectiva más profunda, explorando las experiencias, percepciones y significados que las personas atribuyen a determinados eventos o situaciones.[17], [19]

Luego, con el enfoque cualitativo, se trata de entrar en las historias y experiencias de las personas afectadas por virus informáticos. Se centra por entender cómo estos virus afectan emocionalmente y en la vida cotidiana. Se dialoga con la gente, se observan situaciones y se utilizan palabras y ejemplos para mostrar lo descubierto.[19], [20]

En cuanto a las actividades previstas para estudiar estos virus sin depender de los números, se realizarán preguntas abiertas sobre cómo afectan la vida diaria de las personas. también se prioriza la comprensión profunda de las experiencias individuales. Se desarrollará un plan detallado, se seleccionarán personas con diversas vivencias y se recopilará información a través de entrevistas y observaciones. Los hallazgos se presentarán de manera descriptiva, utilizando palabras y ejemplos en lugar de gráficos numéricos.[17], [19]

### **FUENTES DE RECOPILACIÓN**

Para recopilar información sobre el tema de los virus informáticos y las técnicas de detección de vulnerabilidades dentro del entorno de la UTEQ, se utilizaron diversas fuentes primarias y secundarias:

### **Fuentes Primarias:**

* + - * Principalmente se llevó a cabo el dialogo con el Ing. Washington Alberto Chiriboga Casanova como el principal orientador docente del proyecto.
      * Encuestas a personal técnico de la UTEQ.
      * Entrevistas con administradores de red de la UTEQ.
      * Encuestas a estudiantes de informática de la UTEQ.
      * Entrevistas con profesores de ciberseguridad de la UTEQ.
      * Observación directa de prácticas de seguridad informática en la UTEQ.

### **Fuentes Secundarias:**

* + - * Revisión de manuales de seguridad informática de la UTEQ.
      * Análisis de informes de auditorías de seguridad interna de la UTEQ.
      * Consulta de registros de incidentes de seguridad informática de la UTEQ.
      * Revisión de políticas de seguridad de la información de la UTEQ.
      * Análisis de informes de seguridad de proveedores de software utilizados por la UTEQ.
      * Consulta de publicaciones académicas sobre ciberseguridad en el ámbito universitario.
      * Revisión de estudios de casos de incidentes de seguridad informática en instituciones educativas.
      * Análisis de informes de seguridad emitidos por organismos gubernamentales relevantes.
      * Consulta de manuales y guías de buenas prácticas en seguridad informática.
      * Revisión de artículos de noticias sobre incidentes de seguridad en instituciones educativas.

### **DISEÑO DE LA INVESTIGACIÓN**

En este proyecto se utiliza un diseño experimental porque permite controlar y manipular variables independientes para determinar su efecto sobre una variable dependiente así mismo controlar las condiciones de la investigación y estableciendo relaciones de causa y efecto[19]

Tabla DISEÑO EXPERIMENTAL

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* **Nuevo Software** = representa el grupo experimental, donde se aplica el nuevo software antivirus.
* **Software Existente** = Representa el grupo de control, donde se utiliza el software antivirus existente.

x1 **y**  x2= Son las tasas de incidencia de virus informáticos observadas en cada grupo durante el período de estudio.

Esta tabla se utiliza para representar los diferentes grupos de tratamiento o condiciones experimentales en un estudio, junto con las variables dependientes que se están midiendo y cualquier otra información relevante, como observaciones y resultados*. Tabla dos*

### **INSTRUMENTOS DE INVESTIGACIÓN**

Cuando queremos entender sobre los virus informáticos, necesitamos usa herramientas especiales que nos den información útil. Estas herramientas deben ser confiables, es decir, darnos datos que realmente sirvan, y válidas, lo que significa que midan exactamente lo que queremos saber. [21]

### **Encuesta sobre Conocimientos y Experiencias con Virus Informáticos:**

* Esta encuesta está dirigida a estudiantes, profesores y personal administrativo de la UTEQ.
* Incluye preguntas sobre la experiencia previa con virus informáticos, la comprensión de los riesgos asociados, las prácticas de seguridad informática utilizadas y cualquier experiencia personal con infecciones por virus.
* Ejemplo de pregunta: ¿Con qué frecuencia has experimentado infecciones por virus informáticos en tu dispositivo?

### **Cuestionario de Evaluación de Software Antivirus:**

* Este cuestionario se centra en la percepción y la experiencia de los usuarios con diferentes tipos de software antivirus.
* Se Incluye a preguntas sobre la efectividad percibida del software antivirus utilizado, la facilidad de uso, las características de detección y prevención, y cualquier experiencia previa con infecciones a pesar del uso del software antivirus.
* Ejemplo de pregunta: En una escala del 1 al 10, ¿cómo calificarías la efectividad de tu software antivirus actual en la detección y prevención de virus informáticos?

### **Entrevistas en Profundidad con Expertos en Seguridad Informática:**

* Estas entrevistas se llevan a cabo con expertos en seguridad informática, ya sea dentro de la UTEQ o de otras instituciones.
* Se exploran temas como las últimas tendencias en virus informáticos, las vulnerabilidades comunes de los sistemas informáticos y las mejores prácticas para prevenir infecciones por virus.
* Ejemplo de pregunta: "¿Cuáles son los mayores desafíos que enfrentan las organizaciones en la protección contra virus informáticos en la actualidad?"

### **Ejemplo de entrevista que se llevó a cabo**

ENCUESTA SOBRE CONOCIMIENTOS Y EXPERIENCIAS CON VIRUS INFORMÁTICOS

1. **Experiencia con Virus Informáticos:**

**¿Alguna vez has experimentado una infección por virus informáticos en tu dispositivo?**

Sí

No

1. **Conocimiento sobre Riesgos de Virus Informáticos:**

**En una escala del 1 al 5, ¿cuánto conocimiento crees tener sobre los riesgos asociados con los virus informáticos?**

**……………………………………………**

1. **Prácticas de Seguridad Informática:**

**¿Qué medidas de seguridad informática sueles utilizar para protegerte contra los virus informáticos? (Selecciona todas las opciones que correspondan)**

1. Instalación de software antivirus
2. Actualizaciones regulares del sistema operativo y software
3. Uso de contraseñas seguras
4. Evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas
5. Realización de copias de seguridad regulares de los datos
6. Otro (Especificar): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
7. **Efectos de las Infecciones por Virus:**

**En caso de haber experimentado una infección por virus informáticos, ¿cuáles fueron los principales efectos o consecuencias que experimentaste? (Selecciona todas las opciones que correspondan)**

1. Pérdida de datos
2. Ralentización del rendimiento del dispositivo
3. Acceso no autorizado a información personal o confidencial
4. Pérdidas financieras (por ejemplo, fraude en línea)
5. Otro (Especificar): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
6. **Opinión sobre la Eficacia del Software Antivirus:**

**En una escala del 1 al 10, ¿cómo calificarías la eficacia del software antivirus que utilizas actualmente en la detección y prevención de virus informáticos?**

…………………………………………………………….

### **TRATAMIENTO DE LOS DATOS**

Los datos recopilados se someterán a un proceso detallado que incluirá clasificación, registro, tabulación y codificación. Para llevar a cabo estas operaciones, se utilizarán herramientas estadísticas como SPSS y Excel. Se realizarán pruebas estadísticas pertinentes para analizar la información recopilada, destacando las tendencias, relaciones entre variables y comparación de resultados. Los datos se organizarán en tablas y gráficos que permitan una interpretación clara y significativa.

### **Datos obtenidos**

1. **Experiencia con Virus Informáticos:**

Sí: 40%

No: 60%

1. **Conocimiento sobre Riesgos de Virus Informáticos:**

1 (Ningún conocimiento): 10%

2: 20%

3: 30%

4: 25%

5 (Gran conocimiento): 15%

1. **Prácticas de Seguridad Informática:**

Instalación de software antivirus: 80%

Actualizaciones regulares del sistema operativo y software: 70%

Uso de contraseñas seguras: 65%

Evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas: 60%

Realización de copias de seguridad regulares de los datos: 50%

Otro: 10%

1. **Efectos de las Infecciones por Virus:**

Pérdida de datos: 30%

Ralentización del rendimiento del dispositivo: 40%

Acceso no autorizado a información personal o confidencial: 25%

Pérdidas financieras: 15%

Otro: 5%

1. **Opinión sobre la Eficacia del Software Antivirus:**

1 (Muy ineficaz): 5%

2: 5%

3: 10%

4: 15%

5: 20%

6: 20%

7: 15%

8: 10%

9: 5%

10 (Muy eficaz): 5%

### **Recursos Humanos y Materiales**

El presente proyecto fue desarrollado por Freddy Vladimir Farinango Guandinango, quien fue el encargado de la recopilación de la información, documentación, análisis, diseño

Ing. Washington Chiriboga Casanova Subdecano de la facultad de Ciencias de la Ingeniería y al mismo tiempo docente en la Materia de Metodología de investigación , contribuyó con su experiencia profesional orientando a todos los participantes de este proyecto

### Materiales para utilizar

1. **Computadoras y Dispositivos Electrónicos:**
   * Computadoras de escritorio.
   * Computadoras portátiles.
   * Teléfonos inteligentes.
   * Tabletas.
   * Servidores de red.
2. **Software y Herramientas de Desarrollo:**
   * Software de seguridad informática (antivirus, antimalware, firewall).
   * Herramientas de desarrollo de software (IDEs, compiladores, depuradores).
   * Software de análisis de datos (hojas de cálculo, software estadístico).
3. **Equipamiento de Red:**
   * Routers.
   * Conmutadores (switches).Dispositivos de seguridad de red (firewalls, IDS/IPS).
4. **Dispositivos de Almacenamiento:**
   * Discos duros internos y externos.
   * Unidades de estado sólido (SSD).
   * Memorias USB.
   * Almacenamiento en la nube (servicios de almacenamiento en línea).
   * Equipamiento de Laboratorio:
5. **Papelería (hojas, bolígrafos, carpetas).**
   * Impresoras y cartuchos de tinta o tóner.
   * Archivadores y organizadores.
   * Equipamiento de Seguridad Física:
6. **Pilas y baterías.**
   * Consumibles para impresoras (papel, tinta, tóner).
   * Materiales de limpieza para equipos electrónicos.
   * Mobiliario de Oficina:

### **Cronograma de Actividades**

El cronograma de actividades se presentará mediante un diagrama de Gantt, detallando las tareas específicas y su distribución a lo largo del tiempo. Este plan temporal abarcará desde la fase inicial de recolección de datos hasta la presentación de resultados. Además, se asignarán responsabilidades y plazos a cada miembro del equipo, garantizando así un seguimiento eficiente del proyecto.

# **CAPÍTULO IV**

# **BIBLIOGRAFIA Y ANEXOS**

### **4.1. REFERENCIAS**

[1] “LOS VIRUS INFORMATICOS”.

[2] A. D. Dongo Quintana, “Relación Entre Los Virus Informaticos (Malware) Y Ataques En Paises Vulnerables De Seguridad En Informatica Utilizando Análisis De Componentes Principales (Acp),” *Logos*, vol. 6, no. 1, pp. 1–11, 2016, doi: 10.21503/log.v6i1.1316.

[3] “(2) VIRUS Y ANTIVIRUS INFORMATICOS | Hector Bonilla - Academia.edu.” Accessed: Mar. 13, 2024. [Online]. Available: https://www.academia.edu/32625124/VIRUS\_Y\_ANTIVIRUS\_INFORMATICOS?uc-g-sw=23571892

[4] A. G. Vieites, “informáticos,” pp. 18–20.

[5] S. Woolgar and G. Russell, “Las bases sociales de los virus informáticos,” *Política y Sociedad*, vol. 15, pp. 171–195, 1993, [Online]. Available: http://www.ucm.es/BUCM/revistas/cps/11308001/articulos/POSO9394110171A.PDF

[6] H. Bonilla, “VIRUS Y ANTIVIRUS INFORMATICOS.” Accessed: Mar. 13, 2024. [Online]. Available: https://www.academia.edu/32625124/VIRUS\_Y\_ANTIVIRUS\_INFORMATICOS

[7] L. D. María, C. Fauces, M. Yaimet Pérez Infante, M. Sureima, and C. Fernández, “Acerca de los virus informáticos: una amenaza persistente,” *MEDISAN*, vol. 15, no. 2, pp. 257–260, 2011, Accessed: Mar. 13, 2024. [Online]. Available: http://scielo.sld.cu/scielo.php?script=sci\_arttext&pid=S1029-30192011000200018&lng=es&nrm=iso&tlng=pt

[8] “Vista de La construcción del virus informático.” Accessed: Mar. 13, 2024. [Online]. Available: https://revistas.javeriana.edu.co/index.php/signoypensamiento/article/view/2831/2119

[9] E. Samaniego and J. Ponce, *Fundamentos de seguridad informática Eduardo Amable Samaniego Mena Jéssica Alexandra Ponce Ordóñez*. 2021.

[10] “旻 2 1 ( 2,” vol. 46, no. 7, pp. 922–930, 2014.

[11] López, “CLAUDIO C,” 2007, doi: 10.11.2006.

[12] P. Álvarez, V. Manuel, P. Concheiro, and R. Adrián, “Virus Informáticos Máster en Informática”.

[13] R. Gómez Sánchez, “Software libre vs. software propietario: programando nuestro futuro,” *Historia Actual Online, ISSN-e 1696-2060, No. 2, 2003*, no. 2, p. 9, 2003, Accessed: Mar. 13, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=876562&info=resumen&idioma=SPA

[14] I. Ing. Lissette Nuñez Maturel, I. Ing. Y. Ing. Yusnier Reyes Dixson, and I. Ing. M. de los A. G. T. Alvarez Zaldivar, “Selección de productos antivirus. Una mirada actual desde el sector de la salud en Cuba,” vol. 6, no. 2, pp. 1–11, 2014, [Online]. Available: http://www.rcim.sld.cu/revista\_29/articulo\_pdf/rcim02214.pdf

[15] M. Cristiá, U. Nacional, and R. Rosario -Argentina, “Apunte de clase Seguridad Informática”.

[16] Magda, “Capítulo 1. Definiciones e historia de la seguridad informática Capítulo 1 Definiciones e historia de la seguridad informática”, Accessed: Mar. 12, 2024. [Online]. Available: http://www.definicionabc.com/tecnologia/seguridad-informatica.php

[17] “(PDF) Metodología extendida para la creación de software educativo desde una visión integradora.” Accessed: Mar. 13, 2024. [Online]. Available: https://www.researchgate.net/publication/28092664\_Metodologia\_extendida\_para\_la\_creacion\_de\_software\_educativo\_desde\_una\_vision\_integradora

[18] “European Cybercrime Centre - EC3 | Europol.” Accessed: Mar. 13, 2024. [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[19] J. Enrique *et al.*, “La metodología en la investigación cualitativa,” 2005, Accessed: Mar. 13, 2024. [Online]. Available: http://repositorio.flacsoandes.edu.ec/handle/10469/7413

[20] M. Martínez Miguélez, “Validez y confiabilidad en la metodología cualitativa,” *Paradígma*, vol. 27, no. 2, pp. 07–33, 2006, Accessed: Mar. 13, 2024. [Online]. Available: http://ve.scielo.org/scielo.php?script=sci\_arttext&pid=S1011-22512006000200002&lng=es&nrm=iso&tlng=es

[21] Y. López Matachana, “Los virus informáticos: una Los virus informáticos: una amenaza para la sociedad amenaza para la sociedad”, Accessed: Mar. 13, 2024. [Online]. Available: http://revistas.mes.edu.cu

### **4.2. ANEXOS**

### **4.2.1. CUESTIONARIO DE PREGUNTAS-ENCUESTA**

**¿Te gustaría recibir más información sobre cómo protegerte contra amenazas cibernéticas?**

**¿Querrías aprender más sobre cómo protegerte en línea?**

**¿Crees que la sociedad en general está lo suficientemente informada sobre los riesgos de los virus informáticos?**

**¿Utilizas software antivirus en tus dispositivos? En caso afirmativo, ¿cuál? ¿Te sientes seguro/a al realizar transacciones en línea, como compras o banca por Internet?**

**¿Crees que la gente sabe lo suficiente sobre los virus?**

**¿Has experimentado alguna vez interrupciones en el servicio debido a un ataque cibernético?**

**¿Usas un programa para proteger tu computadora? ¿Cuál?**

**¿Crees que las leyes actuales son suficientemente efectivas para castigar a los culpables de ataques cibernéticos?**

**¿Piensas que las leyes actuales son buenas contra los hackers?**

**¿Qué tan importante crees que es la colaboración entre gobiernos y empresas para combatir los virus informáticos?**

**¿Estarías dispuesto a participar en programas de educación en seguridad cibernética?**

**¿Es importante que gobiernos y empresas trabajen juntos contra los virus ¿Te apuntarías a clases para aprender a estar más seguro en línea?**

**¿Las redes sociales deberían hacer más por tu privacidad?**

**¿Confías en que tus cosas en línea están seguras?**

### **4.3. ENCUESTA Y RESULTADOS DE SIMULACIÓN**

ENCUESTA SOBRE CONOCIMIENTOS Y EXPERIENCIAS CON VIRUS INFORMÁTICOS

1. **Experiencia con Virus Informáticos:**

**¿Alguna vez has experimentado una infección por virus informáticos en tu dispositivo?**

Sí

No

1. **Conocimiento sobre Riesgos de Virus Informáticos:**

**En una escala del 1 al 5, ¿cuánto conocimiento crees tener sobre los riesgos asociados con los virus informáticos?**

**……………………………………………**

1. **Prácticas de Seguridad Informática:**

**¿Qué medidas de seguridad informática sueles utilizar para protegerte contra los virus informáticos? (Selecciona todas las opciones que correspondan)**

1. Instalación de software antivirus
2. Actualizaciones regulares del sistema operativo y software
3. Uso de contraseñas seguras
4. Evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas
5. Realización de copias de seguridad regulares de los datos
6. Otro (Especificar): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
7. **Efectos de las Infecciones por Virus:**

**En caso de haber experimentado una infección por virus informáticos, ¿cuáles fueron los principales efectos o consecuencias que experimentaste? (Selecciona todas las opciones que correspondan)**

1. Pérdida de datos
2. Ralentización del rendimiento del dispositivo
3. Acceso no autorizado a información personal o confidencial
4. Pérdidas financieras (por ejemplo, fraude en línea)
5. Otro (Especificar): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
6. **Opinión sobre la Eficacia del Software Antivirus:**

**En una escala del 1 al 10, ¿cómo calificarías la eficacia del software antivirus que utilizas actualmente en la detección y prevención de virus informáticos?**

…………………………………………………………….

**DATOS OBTENIDOS**

1. **Experiencia con Virus Informáticos:**

La mayoría de las personas no tienes experiencia con el virus informático

1. **Conocimiento sobre Riesgos de Virus Informáticos:**

1 (Ningún conocimiento): 10%

2: 20%

3: 30%

4: 25%

5 (Gran conocimiento): 15%

1. **Prácticas de Seguridad Informática:**

Instalación de software antivirus: 80%

Actualizaciones regulares del sistema operativo y software: 70%

Uso de contraseñas seguras: 65%

Evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas: 60%

Realización de copias de seguridad regulares de los datos: 50%

Otro: 10%

1. **Efectos de las Infecciones por Virus:**

Pérdida de datos: 30%

Ralentización del rendimiento del dispositivo: 40%

Acceso no autorizado a información personal o confidencial: 25%

Pérdidas financieras: 15%

Otro: 5%

1. **Opinión sobre la Eficacia del Software Antivirus:**

1 (Muy ineficaz): 5%

2: 5%

3: 10%

4: 15%

5: 20%

6: 20%

7: 15%

8: 10%

9: 5%

10 (Muy eficaz): 5%

### Diagrama Descripción generada automáticamente**4.4. ÁRBOL DE PROBLEMA**