Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real

Juan David Argoti Puchana, juanargoti2015@hotmial.com

Informe final como requisito para optar al título de Ingeniero de sistemas

Asesor: Luis Arnoby Escobar Hernández Mg. En seguridad Informática

Universidad CESMAG
Facultad de Ingeniería de Sistemas
San Juan de Pasto
2024

DEDICATORIA

A Dios,

El guía de mi vida y la fuente de todo entendimiento y fortaleza, en humildad y gratitud dedico este logro a ti. A lo largo de este viaje de aprendizaje y crecimiento, has sido mi luz en la oscuridad, fortaleza en la debilidad, inspiración en los momentos de dudas. Tu amor incondicional y tu gracia me han sostenido a lo largo de esta travesía

A mis padres,

Aquellos que nos brindaron su apoyo inquebrantable, su amor incondicional y su constante inspiración a lo largo de esta ardua travesía académica. Sin su guía y aliento, esta tesis no hubiera sido posible, sus palabras fueron inspiradoras para seguir adelante con nuestras metas, fue un camino largo y con muchos obstáculos, pero gracias a ustedes di el mayor esfuerzo sin parar en ningún momento y sin dar marcha atrás.

A mi amigo de Investigación Luis Gabriel Molina Córdoba,

Por su paciencia, comprensión, apoyo, sus palabras alentadoras, sus consejos sabios, fueron lo que me impulsó a seguir adelante incluso en los momentos más difíciles.

A nuestros docentes y asesores,

Quiero expresar mi más profundo agradecimiento por su dedicación y paciencia y la orientación a lo largo de este arduo proceso de investigación, vuestra sabiduría y apoyo incondicional fueron lo que me ayudaron a guiarme al camino del éxito para culminar el gran viaje académico. Sus lecciones, críticas constructivas y compromiso con el crecimiento intelectual han sido invaluables. Sin su guía experta y su fomento constate esta tesis no habría alcanzado las alturas que han logrado

Dedicatoria en memoria de Olga Lucia Puchana Zambrano

A Olga Lucia Puchana Zambrano

Aunque ya no está físicamente presente, tu influencia y tú legado perdurará en mi corazón, siempre recordaré que tu apoyo, tu pasión por el conocimiento y tu apoyo inquebrantable fueron fuentes de inspiración en este viaje, esta tesis es un tributo a tu memoria y a todo lo que me enseñó, cada idea está plasmada en estas palabras son un reflejo de tu impacto en mi vida.
Descansa en paz, te recordaré con cariño y agradecimiento

Esta tesis es un reflejo de mi compromiso con la excelencia académica y de la gratitud que siento hacia todos aquellos que me han apoyado.

Juan David Argoti Puchana
San Juan de pasto, 2024

AGRADECIMIENTOS

En primer lugar, doy gracias a Dios por brindarme la sabiduría y la salud para salir adelante en el desarrollo de mi profesión y poder culminar el trabajo de grado, a todos nuestros amigos por compartir sus conocimientos, experiencias y amistad fueron la base para este proceso, a nuestros docentes y asesores, su guía experta, sabiduría y apoyo constante fueron fundamentales en la realización de esta investigación, sus orientaciones fueron cruciales para nuestro crecimiento académico. A mis familiares y seres queridos Su gran apoyo incondicional, paciencia y el amor para lograr esta gran travesía, la confianza que me brindaron fue la motivación la colaboración y el apoyo moral fue lo que me ayudó a culminar este gran desafío.

Este logro no hubiera sido posible sin la ayuda de cada uno de ustedes, Ahora me enfrento a un nuevo mundo lleno de virtudes y nuevos desafíos y de grandes oportunidades para mejorar la calidad de vida y la de los demás.
A ustedes les expreso mi más sincero agradecimiento.

Juan David Argoti Puchana
San Juan de pasto, 2024

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

NOMBRE JURADO 1

_____

NOMBRE JURADO 2

San Juan de Pasto, 2024

NOTA DE EXCLUSIÓN

El autor de esta obra es el único responsable
de las ideas expresadas en ella, y esta no refleja o no compromete la ideología de la Universidad Cesmag.

RESUMEN ANALÍTICO

La investigación titulada “Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real”. La meta principal es asegurar que estos dispositivos cumplan con los estándares mínimos de seguridad establecidos utilizando parámetros derivados de la norma ISO 27001 conforme a su estado de seguridad.

La investigación busca abordar la importancia de verificar y garantizar que los equipos cumplan con requisitos de seguridad específicos. La utilización de pruebas en un entorno real agrega un nivel adicional de validez y relevancia a la evaluación, ya que con la práctica proporciona resultados más cercanos a los entornos reales.

El software propuesto se desarrolla para aplicar pruebas de validación referente a criterios de seguridad para asegurar la eficacia y la confiabilidad del software. La generación de un reporte permitirá a los usuarios obtener una visión clara y detallada del estado de seguridad de los equipos, facilitando la toma de decisiones.

Es esencial destacar que la norma ISO 27001 proporciona un marco de referencia ampliamente reconocido para la gestión de la seguridad de la información. Por lo tanto, la utilización de parámetros derivados de esta normativa garantiza que las evaluaciones de seguridad, además de la eficacia y la confiabilidad, el software también se enfoca en la usabilidad y accesibilidad para los usuarios, se desarrolla una interfaz intuitiva que permita a los usuarios efectuar fácilmente las pruebas y comprender los resultados.

Se espera que los resultados de este estudio contribuyan significativamente a fortalecer la seguridad de los dispositivos en diversas situaciones, proporcionando una herramienta eficaz y confiable para evaluar y mejorar continuamente la seguridad de la información.

Palabras clave: Validación, seguridad, pruebas, entorno real, equipos, Norma ISO 27001

TABLA DE CONTENIDO

LISTA DE GRÁFICAS

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Los equipos electrónicos, su correspondiente software están presentes en numerosos sectores, como la industria, la medicina, las comunicaciones y el transporte, entre otros. En la era actual, donde la tecnología avanza a pasos agigantados juega con un papel fundamental en todos los aspectos de la vida, la seguridad de los equipos, los sistemas se han convertido en una preocupación de vital importancia. Sin embargo, la creciente complejidad y sofisticación de estos sistemas ha dado lugar a un incremento en los riesgos y vulnerabilidades asociados.

Es esencial garantizar que estos equipos funcionen en un estado de seguridad óptimo, ya que un fallo en su operación podría tener consecuencias graves, como pérdida de datos, interrupción de servicios críticos o incluso daños físicos. Por lo tanto, la validación de los estados de seguridad en estos equipos se ha convertido en una tarea fundamental para garantizar su correcto funcionamiento, según la investigación realizada por Parra Barzola Liliana Milagros, Yánez Cedeño Erick Steven "Tiene como objeto general realizar pruebas de vulnerabilidades para identificar las amenazas de seguridad en la red, verificar el acceso para que los usuarios no puedan robar información confidencial y vital para el funcionamiento de la empresa" [1] esta investigación utiliza el análisis de la metodología abierta de testeo de seguridad el cual permite mirar las fases a revisar.

En este contexto, desarrollar un software especializado que permita llevar a cabo pruebas de validación de estados de seguridad en entornos reales, se pueden clasificar las condiciones o configuraciones específicas de un sistema, red o aplicación en un momento dado, estos estados pueden varias según la configuración, el acceso a usuarios, mantener registros y seguir buenas prácticas de gestión de cambios es esencial para mantener la integridad y la seguridad de los sistemas y datos en un entorno cibernético en pocas palabras un estado puede ser abierto, cerrado, cumple o no cumple un cierto criterio definido.

La validación de estados en entornos reales es una parte fundamental de cualquier proceso de

desarrollo de software, la validación de estados en entornos reales se refiere a la verificación y pruebas de un sistema en situaciones del mundo real en un lugar de entornos controlados. Este software debe ser capaz de simular condiciones de funcionamiento reales y evaluar el comportamiento de los equipos ante posibles amenazas o situaciones de riesgo. De esta manera, se busca detectar debilidades en los sistemas.

El proyecto de investigación se orientó en desarrollar un software de validación de estados de seguridad Según Teruel, David [2] el incremento de los riesgos asociados como ataques o amenazas propone un enfoque de monitorización para detectar las amenazas conforme a las Auditorías de seguridad y las políticas de ciberseguridad, de tal forma que el desarrollo de validación de estados en los equipos sea eficiente, confiable y escalable. Para lograrlo, se seguirá un enfoque metodológico que involucra el análisis de requisitos, el diseño de arquitectura, la implementación del software y la evaluación de su desempeño. Además, se aplicarán pruebas en entornos reales, a fin de obtener resultados precisos y robustos.

Se estructurará en varios capítulos, donde se abordarán los aspectos teóricos y prácticos relacionados con la validación de estado de seguridad en equipos. Asimismo, se presentarán los resultados obtenidos durante la implementación del software y se discutirán las conclusiones y posibles recomendaciones para futuros trabajos en este campo.

1. PROBLEMA DE INVESTIGACIÓN

1.1 Objeto o tema de investigación

Desarrollo de un software que permita identificar vulnerabilidades y estados para ofrecer apoyo en Auditoría de seguridad, en los equipos mediante pruebas realizadas en un entorno real.

1.2 Línea de Investigación

Seguridad informática se entiende como: "Seguridad de la información. Es la disciplina que, con base en políticas y normas internas y externas, se encarga de proteger la integridad, privacidad y disponibilidad de la información, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta, abarcando información en medios físicos y digitales. [3].

1.3 Sub línea de Investigación

Seguridad informática "La seguridad informática enmarca todos los métodos y controles tecnológicos que se pueden implementar con el fin de mitigar el riesgo relacionado a las amenazas cibernéticas que pueden comprometer la privacidad, integridad o confidencialidad de los sistemas de información, incluyendo la transmisión y almacenamiento de la información tratada por los mismos, entre las principales amenazas se encuentran: Infección por malware, ataques de denegación de servicio, suplantación de identidades, errores de los usuarios, interceptación de las comunicaciones, entre otros". [3].

1.4 Planteamiento del problema

En el ámbito de la seguridad de los equipos informáticos y sistemas tecnológicos, existen desafíos significativos para garantizar su correcto funcionamiento y protección contra posibles amenazas y riesgos. Por lo general, las pruebas de seguridad se realizan en entornos simulados, según el estudio del Ponemon Institute, el 73% de las organizaciones realizan pruebas de seguridad en un entorno simulado [4], lo que limita su capacidad para reflejar las condiciones reales de su operación y los escenarios de amenazas potenciales.

Estas pruebas en entornos simulados no proporcionan una evaluación completa de los estados de seguridad de los equipos, lo que puede resultar en la falta de detección de vulnerabilidades, debilidades reales. Así mismo, el proceso de prueba manual puede ser de costos en término de tiempo, recurso y no garantiza una cobertura exhaustiva de todas las posibles situaciones de riesgo, según Omar Camilo Santiago García [5] tiene como objetivo utiliza la metodología OWASP para identificar vulnerabilidades en la validación de la seguridad, el diseño, la operación de aplicaciones web seguras, con el fin de verificar las posibles vulnerabilidades que se pueden presentar.

Por lo tanto, el problema radica en la necesidad de desarrollar un software de validación de estados de seguridad en los equipos que permitan realizar en entorno real, superando las limitaciones de las pruebas en entornos simulados, optimizando el tiempo los recursos utilizados en el proceso de validación. Este software deberá proporcionar una evaluación precisa, exhaustiva de los estados de seguridad de los equipos, identificando posibles vulnerabilidades y debilidades de manera temprana y eficiente.

Se centra en la falta de una solución adecuada y efectiva para validar los estados de seguridad de los equipos en condiciones reales, así como la continuidad de las operaciones de las organizaciones. Según Giraldo Ramírez las amenazas de ciberseguridad son riesgos potenciales que tiene como objetivo explotar vulnerabilidades en los sistemas informáticos para comprometer la confidencialidad, integridad o disponibilidad de los datos, son iguales para

grandes y pequeñas empresas, los riesgos y las técnicas de prevención y mitigación son diferente, su objetivo principal es comprometer la seguridad de la información y dañar los sistemas. [6] Un problema común en la seguridad informática de las empresas es la falta de recursos y conocimientos especializados para auditar y mantener una base de buenas prácticas. La falta de herramientas efectivas puede hacer que las personas no sepan de vulnerabilidades, poniendo en peligro la seguridad de las empresas

1.5 Formulación del problema

¿Cómo fortalecer la validación de estados de seguridad en equipos de cómputo, mediante la implantación de pruebas basadas en la norma ISO 27001?

1.6 Objetivos

1.6.1 Objetivo General

Fortalecer la validación de estados mediante un software que permita evaluar la seguridad e integridad de los sistemas informáticos y de la información en pruebas de entorno real.

1.6.2 Objetivos específicos

- Analizar las herramientas y técnicas necesarias para comprender los diferentes tipos de estados de seguridad que pueden afectar a los sistemas informáticos.
- Desarrollar un software que permite analizar partes básicas del sistema operativo y la red en busca de estados, siguiendo las mejores prácticas de seguridad basados en la norma ISO 27001.
- Validar la efectividad del software mediante pruebas aplicadas en un entorno real.

1.7 Justificación

La creciente importancia de la ciberseguridad y la protección de datos en el entorno tecnológico actual muestran la urgente necesidad de abordar las ciberamenazas relacionadas con la creciente dependencia de sistemas y equipos técnicos. Si bien a pesar del aumento de estas amenazas, las soluciones actuales de verificación de seguridad a menudo carecen de la precisión y agilidad necesarias para modelar escenarios de riesgos en entornos del mundo real. Importante para prevenir riesgos de seguridad. Verificar la postura de seguridad se convierte en una parte importante para garantizar que los dispositivos cumplan con los estándares, regulaciones y proporciona una capa adicional de protección contra las complejidades del entorno cibernético en constante cambio.

Para prevenir amenazas y riesgos, es importante garantizar el funcionamiento seguro y confiable de los equipos. La verificación de la posición de seguridad es importante para que el equipo cumpla con estándares establecidos. Un estudio de Gallardo Urbini Ignacio Martin, se centró en la planificación de la protección estática y propuso una nueva técnica relacionada con la ciberinteligencia. Las estrategias de defensa que se centran en la inteligencia se afinan para lograr la dinámica y la resolución de la red que lo permite comprender en un entorno hostil [7].

Las pruebas en entornos simulados son útiles para evaluar el comportamiento teórico de la computadora, pero no lo es. Reflejan siempre las condiciones de operación y las condiciones de amenaza potencial. Los entornos del mundo real son más complejos y requieren que el software se pruebe en condiciones del mundo real para identificar vulnerabilidades. Al comparar riesgos y evaluar respuestas, el software ayuda a fortalecer la seguridad, mejorar la confiabilidad y el rendimiento del sistema.

La justificación de este proyecto surge de la necesidad general de que las organizaciones cuenten con herramientas para gestionar el cumplimiento y estándares de seguridad cada vez más altos, así como para garantizar la integridad y continuidad de los datos. En situaciones en las que los

ciberataques pueden tener graves consecuencias, desarrollar un software de seguridad informática es una inversión. Esta implementación no es solo una respuesta a la urgencia de la prevención de amenazas sino también a la urgente necesidad de reducir los riesgos que puedan amenazar la estabilidad y seguridad de la organización en la situación actual.

1.9 Delimitación

La investigación se fundamenta en el desarrollo de un software para validación de seguridad informática, empleando métodos y técnicas prácticas de auditoría y pruebas en seguridad en situaciones de la vida real basadas en algunos controles de la Norma ISO 27001. La investigación tendrá una duración desde febrero del 2024 hasta junio del 2024, proceso en el cual se logrará cumplir con los propósitos propuestos.

2. MARCO TEÓRICO

2.1 Antecedentes

Los antecedentes destacan la creciente importancia de asegurar la integridad y la confiabilidad de los sistemas informáticos en un contexto de amenazas cibernéticas cada vez más sofisticadas. Examinando experiencias anteriores, se identifican limitaciones significativas en las herramientas de validaciones existentes, especialmente aquellas que se enfocan en entornos reales.

Han subrayado la necesidad de abordar las diferencias cruciales entre el comportamiento teórico y las condiciones reales de operación, resaltando la complejidad inherente de los entornos reales. Experiencias exitosas y casos de estudio han demostrado que las pruebas en entornos reales son fundamentales para identificar vulnerabilidades y debilidades de manera más precisa, además se observa una tendencia hacia el desarrollo de software de seguridad más dinámico y adaptable, basado en estrategias defensivas que incorporan operaciones de inteligencia, la evolución de normativas y estándares de seguridad también destacan la necesidad de soluciones avanzadas y validaciones más efectivas para cumplir con los requisitos en constante cambio.

2.1.2 Antecedentes Internacionales

El estudio denominado Análisis de vulnerabilidades en la red LAN usando herramientas de hacking ético para una empresa de la provincia de santa Elena, realizado por Suarez Panchana Lissette Carolina en el año 2021 en la ciudad la Libertad - Ecuador tiene como objetivo general, identificar las vulnerabilidades de la red de datos utilizando la metodología de Hacking Ético para mejorar la seguridad informática de la empresa. [8] Los métodos utilizados en el área de investigación son proporcionar una evaluación de las amenazas percibidas e idéntica, clasificar, priorizar las debilidades para responder adecuadamente. Los hallazgos proporcionan un método eficaz para identificar vulnerabilidades en redes de datos a través del hacking ético, que implica

investigación y desarrollo en el diseño de validación de pruebas en un entorno global para mejorar la seguridad informática de los equipos informáticos. Es un método más preciso y eficiente.

En este contexto en el estudio de la Propuesta De Una Implementación De Un Programa De Gestión De Vulnerabilidades De Seguridad Informática Para Mitigar Los Siniestros De La Información En El Policlínico De Salud Amc Alineado A La Ntp-Iso/Iec 27001:2014 En La Ciudad De Lima-2021 Realizada por Alber Alan Dávila Ángeles y Brian Jasón Dextre Alarcón en el año 2021 en Lima – Perú Como objetivo general la gestión de Vulnerabilidades contribuirá en lograr un óptimo Nivel de Seguridad en el policlínico AMC, se basa en contar con todos los controles y medidas sobre las entidades con la clave para la contención y protección en estas Situaciones la detección, análisis de las debilidades en AMC a través de herramientas de escaneos automatizados sobre la infraestructura de la entidad cuando se aplica una adecuada gestión de vulnerabilidades ya sean realizados a partir del inventario de los activos de la entidad, con el fin de informar que incidentes se afecta por cuestiones de actualización de parches de seguridad , actualización de equipos o descuidos en los usuarios. [9] Como conclusión de esta investigación de Dávila, enfatiza la importancia de una gestión efectiva de vulnerabilidades para alcanzar un alto nivel de seguridad informática, con esto se puede respaldar la investigación al destacar la necesidad de un software de validación de estados de seguridad que pueda identificar y abordar debilidades en equipos incluyendo problemas de actualizaciones de parches, vulnerabilidades en la infraestructura, su enfoque en la detección, análisis de debilidades proporciona una base sólida para el desarrollo de pruebas en entorno real.

En este sentido en el libro hacker´s White book escrito por Pablo Gutiérrez Salazar director general del WhiteSuit Hacking profesional en el área de pentesting, de la empresa de seguridad anti espionaje y creador de la certificación del curso G.H.O.S.T (Grey Hat Offensive Security technician) brinda los argumentos para convertirse en un hacker profesional, en el área de seguridad informática con el objetivo principal para guiar al área de seguridad, trabajado en el punto de vista técnico, usando las metodologías adecuadas para realizar las pruebas de penetración o de Auditoría de seguridad en distintos casos el libro está estructurado a base de

las metodologías internacional de penetración, la metodología que se utiliza es método científico, esencialmente se obtiene la información, se analiza luego se ataca, en base al alcance del ataque, reportara, dependiendo del objetivo, adicionalmente se verá un poco del análisis forense de formar superficial" [10]. Como conclusión el libro de Pablo Salazar proporciona una valiosa habilidad para convertirse en Hacker Profesional en seguridad informática, enfocándose en pruebas de penetración, Auditorías de seguridad, destacar la importancia de contar con un software de validación de seguridad que pueda aplicar metodologías sólidas como el método científico, para identificar abordar vulnerabilidades en entornos reales, además la mención de esta investigación se resalta que en la investigación utilizó un análisis forense completa el enfoque de seguridad informática de manera integral.

Además de esto el estudio de la investigación aplicaciones de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección de comunicación y criminalística de la policía de perú-huraz-2015 realizado por Frans Renzo de la Cruz Jo en Huaraz –Perú en el año 2017 el propósito principal de la investigación la aplicación de metodologías y herramientas, la informática forense para poder lograr reducir la inseguridad informática en esta investigación se resalta que en la investigación utilizó el análisis estadístico utilizando el instrumento del cuestionario a un número en específico en la dirección Nacional de Comunicaciones y Criminalística de la PNP. [11] Como conclusión en la investigación de Frans la importancia de la informática forense para reducir la inseguridad informática el uso de análisis estadístico a través de cuestionarios proporciona una perspectiva valiosa sobre las necesidades, preocupaciones de las organizaciones, esto ayuda a diseñar un software de validación de seguridad, efectivo al considerar las amenazas, debilidades específicas en el contexto real de las instituciones.

2.1.3 Antecedentes Nacionales

En el estudio denominado seguridad informática en el desarrollo de aplicaciones web mediante el uso de metodología OWASP, Realizada por Tania Sierra Huertas en el año 2023 en la ciudad de Bogotá - Colombia, su objetivo general trata establecer cuáles son las vulnerabilidades de

seguridad en el desarrollo de aplicaciones web a partir de metodología OWASP, la metodología que se empleó permite tener una visión que pueda valorar las variables con la seguridad la cual le permite darle calidad y permite realizar correcciones de software desarrollado. [12] Como conclusión de la investigación de Tania, la importancia de identificar vulnerabilidades en el desarrollo de aplicaciones Web mediante la metodología OWASP para mejorar la seguridad en entornos reales.

Con este propósito en el estudio de la investigación titulada Capacidades técnicas, legales y de gestión para equipos Blueteam y Redteam Realizada por Jorge Alirio Caballero Borda en el año 2020 en la ciudad de Bogotá – Colombia, su objeto principal "a través de un entorno de práctica, la forma de vulnerar el fallo de seguridad asociado a la falta de actualización del sistema operativo del computador" las herramientas y/o librerías que se utilizaron para este desarrollo son, Nmap, Metasploit, Firewall, Exploit, CVE, Antivirus y actualización o Parche de seguridad, con el fin de formular una cantidad de estrategias conforme a los análisis de las vulnerabilidades encontradas mediante los riesgos de las infraestructuras. [13] Como conclusión de la investigación de Jorge destaca la importancia de abordar las vulnerabilidades relacionadas con las actualizaciones del sistema operativo, surge la necesidad de validar la información de los equipos conforme a las actualizaciones y parches de seguridad faltantes.

Por lo tanto en la investigación titulada Análisis de amenazas y vulnerabilidades informáticas basados en la norma ISO 27002 en el proceso de citas del servidor web de una institución Realizada por Catuto Pilay y Richard Manuel en el año 2021 en la libertad –Ecuador su principal objetivo fue se basa en detectar amenazas, vulnerabilidades que se encuentran en los activos de la información como en las historias clínicas, citas, tratamiento por paciente se propone elaborar un plan de seguridad informático alineado con los controles de la normativa ISO 27002 Las herramientas que se basan son NMAP, NIKTO, OWASP con el fin de aplicar los estándares de la norma ISO Y asignar los controles, así surge la necesidad de generar una Auditoría a partir del análisis y el escaneo de la información para la obtención de las posibles amenazas. [14] Como conclusión de esta investigación de Catuto es identificar las amenazas y vulnerabilidades en los activos de información, con el propósito de desarrollar un plan de

seguridad que cumpla con los controles establecidos por la norma ISO 27002 para aplicar los estándares de la ISO, asignar controles necesarios, generando así una Auditoría basa en el análisis y escaneo de información con el fin de detectar posibles amenazas.

2.1.3 Antecedentes Regionales

Por consiguiente en la investigación titulada diseño de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 e ISO 27002 aplicada a procesos de gestión tic de la gobernación de Nariño Realizada por William Alfredo Inampues Villa y Daniel Esteban Lara Rosero en el año 2018 en la ciudad de San Juan de Pasto Nariño Su objetivo general Mejorar la gestión de la seguridad en los procesos, sistemas de información mediante el diseño de un SGSI basados en las normas ISO 27001 Y 27002 para la Gobernación de Nariño, identificar determinar los activos para establecer los dominios de los estándares de las normas en mención, la clave principal fue determinar las vulnerabilidades, amenazas, riesgos existentes aplicando la metodología MAGERIT Es una metodología de gestión de riesgos según la información desarrollada por el centro Criptológico Nacional (CCN) de España su objetivo principal es identificar, evaluar, gestionar los riesgos relacionados con la seguridad de la información en sus sistemas de información se enfoca en la validación de los activos, la valoración de activos, identificación de amenazas y vulnerabilidades, evaluación del riesgo, implementación de controles de seguridad, el seguimiento, revisión. Se basa en buenas prácticas relacionadas con la norma ISO 27001. [15] Como conclusión de la investigación de William destaca la importancia de la gestión de seguridad de la información en los procesos y sistemas a través de las normas y el enfoque de la metodología MAGERIT diseñada para identificar, evaluar y gestionar los riesgos, esto sugiere implementar algunos controles de seguridad basados en las buenas prácticas de la norma ISO 27001, esto permite una mejor detección y mitigación de amenazas y vulnerabilidades en entorno reales.

Con este propósito en la investigación titula diseño e implementación de una infraestructura de servicios telemáticos y protección de red bajo plataforma Linux dentro de la empresa licores CAPRI realizada por Christian David Naranjo López y David Esteban Gómez Coral en el año 2017 en la ciudad de San Juan De Pasto Nariño como objetivo Alcanzar la justificación

expuesta y fundamentada de las ventajas que se obtienen al añadir nuevos servicios para la seguridad, conexión, comunicación y administración de dispositivos de la empresa, mejoramiento en la red, como en la topología, componentes, dispositivos, modelos de frecuencia, protocolos y servicios de red, se basa en un informe el cual presenta un diagnóstico inicial de la red y los requerimientos se enfoca en el monitoreo y control del tráfico de datos entrante y saliente de la red, estableciendo unas reglas de seguridad con funciones de lógica del negocio y utilizando archivos tipo HTML y la implementación de un servidor que permite que las aplicaciones, datos y los procesos requeridos por la empresa estén salvaguardados "la creación de las políticas de seguridad de protección de información, mejorar los servicios de red con un servicio de DHCP para el direccionamiento IP de la red interna y externa y el servicio DNS para una asignación de un dominio disponible." [16] Como conclusión de la investigación de Christian la importancia de la seguridad, la infraestructura de red con la implementación de servicios telemáticos en plataforma Linux con el enfoque de monitoreo, tráfico de datos junto a la creación de políticas de seguridad.

Por lo tanto en la investigación titulada Auditoría a la infraestructura física de red y equipos de cómputo de la notaría de Túquerres realizada por Euler Remigio Basante Mora y Gilberth Andrey Ipaz en el año 2016 en la ciudad de San Juan de Pasto su Objetivo principal es identificar los fallos, riesgos y amenazas para minimizar el impacto y probabilidad de ocurrencia para mejorar el funcionamiento de la entidad, este trabajo se basó en el estándar COBIT (Objetivos de control para información y tecnologías relacionadas) se puede evidenciar que en el desarrollo de esta investigación está centrada en fortalecer los procesos de control a base de las Auditorías para evaluar el cumplimiento de las normas de instalación, los fallos en la red, en la transmisión de datos la verificación del plan de contingencia de la información, desarrollan un plan de Auditoría en el cual evalúan "Exploración del entorno, planeación de actividades, realización de la Auditoría y la presentación del informe final". [17] Como conclusión de la tesis de Euler es la identificación de los fallos, riesgos y amenazas en la infraestructura de red y equipos de cómputo con el objetivo de minimizar el impacto y la probabilidad de ocurrencia de estos problemas alineándose como los principales controles y gestión aplicando las buenas prácticas de un plan de Auditoría que comprende las etapas de exploración del entorno la planificación

de las actividades y la presentación del informe final.

Como conclusión integral de la revisión exhaustiva de los antecedentes resalta de manera contundente la imperiosa necesidad de desarrollar un software que aplique algunas de las metodologías prácticas para mejorar la seguridad, contribuyendo la protección de datos, Este software se centra específicamente en la validación de estados de seguridad en equipos abordando de manera directa y efectiva en los entornos reales. Su objetivo principal es elevar los estándares de seguridad mediante buenas prácticas y la realización de pruebas en condiciones dinámicas, en resumen, el desarrollo de esto software representa una contribución significativa a la mejora continua de la seguridad informática con el fin de mantener la integridad de la información en el entorno tecnológico moderno. Busca mejorar la seguridad de los equipos y la implementación de las buenas prácticas de seguridad, mediante pruebas en situaciones reales.

2.2 SUPUESTOS TEÓRICOS

2.2.1 Seguridad Informática

En el ámbito de la seguridad de los equipos informáticos y sistemas tecnológicos, existen desafíos significativos para garantizar su correcto funcionamiento y protección contra posibles amenazas y riesgos. En un mundo altamente interconectado, digitalizado la seguridad de la información se ha convertido en un aspecto de suma importancia para las organizaciones, se expresa que en la norma ISO 27001, establece un marco sólido para la gestión de la seguridad de la información, definido una serie de controles espacios en su diferentes numerales, según Borreo Ochoa “la importancia de identificar y proteger los activos necesarios para la gestión de la información de las organizaciones” [18], se utiliza los parámetros de la norma ISO 27001 como guías para la seguridad de la información y la clasificación de los riesgos.

La falta de una metodología y herramienta específicas para validar, verificar los estados de cumplimiento de estos controles en contextos prácticos puede dar lugar a inconsistencias, errores potenciales y a una exposición a riesgos de seguridad, la validación manual de estos

controles es propensa a ineficiencias, dificultades en la monitorización constante, la falta de rigurosidad en el proceso.

Estas pruebas en entornos simulados no proporcionan una evaluación completa de los estados de seguridad de los equipos, lo que puede resultar en la falta de detección de vulnerabilidades y debilidades reales. Además, el proceso de prueba manual puede ser de costos en término de tiempo y recurso y no garantiza una cobertura exhaustiva de todas las posibles situaciones de riesgo.

El planteamiento del problema se centra en la falta de una solución adecuada y efectiva para validar los estados de seguridad de los equipos en condiciones reales, lo que puede poner en riesgo la integridad, la confidencialidad de la información, así como la continuidad de las operaciones de las organizaciones.

En un entorno digital en constante evolución, los riesgos de seguridad de la información conforme al argumento de Moreira Álvarez "un sistema de gestión de seguridad de información tiene la necesidad de cumplir con regulaciones en proteger la reputación, reducir los costos y fomentar la mejora continua" [19] cada vez son más sofisticados y cambiantes, la falta de una herramienta automatizada para verificar y validar estados de cumplimiento con el beneficio de que las organizaciones estén libres de amenazas y ataques cibernéticos.

La validación manual de los controles de seguridad es propensa a errores humanos y requiere una inversión significativa de tiempo y recursos, un software de validación de estados podría automatizar el proceso, mejorando la eficiencia y la precisión en la verificación del cumplimiento de los controles.

Las organizaciones operan en contextos empresariales dinámicos y tecnológicamente cambiantes, esto hace que el software permite una respuesta más rápida y efectiva a las transformaciones en los sistemas y procesos, asegurando que los controles de seguridad se mantengan relevantes y eficaces.

Se estructurará en varios capítulos donde se abordan los aspectos teóricos y prácticos relacionados con la validación de estado de seguridad en los equipos, asimismo se presentará los resultados obtenidos durante la implementación del software, este estudio presenta un esfuerzo de aprovechar la tecnología en pro de la seguridad y el cumplimiento de los estándares en la norma ISO 27001 2013. En los controles definidos en los numerales [20]

- **9.1.2 Acceso a redes y servicios en red.**
  - Control: solo se debe permitir acceso de los usuarios a la red y a los servicios de red para lo que hayan sido autorizados específicamente. [20]
- **9.2.1 Registro y cancelación de registro de usuarios.**
  - Control: se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. [20]
- **9.2.2 Suministro de acceso de usuarios**.
  - Control: se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. [20]
- **9.4.3 Sistema de gestión de contraseñas**.
  - Control: los sistemas de gestión de contraseñas deben de ser interactivos y deben asegurar la calidad de las contraseñas [20]
- **12.3 Copias de respaldo.**
- Objetivo Proteger contra la pérdida de datos [20]
- **12.3.1 Respaldo de la información.**
  - Control: se debe hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a pruebas regularmente de acuerdo con una política de copias de respaldo acordadas [20]
- **12.4 Registro y seguimiento.**
- Objetivo registrar eventos y generar evidencia [20]

- **12.4.1 Registro de eventos.**
  - Control: se deben elaborar, conservar y revisar regularmente los registros acerca

de actividades del usuario, excepciones, fallas y eventos de seguridad de la información [20]

- **13 seguridad de las comunicaciones.**
- Objetivo asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información sistemas y aplicaciones [20]
- **13.1.1 Controles de redes.**
  - Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. [20]

- **13.1.2 Seguridad de los servicios de red.**
  - Control Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios presten internamente o se contrate externamente [20]
- **13.1.3 Separación en las redes.**
  - Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes [20]

Estos son algunos ejemplos de amenazas e intrusiones en red, se resalta que constantemente surgen nuevas formas de amenazas e intrusiones en red, es importante actualizar y aplicar las técnicas de detección y prevención.

- **Virus informáticos:**

  Estos son programas maliciosos que se programan y se replican a través de la red y pueden dañar sistemas y datos. [21]
- **Malware:**

  Es un software malicioso que puede robar información, tomar control de un sistema o causar daños. [22]
- **Ataques Phishing:**

  Son intentos de engañar a los usuarios para que compartan información personal o

financiera a través de correos electrónicos, mensajes de texto o sitios web falsos. [23]

- **Ataques de denegación de servicio (DDos)**

  Son intentos de inundar un servidor con tráfico para que no pueda responder a las soluciones legítimas. [24]

- **Ataques de fuerza bruta:**

  Son intentos de adivinar contraseñas o claves de cifrado probando combinaciones hasta que se encuentre la correcta. [25]

- **Ataques de inyección de códigos:**

  Son intentos de insertar código malicioso en una aplicación web para tomar el control del servidor o robar información. [26]

- **Ataques de redirección de DNS:**

  Son intentos de redirigir el tráfico de un sitio web legítimo a uno malicioso para robar información o propagar malware. [27]

- **Ataques de intermediación:**

  Son intentos de interceptar el tráfico de red para robar información o tomar control de un sistema. [28]

2.2.2 Auditoría de seguridad

Según Álvaro Gómez Vieites "La auditoría de seguridad es un proceso integral y sistemático que tiene como objetivo evaluar y verificar la efectividad de los controles de seguridad, implementados en un sistema informático, se trata de un proceso crítico que busca identificar vulnerabilidades, debilidades y riesgos en la seguridad de los sistemas informáticos, y garantizar que se adopten medidas efectivas para prevenir, detectar y mitigar los riesgos de seguridad." [29]

Se enfoca en la evaluación de los sistemas de información, redes, aplicaciones incluyendo la identificación de las vulnerabilidades, evaluación de las políticas procedimientos de seguridad, revisión de logs registros de eventos, y otros análisis técnicos y de gestión.

Su principal objetivo es mejorar la eficacia y eficiencia de los procesos las prácticas de seguridad, promoviendo una cultura de seguridad en toda la organización, por otro lado, es un proceso clave para garantizar la protección de la información la continuidad del negocio, la reputación de la organización

En el área de la seguridad informática los sistemas informáticos son un elemento fundamental, ya que son la base sobre la cual se construyen y se implementan los controles y medidas de seguridad necesarias para proteger la información y los recursos estos sistemas se puede incluir desde computadoras personales, servidores dispositivos móviles, redes de computadoras entre otros dispositivos conectados en red a estos sistemas se deben proteger adecuadamente para prevenir y mitigar los riesgos de seguridad con la pérdida de datos la exposición de información confidencial el robo de identidad y el acceso no autorizado, Según Oscar Arango esto implica la implementación de medidas de protección como la autenticación la autorización, el cifrado, la segmentación de red, la monitorización de eventos, establecer políticas y procedimientos de seguridad para garantizar que los sistemas informáticos sean utilizados de manera segura y responsable. [30]

2.2.3 Metodologías de auditoría de seguridad

La metodología de auditoría de seguridad suele incluir una serie de pasos y fases que se deben seguir para llevar a cabo una auditoría de seguridad de manera efectiva y rigurosa, estos pasos pueden incluir desde la definición de alcance de la auditoría y la definición de los objetivos y metas, hacia la ejecución de pruebas de penetración, análisis de vulnerabilidades, evaluación de políticas y procedimientos de seguridad y la elaboración de informes y recomendaciones. Conforme a la investigación Desarrollo de un sistema web para fortalecer el proceso de auditoría y seguridad informática en instituciones de educación superior realizada por Escobar Meneses Jhon Lenin en el año 2021 expresa “los tipos de auditorías se basan en las TIC`S, en la selección de metodologías de Auditoría de información y evaluación de las mismas” [31] Existen diversas

metodologías de auditoría de seguridad entre las cuales se pueden mencionar, algunas de las más utilizadas como:

- **Metodología OSSTMM**

  Esta metodología se centra en la evaluación de la seguridad de los sistemas informáticos mediante la realización de pruebas de penetración, análisis de vulnerabilidades y evaluación de las políticas y procedimientos de seguridad. [32]

- **Metodología NIST SP 800-53**

  Esta metodología se enfoca en la evaluación de la seguridad de los sistemas informáticos a través de un conjunto de controles de seguridad que deben ser implementados y evaluados [33]

- **Metodología ISSAF**

  Esta metodología se basa en la ejecución de una serie de fases para llevar a cabo la auditoría de seguridad desde la definición del alcance y objetivos y la elaboración de informes y recomendaciones. [34]

- **Metodología ITIL**

  Esta metodología se centra en la gestión de servicios de tecnología de la información y se utiliza para evaluar la seguridad de los sistemas informáticos desde la perspectiva de gestión de servicios la metodología ITIL proporciona un marco para la gestión de servicios de TI, que incluye la evaluación de la seguridad de los sistemas informáticos [35]

2.2.4 Pasos para la Auditoría en sistemas

Un programa de auditoría es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de la auditoría planificados, según Cárdenas Castillo "es importante que los resultados de la auditoría se comuniquen de manera efectiva a los responsables de la gestión de la seguridad del sistema, para que se pueda tomar medidas adecuadas para mejorar la seguridad" [36], además la auditoría de seguridad debe ser un proceso continuo y respectivo para garantizar la protección continua del sistema, la red. Un software de auditoría, es una herramienta diseñada para ayudar en automatizar gran parte del proceso y ofreciendo información y análisis detallados donde pueden incluir un amplio rango de características y funcionalidades que suelen incluir, escaneo de puertos, detección de vulnerabilidades, identificación de activos, análisis de configuraciones, análisis de logs.

- Tema de la auditoría
- Planificación
- Recopilación de información
- Objetivo de la auditoría
- Análisis de las vulnerabilidades
- Evaluaciones de controles de seguridad
- Planificación previa
- Metodología:
- Recogida de información
- Alcances de la auditoría
- Definición del alcance
- Hallazgos
- Resultados
- Recomendaciones
- Informe final
- Seguimiento y verificación

2.2.5 Organizaciones y herramientas de gestión de vulnerabilidades

Las herramientas y técnicas de manejo de vulnerabilidades son recursos y enfoques utilizados por las organizaciones y profesionales de seguridad cibernética para identificar, evaluar, mitigar y gestionar las debilidades o vulnerabilidades en sistemas, aplicaciones y redes de tecnología de la información, entre ellas se tienen las siguientes:

- **Mitre**

  Es una organización sin fines de lucro dedicada a investigar y resolver problemas complejos de seguridad en diversas áreas, incluyendo la seguridad cibernética, la seguridad nacional y la atención médica, entre las iniciativas más conocidas, además mitre se conecta a una red para identificar amenazas y actuar para que se ejecute como una tarea programada, luego de esto el ataque puede ser capaz de moverse lateralmente a través de la red y programar su software de extracción, mitre trabajo en estrecha colaboración con el gobierno de EE.UU en temas de seguridad y defensa nacional. [37]

- **OWASP Top Ten**

  Es un proyecto de la organización Open Web Application Security Project [38] que se centra en identificar y concienciar sobre las diez principales vulnerabilidades de seguridad que afectan a las aplicaciones web, el propósito de la página OWASP Top Ten es proporcionar a los desarrolladores, una lista actualizada de las principales amenazas y riesgos a lo que se enfrentan, su metodología implica la recopilación y análisis de datos de vulnerabilidades en aplicaciones web como la recolección de datos, clasificaciones de vulnerabilidades, selección de las diez principales, actualización periódica, involucramiento de la comunidad, documentación detallada, concientización y educación, guía para desarrolladores, herramientas de pruebas de seguridad y promoción de la seguridad en el ciclo de vida del desarrollo. La metodología del OWASP implica la identificación, clasificación y divulgación de las 10 vulnerabilidades más críticas en aplicaciones web con un enfoque en la educación y la promoción de buenas prácticas de seguridad en el desarrollo de software. El equipo de OWASP selecciona las diez principales vulnerabilidades más críticas y frecuentes para crear la lista:

- **A01:2021 Pérdida de control de acceso:** Sube de la quinta posición a la categoría con el mayor riesgo en seguridad de aplicaciones web. [38]
- **A02:2021 Fallas Criptográficas:** Sube en una posición ubicándose en la segunda, antes conocida como A03:2017-Exposición de datos sensibles. [38]
- **A03:2021 Inyección:** Desciende hasta la tercera posición, tiene la segunda cantidad de ocurrencias en aplicaciones con 274.000 ocurrencias. [38]
- **A04:2021 Diseño Inseguro:** Nueva categoría para la edición 2021, con un enfoque en los riesgos relacionados con las fallas de diseño, los controles de seguridad necesarios nunca se crearon para defenderse de ataques específicos. [38]
- **A05:2021: Configuración de seguridad incorrecta:** Asciende desde la sexta posición en la edición anterior; el 90% de las aplicaciones se probaron para detectar algún tipo de configuración incorrecta. [38]
- **A06:2021 Componentes vulnerables y desactualizados**: Esta categoría asciende desde la novena posición en la edición 2017 y es un problema conocido que cuesta probar y evaluar el riesgo. [38]
- **A07:2021 Fallas de identificación y autenticación:** Esta categoría sigue siendo una parte integral del Top 10, pero el incremento en la disponibilidad de frameworks estandarizados. [38]
- **A08:2021 Fallas en el software y en la integridad de los datos**: Es una categoría para la edición 2021, que se centra en hacer suposiciones relacionadas con actualizaciones de software, los datos críticos y los pipelines CI/CD sin verificación de integridad.

[38]

- **A09:2021 Fallas en el registro y monitoreo**: Esta categoría se amplía para incluir más tipos de fallas, es difícil de probar y no está bien representada en los datos de CVE/CVSS. Sin embargo, las fallas en estas categorías pueden afectar directamente la visibilidad, las alertas de incidentes y los análisis forenses. [38]
- **A10:2021 Falsificación de solicitudes del lado del servidor:** Esta categoría representa el escenario en el que los miembros de la comunidad de seguridad nos dicen que esto es importante. [38]

- **Sans (SysAdmin, Audit, Network, Security)**

  Es una organización sin fines de lucro dedicada a la formación y certificación de profesionales en seguridad informática, es la fuente más grande y confiable en seguridad contra amenazas en ciberseguridad, es la mayor organización del mundo que reúne información sobre todo lo referente a seguridad informática y las TIC teniendo una mayor organización en seguridad de aplicaciones como también en su seguridad de redes y auditorías. [39]

- **Shodan**

  Es un motor de búsqueda especializado en dispositivos conectados a internet, como servidores, enrutadores, cámaras IP, sistemas de control industrial, dispositivos médicos entre otros conectados a internet de las cosas, Shodan indexa u almacena información sobre estos dispositivos, como las direcciones IP, el tipo de dispositivo, la versión del sistema operativo, el software que se está ejecutando y otro detalle que puede ser útiles para los investigadores de seguridad y los atacantes. [40]

- **Nmap**

  Es una herramienta de exploración de redes que se utiliza para realizar escaneos de puertos y descubrir dispositivos y servicios en una red, también puede ser utilizado para detectar vulnerabilidades en los servicios encontrados. [41]

- **Metasploit**

  Es una herramienta de pruebas de penetración que se utiliza para encontrar y explotar vulnerabilidades en sistemas informáticos, también puede ser utilizada para validar la efectividad de los controles de seguridad implementados en una organización. [42]

- **Nessus**

  Es una herramienta de análisis de vulnerabilidades que se utiliza para identificar y evaluar vulnerabilidades en sistemas informáticos y redes, proporciona un amplio conjunto de pruebas de seguridad predefinidas y permite la personalización de las pruebas de seguridad para adaptarse a las necesidades específicas de la organización. [43]

- **Wireshark**

  Es una herramienta de análisis de tráfico de red que se utiliza para capturar el tráfico de red en tiempo real, puede ser utilizado para detectar posibles amenazas de seguridad y para identificar vulnerabilidades en los protocolos de red utilizados por los sistemas informáticos. [44]

- **OpenVAS**

  Es una herramienta de análisis de vulnerabilidades de código abierto que se utiliza para evaluar la seguridad de los sistemas informáticos, proporciona un amplio conjunto de pruebas de seguridad predefinidas y permite la personalización de las pruebas de seguridad para adaptarse a las necesidades específicas de la organización. [45]

- **CENTRO Criptológico Nacional**

  La gestión efectiva de la ciberseguridad se convierte en un desafío colectivo esencial para proteger la economía la proliferación de ataques cibernéticos y el robo de información destacan la necesidad de comprender las amenazas asociadas a las tecnologías de la información, la ley 11/2002 asigna al Centro Nacional de Inteligencia (CNI) y al Centro Criptológico Nacional (CCN) las responsabilidades claves en la seguridad de la información [46], los documentos reflejan la mejora para las políticas y procedimientos como la Plantilla del informe técnico de evaluación de la certificación nacional esencial de seguridad (lince). [47]

2.2.6 Normas Y Leyes Relacionados Con La Ciberseguridad A Nivel Internacional Y Nacional

Como indica Carlos Martin Establecer y aplicar normas y leyes relacionadas con la ciberseguridad a nivel internacional y nación en cualquier organización [48] con el fin de garantizar la protección de los activos digitales, datos sensibles y la continuidad de las operaciones como son el cumplimiento legal, protección de datos, mitigaciones de riesgos, la continuidad de negocio, fortalecimiento de la seguridad, fomentación de una cultura de ciberseguridad, respaldo de la reputación y la preparación de amenazas emergentes.

- **Norma ISO 27001**

  Es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) y brinda un marco para la implementación y mejora de la seguridad de la información en una organización. [49]

- **Regulación general de la protección de datos (RGPD)**

  Es una ley europea que regula la protección de los datos personales de los ciudadanos de la unión europea y establece las obligaciones de las organizaciones que procesan datos personales. [50]

- **Ley 527 de 1999**

  Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Tiene como objetivo establecer las normas y regulaciones para el uso de medios electrónicos en transacciones eléctricas, aborda aspectos como los mensajes electrónicos, la firma digital y la protección de la información en el entorno digital. [51]

- **Ley 594 del 2000**

  Por medio de la cual se expide la ley general de archivos. Tiene como objetivo establecer las normas para la organización y administración de archivos en el ámbito público y privado, busca garantizar el acceso, conservación y la gestión eficiente de la documentación promoviendo la transparencia, la memoria histórica y la eficacia administrativa. [52]

- **Ley 1266 de 2008**

  Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos. Su objetivo principal es regular el manejo de la información crediticia y establecer los derechos y deberes de los titulares de la información, así como de las entidades que recopilan, manejan y suministran datos crediticios. Busca garantizar la privacidad y seguridad de la información financiera de los individuos. [53]

- **Ley 1221 de 2008**

  Por la cual se establecen normas para promover y regular el teletrabajo. Busca incentivar la participación activa de la comunidad en la toma de decisiones

locales, contribuyendo así a una gestión más efectiva y transparente. [54]

- **Ley 1273 de 2009**

  Es una ley colombiana que su objetivo principal de esta ley es proteger la seguridad informática y la privacidad de los ciudadanos, promover el uso responsable y seguro de la información y comunicación (TIC) y combatir los delitos informáticos que pueden afectar la integridad de los sistemas informáticos, la economía y la seguridad nacional , también establece sanciones penales y administrativas para aquellos que cometen delitos informáticos con el fin de disuadir a los posibles infractores y crear un ambiente de confianza en el uso de las TIC en Colombia. [55]

- **Ley 1341 de 2009**

  Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC. Busca promover el acceso equitativo a los servicios de telecomunicaciones, fomentar la competencia en el sector y garantizar la calidad de los servicios ofrecidos. [56]

- **Ley 1581 de 2012**

  Por la cual se dictan disposiciones generales para la protección de datos personales. Tiene como objetivo regular el manejo de la información personal y garantizar la privacidad de los ciudadanos. Establece principios para la recolección, almacenamiento, uso y circulación de datos personales, así como derechos para los titulares de esta información, la ley busca fortalecer la seguridad y confidencialidad de los datos, promoviendo su uso adecuado y evitando su indebido manejo. [57]

- **Ley 1712 de 2014**

  Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la

información pública nacional. Tiene como objetivo promover la transparencia en la gestión pública y garantizar el derecho de acceso a la información. La ley establece mecanismos para facilitar la divulgación proactiva de información pública y establece reglas para que los ciudadanos ejerzan su derecho de acceso a la información de manera efectiva. [58]

- **Ley 1915 de 2018**

  Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor. Estas disposiciones son una exportación de normas norteamericanas que regulan aspectos para que puedan hacer unas adecuadas implementaciones de las obligaciones contenidas en el TLC en su sistema de derecho de autor. [59]

- **Ley de Ciberseguridad**

  Esta ley establece los requisitos y obligaciones para proteger la seguridad informática y la privacidad de los ciudadanos y para prevenir y sancionar delitos informáticos. Proporciona un objetivo establecer normas y regulaciones para proteger las infraestructuras críticas y los datos sensibles de ciberamenazas, fortalecer la resiliencia cibernética, prevenir ataques, establecer marcos legales para la investigación y el enjuiciamiento de delitos cibernéticos. [60]

2.2.7 Definición de las tecnologías a utilizar

Para el desarrollo se llevó a cabo con la utilización de Visual Studio Code, lenguaje de programación en Python el uso del Qt Designer y las librerías en scapy.all, socket, inreg, psutil, win32com.client, winreg, platform, subprocess. [61]

- **Librería Socket en Python:** también proporciona un interfaz de programación de aplicaciones para trabajar con sockets y protocolos de red en aplicaciones de

red se pueden utilizar diferentes protocolos de red como TCP, UDP Y ICMP [62]

- **Librería Scapy.all y las clases ARP, Ether y Srp en Python:** son herramientas poderosas para crear, enviar y analizar paquetes en red estas librerías pueden ser utilizadas en una variedad de tareas relacionadas con la red incluyendo el análisis de tráfico, pruebas de seguridad y desarrollo de herramienta de red. [63]

- **Librería Scapy.all en Python:** el objetivo es proporcionar un interfaz fácil de usar para trabajar con paquetes de red en Python ofrece una amplia gama de funcionalidades para crear, enviar, analizar y manipular paquetes de red. [64]

- **Librería importlib.util en Python:** que permite importar módulos en tiempo de ejecución esto permite tener un mayor control sobre el proceso de importación y cargue de módulos. [65]

- **Librería subprocess en Python:** permite interactuar con procesos externos, proporciona una forma conveniente de crear procesos secundarios, conectar con ellos y controlar su entrada y salida como ejecución de comandos de línea de comando. [66]

- **Librería psutil en Python:** obtiene información del sistema operativo y de los procesos que se está ejecutando en el sistema, esta librería permite acceder a un gran cantidad de información sobre el sistema operativo, los procesos el uso del CPU la memoria, los discos, la red, se puede optimizar el rendimiento del sistema, identificar procesos que están utilizando demasiados recursos y solucionar problemas de rendimiento. [67]

-

2.2.9 Metodología de desarrollo.

Metodología XP

Según Kent Beck el objetivo de la metodología "Extreme Programming Explained es mejorar la calidad del desarrollo de software y la satisfacción del cliente a través de la práctica de desarrollo ágil y colaborativo" [68], se basa en una serie de principios y prácticas diseñados para abordar el desarrollo del software
Principales Objetivos

- Satisfacción del Cliente
- Entrega frecuente de software funcional
- Flexibilidad
- Comunicación y colaboración
- Calidad de código
- Retroalimentación continúa

Se centra en la satisfacción del cliente, la funcionalidad y de alta calidad de manera constante, la adaptabilidad a los cambios La metodología XP (Extreme Programming) se utiliza principalmente en el desarrollo de software ágil, los pasos para la metodología XP son los siguientes: [68]

- **Planificación:** se establecen los objetivos, requerimientos y plazos para el proyecto de la investigación.
- **Diseño:** se elabora un diseño detallado del proyecto, que incluye diseño de la investigación, diseño de la solución, diseño de las pruebas, entre otros.
- **Codificación:** Se realiza la implementación del código necesario para la investigación.
- **Pruebas:** se realizan pruebas de validación y verificación del código, asegurando que cumpla con los requisitos y funciones correctamente.

- **Retroalimentación:** se analiza el desempeño del código y se busca mejorar su eficiencia y eficacia.
- **Integración:** se integra el código en el proyecto de investigación y se asegura su correcto funcionamiento en conjunto con los demás elementos del proyecto.
- **Despliegue:** se lanza el código en el ambiente de la producción.
- **Mantenimiento.** Se realiza el mantenimiento del código y se corrigen errores que se presenten después de la implementación.

La programación XP (Extreme Programming) se basa en una serie de valores y principios que guía su enfoque de desarrollo de software" [68].

- **Comunicación:** Ayuda a garantizar que todos tengan comprensión clara de los objetivos y requisitos del proyecto.
- **Simplicidad:** XP aboga por la simplicidad en el diseño y la implementación del software, se enfoca en crear la funcionalidad necesaria sin agregar características innecesarias o complejidad adicional.
- **Retroalimentación:** Esto ayuda a garantizar que el software se adapte a las necesidades cambiantes del cliente.
- **Valentía**: se refiere a la disposición difíciles y a la voluntad de hacer cambios cuando sean necesarios
- **Respeto:** Se valora la opinión y la contribución de todos los miembros del equipo, se busca crear un ambiente de trabajo colaborativo y productivo.

Según Kent Beck "Estos valores son fundamentales en la metodología XP y ayudan a guiar las prácticas y técnicas específicas que se utilizan en el desarrollo del software para lograr un desarrollo de software ágil y de alta calidad." [68]

2.3 VARIABLES DE ESTUDIO

Variable Independiente

- **Software de validación**

  El software implica la definición de reglas, criterios y pruebas específicas que permitan determinar si un programa cumple con las normativas y expectativas establecidas, esto incluye la eficiencia y los estados para así reducir el riesgo.

Variable dependiente

- **Eficiencia del software**

  Capacidad del software desarrollado para realizar pruebas de validación de estados de seguridad de manera rápida y precisa, minimizando el consumo de recurso y tiempo requeridos.

- **Estados de seguridad**

  Los estados de seguridad se refieren a las condiciones o situaciones en las que se minimiza los riesgos u amenazas para la protección de activos, información en un entorno determinado.

2.31 DEFINICIÓN NOMINAL DE LAS VARIABLES

Se buscará diseñar y desarrollar un software que permita evaluar el comportamiento de los equipos si están en un entorno de riesgo. Esta variable será implementada y evaluada para comprobar su eficiencia y confiabilidad. Basada en algunos controles de la norma ISO 27001.

- Software de validación de estados.
- Eficiencia del software.
- Estados de seguridad.

2.3.2 DEFINICIÓN OPERATIVA DE LAS VARIABLES

- **Diseño y programación del software.**

  El diseño de software se refiere a la creación de una arquitectura lógica y funcional del programa, estableciendo cómo interactúan sus componentes y cómo cumplirán con los requisitos específicos del sistema de validación de seguridad, la programación por su parte se encarga de traducir este diseño en código informático implementando algoritmos, estructuras de datos y funcionalidades que permitan ejecutar las pruebas en entornos reales, esto implica la creación de interfaz de usuario, la integración de hardware, la gestión de base de datos con el fin de validar y verificar la seguridad en equipos. El desarrollo del software combina la planificación de la arquitectura con la codificación de funciones críticas para garantizar la seguridad de los dispositivos.

- **Eficiencia del software.**

  La capacidad para realizar las pruebas de validación de manera óptima y efectiva, minimizando el consumo de recursos, el tiempo de ejecución y asegurando una respuesta ágil en las situaciones de seguridad. En este desarrollo se requiere un número de pruebas complejas, con el fin de no sobrecargar el hardware y garantizar un desempeño rápido y efectivo, la escalabilidad para abordar pruebas en equipos con diferentes niveles de complejidad, el software reduce los costos operativos y minimiza el riesgo de errores.

- **Estados de seguridad.**

  Los estados de seguridad se refieren a condiciones o situaciones en las que se encuentran

los equipos, dispositivos o sistemas que se están evaluado con el fin de asegurar que operen de manera segura y confiable que pueden abordar varios aspectos:

- **Integridad:** evaluar si los equipos funcionan sin daños o alteraciones no autorizadas que puedan comprometer su funcionamiento seguro.
- **Funcionamiento adecuado:** comprobar si los equipos realizan sus funciones según lo previsto, sin fallas o errores que puedan causar accidentes o peligros
- **Configuración segura:** asegurarse de que los equipos estén configurados y operen de acuerdo con las pautas de seguridad y políticas establecidas.
- **Actualización:** verificar que los equipos estén al día con las actualizaciones de seguridad necesarias para garantizar su operación segura.

Los estados de seguridad se determinan mediante pruebas en entornos reales, que los equipos pueden enfrentar en su uso cotidiano, por eso es importante que el desarrollo del software proporcione información crítica para garantizar que los equipos estén en condiciones óptimas para su operación segura y confiable.

2.4 FORMULACIÓN DE HIPÓTESIS

2.4.1 Hipótesis de investigación

Hi. El software de validación de estados en equipos a través de pruebas en entornos reales tendrá un impacto positivo en la mejora de la seguridad de los equipos y la protección de la información

2.4.2 Hipótesis nula

Ho. El software de validación de estados en equipos a través de pruebas en entornos reales no tendrá un impacto positivo en la mejora de la seguridad de los equipos y la protección de la información

2.4.3 Hipótesis alterna

Ha. El software de validación de estados en equipos mediante pruebas en entorno real permite que los usuarios tomen conciencia en cuanto a la seguridad de los equipos y la protección de la información.

3 METODOLOGÍA

3.1 PARADIGMA

El paradigma de esta investigación es el denominado positivista, de acuerdo a Quijano [69] el cual dice que está enfocado a una investigación cuantitativa que se entiende como conocimiento científico

3.2 ENFOQUE

El enfoque de la investigación se desarrollará bajo un enfoque cuantitativo de acuerdo a Ignacio Rojas [70], se utilizan datos cuantitativos o cuantificables ya que poseen diversas propiedades que se aplicarán en esta investigación.

3.3 MÉTODO

El método utilizado sería un enfoque Científico Según Sandra Hoyos [71] para obtener conocimiento confiable y verificable, este método implica una serie de pasos, que suelen incluir la formulación de una pregunta de investigación, la recopilación de datos, el análisis de datos, la interpretación de resultados y la comunicación de hallazgos.

3.4 TIPO DE INVESTIGACIÓN

El método utilizado sería un enfoque correlacional para analizar la relación o asociación entre dos o más variables, su objetivo principal es determinar si existe una conexión estadística entre estas variables, si establecer una causa o efecto directa, este método ayuda a identificar patrones, tendencias y proporciona información valiosa para la toma de decisiones y la formulación de hipótesis en la investigación.

3.5 DISEÑO DE INVESTIGACIÓN

El diseño de esta investigación es cuasiexperimental los investigadores no pueden asignar aleatoriamente a los patrones a grupos de tratamiento y de control como se haría en un experimento controlado se intenta establecer relaciones de causa y efecto entre variables, no se puede asegurar la misma validez interna que un experimento puro.

3.6 POBLACIÓN

La población está relacionada con los Equipos de cómputo (Computadores) que se someterán a pruebas de seguridad en entornos reales.

3.7 MUESTRA

La muestra representa con un 90% de probabilidad representación que significa que la probabilidad de que la muestra que se tomara refleje con precisión las características de la muestra, 95% de nivel de confianza indica que se tomarán múltiples muestras de la misma población y se calcularon intervalos de confianza esto proporciona un alto grado de seguridad en las estadísticas de los resultados y con un margen de error del 5% que significa la estimación basada en la muestra, podría variar cuanto menor sea el margen de error mayor será la precisión de la estimación

N = Muestra de población

Z= Nivel de confianza

P= proporción de la población con la característica deseada

Q=Proporción de la población sin la característica deseada

E= Nivel de error dispuesto a cometer

N= Tamaño de la población

Margen de error: 5%

Nivel de confianza: 95%

Tamaño de población: 100 Computadores

$$N = \frac{N*`P*Q*Z^2}{E^2 + (N-1) + P*Q*Z^2}$$

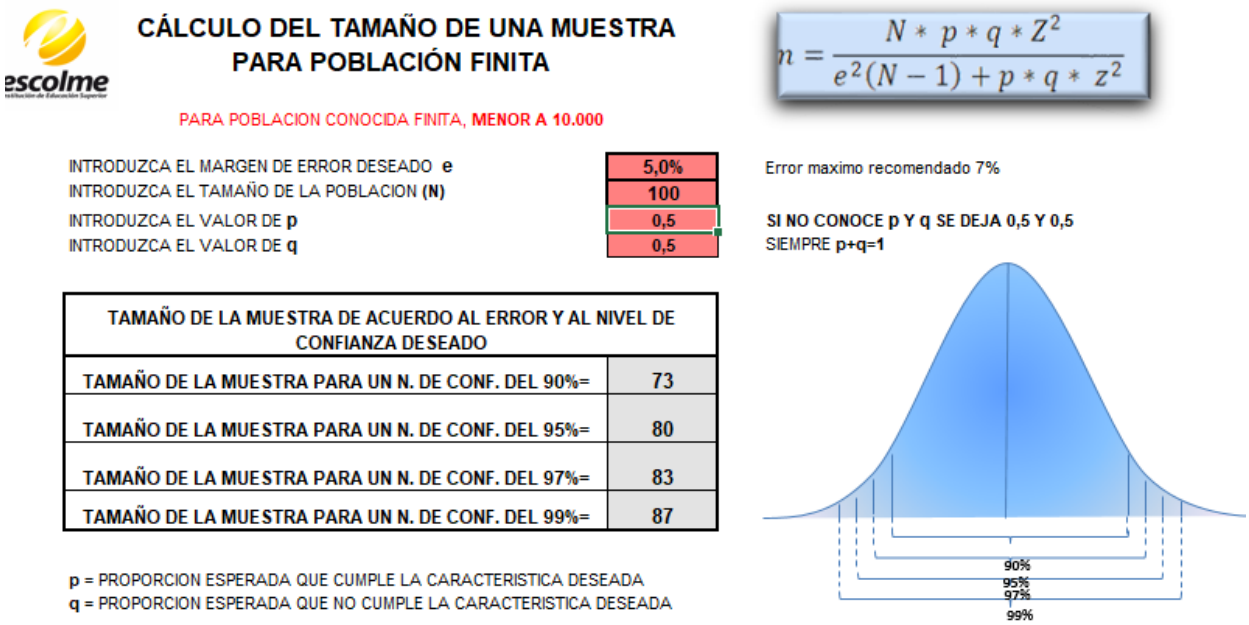


Fig. 1 Cálculo de tamaño de muestra

Fuente Escolme, Institución de Educación Superior

3.8 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN.

La técnica de recolección para esta investigación es la encuesta según Luis Vélez [72], permite recolectar información tanto cualitativa como cuantitativa a ciento tipos de personas que se miden estadísticamente.

3.9 VALIDEZ DE LAS TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Para garantizar la validez de la recopilación de la información se emplea la opinión de expertos, el asesor de investigación Alex Gilberto Urbina Gamboa y el docente de investigación III Luis Arnoby Escobar Hernández de la Universidad CESMAG, ofrecerían sus recomendaciones. La validez de las técnicas de recolección de información se logra a través de la utilización de pruebas, en entornos reales, la participación de expertos y la triangulación de datos. Estas prácticas garantizan la obtención de datos precisos.

3.10 CONFIABILIDAD DE LAS TÉCNICAS DE RECOLECCIÓN

Las técnicas de recolección de información se logran a través de las pruebas, el registro y la documentación adecuada, la evaluación de la confiabilidad mediante técnicas estadísticas cuando sea apropiado, estas prácticas aseguran que los resultados obtenidos sean consistentes y replicables, brindando mayor confianza en los hallazgos de la investigación.

3.11 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

El Instrumento de recolección de información que se va utilizar es el cuestionario; se puede diseñar un cuestionario estructurados para recopilar información cuantitativa sobre características específicas de los equipos, su configuración, su nivel de seguridad actual, y la percepción de los usuarios sobre la efectividad de un software de validación. Se incluirá una lista de chequeo que permita verificar los estados de los equipos acorde con las pruebas que se van a aplicar.

4. RESULTADOS DE INVESTIGACIÓN

En el presente documento, se exponen los resultados de la investigación realizada en el marco del trabajo de grado titulada "Desarrollo De Un Software De Validación De Estados De Seguridad En Los Equipos Mediante Pruebas En Entorno Real". Este estudio ha estado enfocado en la creación del software. A lo largo de la investigación, se realizaron diversos análisis y pruebas que fueron cruciales para el desarrollo y refinamiento del software. Los resultados se dividen en varias categorías:

4.1 Análisis de herramientas y técnicas en seguridad informática

4.1.1 Documentación de vulnerabilidades y metodologías de auditoría

La documentación de vulnerabilidades es esencial en la ciberseguridad para identificar, evaluar y mitigar riesgos en sistemas informáticos. Se analizaron diversas organizaciones y herramientas líderes en este campo, destacando la colaboración entre sectores públicos y privados. Además, se evaluaron metodologías como OSSTMM, ISSAF y NIST SP800-53, cada una con enfoque específico, sin embargo, la decisión de no implementar directamente estas metodologías en el desarrollo del software se fundamenta en que ofrecen un enfoque que puede resultar demasiado específico, robusto y no completamente alineado con los objetivos versátiles del proyecto, adaptables a diferentes entornos.

La Norma ISO 27001:2013 se ha seleccionado como un marco de referencia principal por varias razones. Esta norma no solo es reconocida globalmente, sino que también proporciona un marco integral que se adapta de manera flexible a varias necesidades de las organizaciones.

4.1.2 Análisis de la Norma ISO 27000:2013

La Norma ISO 27001:2013 (Sugerida por el Ingeniero Alex Urbina Gamboa anterior asesor de proyecto) se seleccionó porque proporciona un marco robusto y sistemático para la gestión de

la información, crucial para salvaguardar la confidencialidad, integridad y disponibilidad de los datos en las organizaciones. Su aplicación global se adapta a los objetivos del proyecto y desarrollo del software destacando su relevancia y eficacia en establecer controles de seguridad informática que responden a las necesidades contemporáneas de protección de información. Este estándar ha sido base en la implementación de prácticas de seguridad a través de varios dominios críticos, que refuerzan su posición en la gestión estratégica de la seguridad de la información a nivel internacional.

4.1.3 comparativo de herramientas y metodologías

Se realizó un análisis comparativo de herramientas y metodologías evaluando su uso de las librerías SUBPROCESS SOCKET Y DATETIME, así como su disponibilidad gratuita o de pago.

Tabla No I Comparativo de Herramientas

HERRAMIENTA	USO DE SUBPROCESS	USO DE SOCKET	USO DE DATETIME	LICENCIA
Open VAS	SI	SI	NO	Gratuita
Wireshark	Si	No	No	Gratuita
Nessus	Si	Si	No	Pago
Metasploit	Si	Si	No	Gratuita (con edición comercial disponible)
Nmap	Si	Si	No	Gratuita
Shodan	Si	Si	No	Pago (con versión gratuita limitada)
Scanner Nikto	Si	Si	No	Gratuita
BurpSuit	Si	Si	No	Pago (con versión gratuita limitada)

Tabla No II Comparativo de metodologías

Metodología	USO DE SUBPROCESS	USO DE SOCKET	USO DE DATETIME	LICENCIA
SANS	SI	NO	NO	Gratuita (Con edición comercial disponible)
OWASP Top Ten	Si	NO	No	Gratuita
Mitre	Si	NO	No	Gratuita

4.1.4 Análisis de encuesta aplicada para desarrollo de software

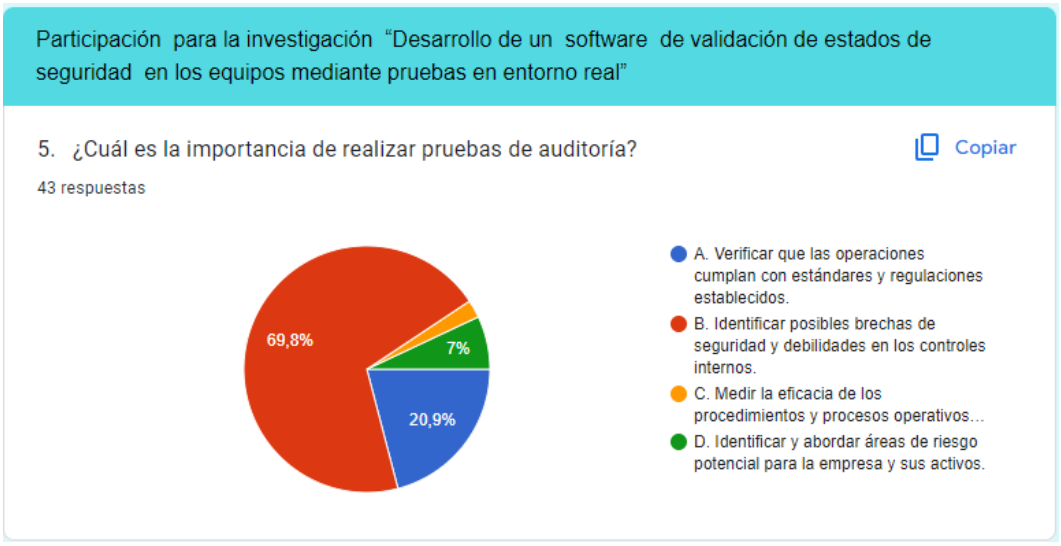
La encuesta sobre los estados de seguridad realizada a estudiantes de décimo semestre, técnicos, tecnólogos e ingenieros de sistemas con roles de soporte técnico en la gestión de información y equipos en diversas organizaciones tenía como meta principal recopilar información detallada sobre la seguridad de la información y sistemas informáticos. Entre los objetivos específicos de la encuesta se encontraban evaluar la conciencia y el conocimiento sobre políticas y prácticas de seguridad entre empleados y usuarios, identificar amenazas y riesgos de seguridad, recoger opiniones sobre la efectividad de las medidas de seguridad implementadas, medir la satisfacción de los usuarios y empleados con dichas medidas, y discernir áreas potenciales de mejora en la seguridad informática de las organizaciones a partir de las experiencias y perspectivas de los participantes. Para llevar a cabo este estudio, se solicitó la colaboración de la Empresa Social Del Estado Pasto Salud E.S.E., así como de compañeros universitarios en fase práctica y de ingenieros de las universidades: Universidad de Nariño (UdeNar), Corporación Universitaria Minuto de Dios (UNIMINUTO) y del Servicio Nacional de Aprendizaje SENA Regional Nariño.

Los resultados de la encuesta son fundamentales para respaldar las conclusiones de la investigación, proporcionando evidencia empírica sobre la utilidad y la viabilidad del software de validación de estados de seguridad en un contexto operativo real. La encuesta reveló un reconocimiento claro de la importancia de disponer de herramientas que permitan la detección y corrección de vulnerabilidades, el cumplimiento de normativas y una amplia cobertura en tipos de pruebas de seguridad, subrayando la necesidad de tales herramientas para fortalecer la

resiliencia de los sistemas ante amenazas cibernéticas y para asegurar la integridad y eficiencia de los equipos tecnológicos.

Dentro de las preguntas clave, diseñadas para evaluar la percepción de los encuestados sobre la eficacia y aplicabilidad del software de validación de estados de seguridad, se destacan las siguientes:

Pregunta 5: Explora la relevancia de las pruebas de auditoría, enfocándose en la identificación de brechas de seguridad y debilidades en los controles internos.



Gráfica No 1 Pregunta 5

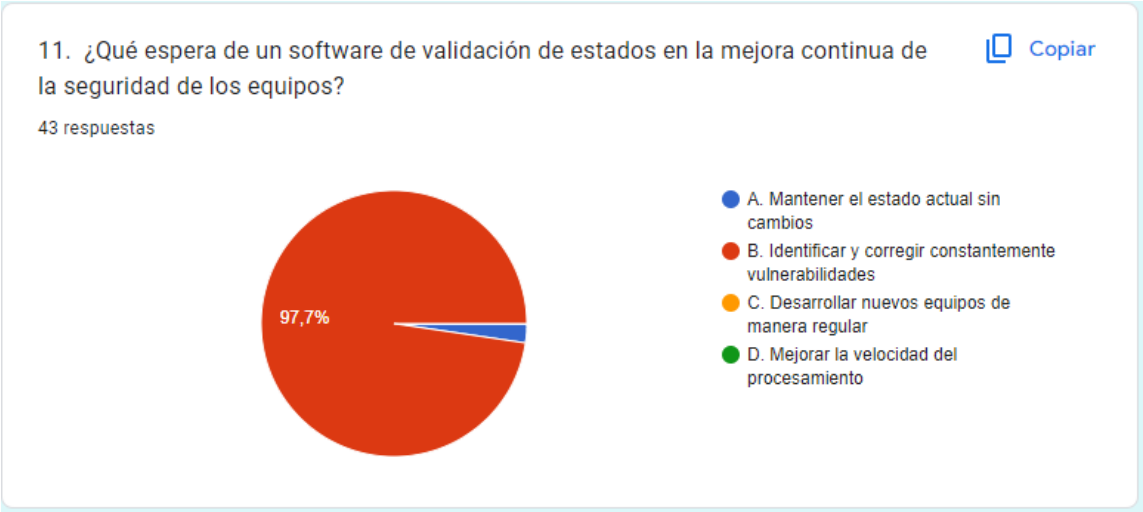
Fuente: Elaboración propia.

Pregunta 10: Se centra en determinar qué tipos de pruebas son consideradas más pertinentes para un entorno operativo real, mostrando una preferencia clara por la inclusión de todas las pruebas posibles.

Gráfica No 2 Pregunta 10

Fuente: Elaboración propia.

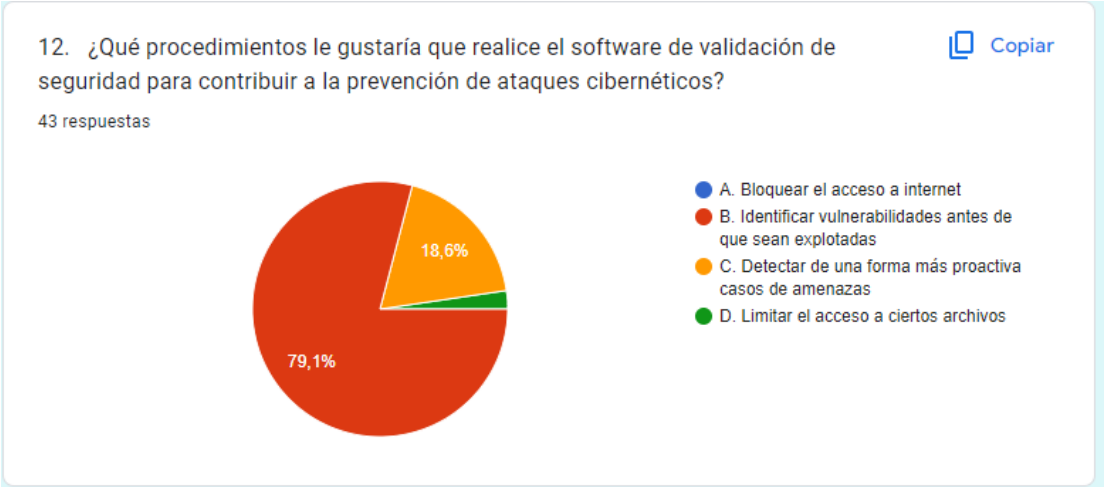
Pregunta 11: Investiga las expectativas hacia el software de validación de estados para la mejora continua de la seguridad de los equipos, revelando un fuerte consenso en la necesidad de identificar y corregir vulnerabilidades.



Gráfica No 3 Pregunta 11

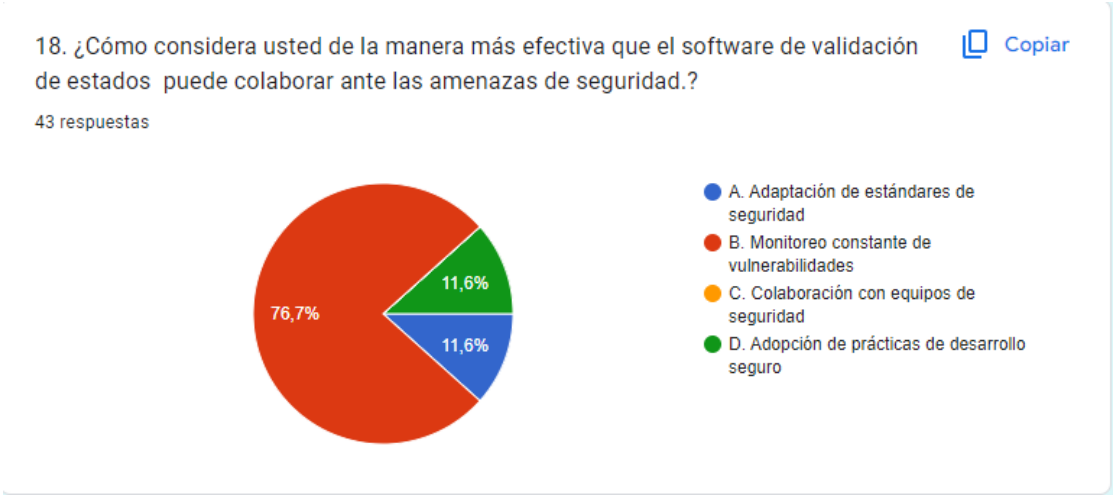
Fuente: Elaboración propia.

Pregunta 12 y 18: Abordan cómo el software podría prevenir ataques cibernéticos y colaborar efectivamente frente a amenazas de seguridad, respectivamente, poniendo énfasis en la detección y el monitoreo constante de vulnerabilidades.



Gráfica No 4 Pregunta 12

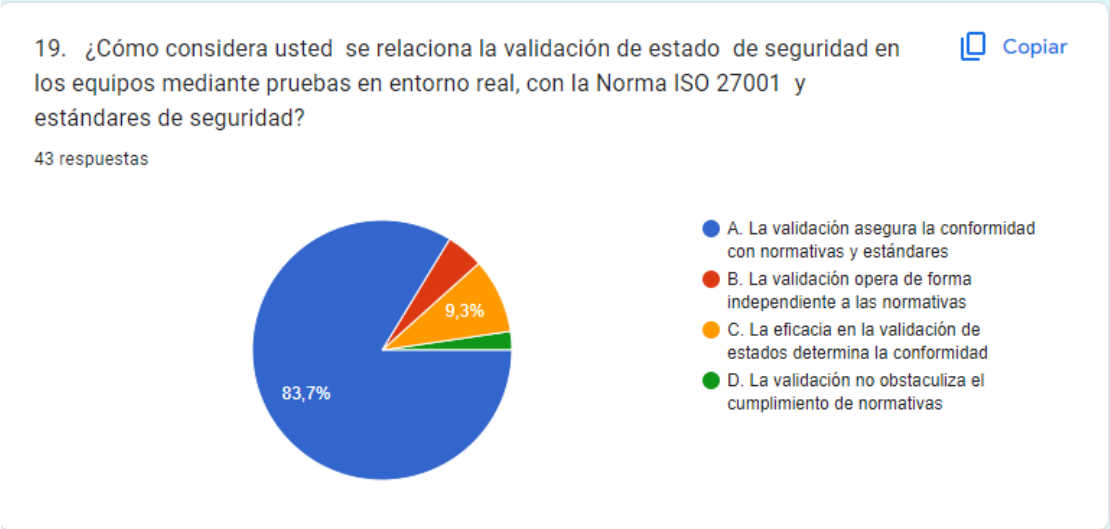
Fuente: Elaboración propia.



Gráfica No 5 Pregunta 18

Fuente: Elaboración propia.

Pregunta 19: Relaciona la validación de la seguridad en equipos con normativas internacionales como la ISO 27001, destacando la importancia del software en cumplir con contextos normativos.



Gráfica No 6 Pregunta 19

Fuente: Elaboración propia.

4.2 Desarrollo del software titulado AuditaPro

4.2.1 AuditaPro software inicial para análisis de estados de seguridad

Para el desarrollo del software, AuditaPro se adoptó la metodología de Extreme Programming (XP) una estrategia ágil que prioriza la satisfacción del cliente a través de la entrega temprana y continúa del software funcional. La implementación de XP en el proyecto garantiza la eficiencia y calidad del software alineándose con las metas de proporcionar soluciones seguras y confiables en la auditoría de TI a continuación se describen los pasos aplicados en el desarrollo de AuditaPro.

4.2.2 Planificación

Se inicia con sesiones de planificación donde se define las historias de usuario más críticas esto asegura que cada característica del software responda efectivamente a las necesidades reales del usuario final.

4.2.2.1 Planificación de Módulo Auditoría

Se desarrollará en el software basado en los controles según la norma ISO 27001:2013 con tres módulos principales:

- **Control de acceso:** se implementaron pruebas para garantizar el acceso autorizado a redes, registro y cancelación de registro de usuarios, suministro de acceso de usuarios y sistema de gestión de contraseñas
- **Seguridad en las operaciones:** se incluyeron pruebas relacionadas con copias de respaldo, respaldo de la información, registro y seguimiento y registro de eventos
- **Seguridad de las comunicaciones:** se incluyeron las pruebas controles de redes, seguridad de los servicios de red y separación en las redes.

4.2.2.2 Planificación del Módulo Estados

Se desarrollará tres módulos principales que nos permite ver los estados en los equipos:

- **Pruebas de Equipo:** se evaluaron la autenticación de usuarios, el estado del sistema, los controladores, tareas en ejecución, información de software, así como la actividad del sistema operativo para garantizar su correcto funcionamiento y seguridad.
- **Pruebas de seguridad:** se verificaron la configuración del firewall, las actualizaciones instaladas, el estado del antivirus y la aplicación de parches de seguridad para proteger el sistema contra amenazas y vulnerabilidades conocidas.
- **Pruebas de red:** se evaluó el estado del tráfico de red, las conexiones activas, la configuración de red y las restricciones de acceso en el host para asegurar una conexión segura y confiable.

4.2.2.3 Planificación de las iteraciones

Para la construcción del software AuditaPro se desarrolla la siguiente tabla con un número de iteraciones para trabajar.

Tabla No III Planificación de las iteraciones

Iteración	Historia de Usuario	Tareas
1	Acceso al sistema	Diseño de interfaz Inicio Selección de Pruebas
2	Módulos prueba	Red
3		Pruebas de generales de un Equipo
4		Pruebas en equipos
5	Análisis General	Reporte

Conforme con los indicadores obtenidos empezamos la fase de planificación con un número de iteraciones para trabajar:

Tabla No IV Inicio Selección de Pruebas

HISTORIA DE USUARIO	
Número 2	Inició de selección de pruebas: Validación de los campos
Usuario: administrador	
Modificación de Historia: N/	Iteración asignada: 2
Prioridad en negocio: Medio (Alta/Medio /Baja)	Puntos estimados: 3
Riesgo en desarrollo: Medio (Alta/Medio /Baja)	Puntos reales: 2
Descripción: Validación del usuario en los campos asignados y validar que pueda acceder al módulo de las pruebas para el acceso a las pruebas.	
Observación: Ninguna.	
Fuente: Elaboración Propia	

Tabla No V Módulos Pruebas

HISTORIA DE USUARIO	
Número 3	Módulos pruebas: Red Pruebas Generales en un equipo Reporte
Usuario: administrador	
Modificación de Historia: N/	Iteración asignada: 3
Prioridad en negocio: Alto (Alta/Medio /Baja)	Puntos estimados: 3
Riesgo en desarrollo: Alto (Alta/Medio /Baja)	Puntos reales: 2
Descripción: En este campo es donde el usuario puede ingresar a realizar todas las pruebas que estén disponibles	
Observación: Tiene como objetivo principal ayudar a las organizaciones a evaluar, mejorar y mantener la seguridad de sus sistemas y activos de información de acuerdo con los estándares establecidos, garantizando así la protección de información y mitigar los riesgos de seguridad.	
Fuente: Elaboración Propia	

Tabla No VI: Análisis General.

HISTORIA DE USUARIO	
Número 4	Análisis General: Pruebas en equipos
Usuario: administrador	
Modificación de Historia: N/	Iteración asignada: 4
Prioridad en negocio: Alto (Alta/Medio /Baja)	Puntos estimados: 3
Riesgo en desarrollo: Alto (Alta/Medio /Baja)	Puntos reales: 2
Descripción: En este campo se pondrá a prueba el software en equipos para ver su rendimiento	
Observación: Este análisis garantiza que las organizaciones cumplen con las mejores prácticas de seguridad, protege sus activos de información y está preparada para enfrentar amenazas y riesgos en un entorno real.	
Fuente: Elaboración Propia	

Tabla No VII Diseño de interfaz inicio de selección de pruebas

Tarea de ingeniería	
Número: 1	Número de historia 1
Nombre de la tarea: Diseño de interfaz inicio de sesión	
Tipo de tarea: Diseño	Puntos estimados: 1
Fecha de inicio: 02/08/2023	Fecha fin: 10/08/2023
Programador responsable: Juan David Argoti Puchana	
Descripción: Buscar el mejor diseño y los colores adecuados para dar un estilo único.	
Fuente: Elaboración Propia	

Tabla No VII Inicio de selección de pruebas

Tarea de ingeniería	
Número: 2	Número de historia 2
Nombre de la tarea: Inicio de selección de pruebas	
Tipo de tarea: Diseño	Puntos estimados: 1
Fecha de inicio: 10/08/2023	Fecha fin: 15/08/2023
Programador responsable: Juan David Argoti Puchana	
Descripción: Validar que los campos asignados funcionen correctamente.	
Fuente: Elaboración Propia	

Tabla No IX Módulo de pruebas

Tarea de ingeniería	
Número: 3	Número de historia 3
Nombre de la tarea: Módulo de Pruebas	
Tipo de tarea: Diseño	Puntos estimados: 1
Fecha de inicio: 15/08/2023	Fecha fin: 26/09/2023
Programador responsable: Juan David Argoti Puchana	
Descripción: Validar que los campos asignados funcionen correctamente	
Fuente: Elaboración Propia	

Tabla No X Análisis General

Tarea de ingeniería	
Número: 3	Número de historia 4
Nombre de la tarea: Análisis General	
Tipo de tarea: Pruebas	Puntos estimados: 4
Fecha de inicio: 26/09/2023	Fecha fin: 14/09/2023
Programador responsable: Juan David Argoti Puchana	
Descripción: En este campo se debe exportar el software, validar en diferentes equipos, análisis de los resultados obtenidos.	
Fuente: Elaboración Propia	

4.2.2.4 Planificación de la clasificación de las pruebas

Se detallaron las actividades para clasificar los scripts su detalle y al módulo que pertenece así se establece la responsabilidad de cada tarea.

Tabla No XI. Módulo Control de acceso

Script No	Detalle	Librerías	Módulo que pertenece
1	Control: solo se debe permitir acceso de los usuarios a la red y a los servicios de red para lo que hayan sido autorizados específicamente.	SOCKET DATETIME	9.1.2 Acceso a redes y servicios en red.
2	Control: se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SOCKET DATETIME PSUTIL	9.2.1 Registro y cancelación de registro de usuarios
3	Control: se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SOCKET DATETIME SUBPROCESS	9.2.2 Suministro de acceso de usuarios
4	Control: los sistemas de gestión de contraseñas deben de ser interactivos y deben asegurar la calidad de las contraseñas	SECRETS STRING SOCKET DATETIME	9.4.3 Sistema de gestión de contraseñas

Tabla XII. Módulo Seguridad en las Operaciones

Script No	Detalle	Librerías	Módulo que pertenece
5	Objetivo: Proteger contra la pérdida de datos.	SOCKET DATETIME OS	12.3 Copias de respaldo
6	Control: se debe hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a pruebas regularmente de acuerdo con una política de copias de respaldo acordadas.	SOCKET DATETIME OS	12.3.1 Respaldo de la información
7	Objetivo registrar eventos y generar evidencia.	SOCKET DATETIME SUBPROCESS	12.4 Registro y seguimiento
8	Control: se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SOCKET DATETIME SUBPROCESS	12.4.1 Registro de eventos

Tabla No VII / 13 Seguridad en las comunicaciones

Script No	Detalle	Librerías	Módulo que pertenece
9	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SOCKET DATETIME SUBPROCESS	13.1.1 Controles de redes
10	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios presten internamente o se contrate externamente.	SOCKET DATETIME	13.1.2 Seguridad de los servicios de red
11	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SOCKET DATETIME	13.1.3 Separación en las redes

Tabla No XIV Módulo Pruebas de Equipo

Script No	Detalle	Librerías	Módulo que pertenece
12	Verificar la capacidad del sistema para autenticar usuarios locales y garantizar la seguridad de las cuentas de usuario con el fin de verificar si los usuarios que fueron asignados tienen el acceso autorizado.	SOCKET DATETIME SUBPROCESS	Autenticación De Usuarios Locales
13	Determinar cuándo se inició el sistema por última vez.	SOCKET DATETIME SUBPROCESS	Fecha Última Vez Que Se Inició El Sistema
14	Identifica los controladores de hardware y software instalados en el sistema, se proporciona una lista de los contadores que pueden ser útil para garantizar que todos estén actualizados y funcionando correctamente.	SOCKET DATETIME SUBPROCESS	Listar Controladores Del Sistema
15	Enumera las tareas en ejecución en el sistema para supervisar el rendimiento y la utilización de recursos lo que ayuda a identificar posibles problemas de rendimiento.	SOCKET DATETIME SUBPROCESS	Listar Tareas De Ejecución
16	Se proporciona el modelo de la placa base, lo que puede ser útil para futuras actualizaciones.	SOCKET DATETIME PSUTIL	Muestra El Modelo De La Placa Base
17	Se proporciona el número de serie de la BIOS que es importante para el soporte técnico y la gestión del hardware.	SOCKET DATETIME SUBPROCESS RE	Muestra el número de serie de la BIOS
18	Se mostrará una lista de programas instalados, lo que es útil para la gestión del software y la seguridad.	SOCKET DATETIME SUBPROCESS	Nombre de los programas instalados
19	Obtener información general sobre el sistema como el hardware, el sistema operativo y otros detalles relevantes, lo que es útil para el mantenimiento y la administración.	SOCKET DATETIME SUBPROCESS	Ver Información Del Sistema

20	Su principal función es contar la cantidad de programas instalados en el sistema lo que es útil para el soporte técnico y la seguridad del equipo.	SOCKET DATETIME SUBPROCESS	Verificar Cuántos Programas Están Instalados
21	Determinar si el sistema operativo está activo lo que es crucial para el funcionamiento general del sistema.	SOCKET DATETIME WINREG	Verificar Si El Sistema Operativo Está Activo

Tabla No XV pruebas de seguridad

Script No	Detalle	Librerías	Módulo que pertenece
22	El objetivo es asegurarse de que las reglas de seguridad estén correctamente establecidas.	SOCKET DATETIME SUBPROCESS	Muestra La Configuración Del Firewall De Windows
23	Proporciona una lista de las actualizaciones, lo que es importante para garantizar que el sistema esté al día en términos de seguridad, funcionalidad y protegido.	SOCKET DATETIME SUBPROCESS	Ver Actualizaciones Instaladas
24	Realizar la verificación del Firewall para asegurar que esté habilitado y funcionando correctamente, lo que es esencial para la seguridad del sistema.	SOCKET DATETIME SUBPROCESS	Verificación Del Firewall
25	Se enfoca en obtener información sobre la protección antivirus incluyendo el nombre del producto y el estado de la protección.	SOCKET DATETIME WINREG	Verificar Estado del Antivirus
26	Verificar si se han aplicado todos los parches de seguridad necesarios en el sistema para protegerlo contra vulnerabilidades conocidas.	SOCKET DATETIME WIN32COM.CLIENT	Verificar Parches De Seguridad En El Equipo

Tabla No XVI Módulo Pruebas de Red

Script No	Detalle	Librerías	Módulo que pertenece
27	Evaluar el estado actual del tráfico de red, el fin de verificar patrones de tráfico sospechoso, el tráfico de red puede ser útil para identificar problemas de congestión o actividad no autorizada en red.	SOCKET DATETIME SUBPROCESS	Estado Del Tráfico De Red
28	Se enumeran las conexiones de red activas en el sistema para identificar quién está accediendo a la red.	SOCKET DATETIME SUBPROCESS	Lista De Las Conexiones De Red Activas
29	Obtiene información detallada sobre la configuración y el estado de la red, como dirección IP entre otros, lo que es importante para la configuración y la solución de problemas de red.	SOCKET DATETIME SUBPROCESS	Mostrar Información De Red
30	Verifica si existen restricciones de acceso en el host que puedan afectar la conectividad o la seguridad de la red.	SOCKET DATETIME	Verificar Restricciones En El Host
31	Verifica una conexión a un sitio web conocido y verificar si la conexión se establece correctamente	SOCKET DATETIME URLLIB.REQUEST	Verificar Conectividad a Internet

4.2.3 Diseño del software AuditaPro

En esta sección, se presenta una guía de uso del software AuditaPro. Al acceder, el usuario encontrará un enunciado de bienvenida que lo orientará en las actividades que desea realizar. El menú principal consta de dos botones:

- **Auditoría:** Este botón dirige al usuario a una serie de actividades conforme a la norma ISO 27001:2013.

- **Módulo Estados**: Este botón lleva al usuario a una variedad de pruebas diseñadas para validar el estado de seguridad de su equipo.

Fig. No 2 menú selección

Fuente: Elaboración propia.

Al hacer clic en el botón "Auditoría", se desplegará una nueva ventana con cuatro opciones:

Botón 1. / 9. Controles de acceso

En esta ventana control de acceso donde esta ubicados en cuatros botones para que el usuario pueda hacer las pruebas que puede realizar el usuario el objetivo es garantizar la seguridad de la información y la integridad de los sistemas informáticos en una organización a través de la implementación de los controles efectivos, esto se logra mediante la gestión adecuada de la identificación de los posibles riesgos y así poder cumplir con los estándares establecidos con base al control (9) de la Norma ISO 27001:

A 9. CONTROL DE ACCESO.

- 9.1.2 Acceso a redes y servicios en red.
- 9.2.1 Registro y cancelación de registro de usuarios
- 9.2.2 Suministro de acceso de usuarios
- 9.4.3 Sistema de gestión de contraseñas

Botón 2. / 12. Seguridad de las operaciones,

En esta ventana Se despliega la ventana llamada control seguridad en las operaciones donde esta ubicados en cuatros botones para que el usuario pueda realizar las pruebas, su objetivo es garantizar la seguridad de la información de la organización a través de la relación de pruebas accesibles a los usuarios y la promoción de una cultura de seguridad sólida y proactiva. Nuevamente bajo estándares establecidos con base al control (12) de la Norma ISO 27001:

A 12. SEGURIDAD EN LAS OPERACIONES.

- 12.3 Copias de respaldo
- 12.3.1 Respaldo de la información
- 12.4 Registro y seguimiento
- 12.4.1 Registro de eventos

Botón 3. /13. Seguridad de las Telecomunicaciones

En esta ventana llamada Seguridad de las comunicaciones están ubicados en cuatros botones para que el usuario pueda realizar las pruebas, su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información transmitida a través de redes y sistemas de comunicaciones en un entorno donde cada vez es más interconectado y digitalizado. Como se puede apreciar basado en los estándares establecidos en el control (13) de la Norma ISO 27001:

A 13 SEGURIDAD DE LAS COMUNICACIONES

- 13.1.1 Controles de redes
- 13.1.2 Seguridad de los servicios de red
- 13.1.3 Separación en las redes

Botón 4 / Módulo de reportes

En esta ventana se encuentran los resultados obtenidos cuando el usuario da clic en el botón guardar el reporte. Ver figura 3.

Fig. No 3 Menú auditoría

Fuente: Elaboración propia.

Para regresar al menú se da clic en el botón inicio que nos devuelve a la anterior interfaz / ventana módulo estados.

Ventana Módulo Estados

Se despliega la ventana llamada pruebas de estados, estas pruebas se encuentran separadas en tres categorías: Pruebas de equipo, pruebas de seguridad y pruebas de red. Las pruebas mencionadas están diseñadas para evaluar tanto la seguridad como el estado general de un sistema informático, con el objetivo primordial de asegurar su protección frente a diferentes tipos de amenazas de seguridad.

Ventana Pruebas de equipo

- Autenticación De Usuarios Locales
- Fecha Última Vez Que Se Inició El Sistema
- Listar Controladores Del Sistema
- Listar Tareas De Ejecución
- Muestra El Modelo De La Placa Base
- Muestra el número de serie de la BIOS
- Nombre de los programas instalados
- Ver Información Del Sistema
- Verificar Cuántos Programas Están Instalados
- Verificar Si El Sistema Operativo Está Activo

Ventana Pruebas de Seguridad

- Muestra La Configuración Del Firewall De Windows
- Ver Actualizaciones Instaladas.
- Verificación Del Firewall
- Verificar Estado del Antivirus
- Verificar Parches De Seguridad En El Equipo

Ventana Pruebas de Red

- Estado Del Tráfico De Red
- Lista De Las Conexiones De Red Activas
- Mostrar Información De Red
- Verificar Restricciones En El Host
- Verificar Conectividad a Internet

Fig. No 4 Menú Estados

Fuente: Elaboración propia.

Para ir al menú de reportes se puede dar clic en el botón módulo reportes que lo dirigirá a la venta reportes.

Ventana módulo reportes

En esta ventana se encontrarán los resultados obtenidos cuando el usuario desee guardar el reporte.

Fig. No 5 Menú Reportes

Fuente: Elaboración propia.

El desarrollo del programa abarca la creación de un manual de usuario detallado, titulado **"Anexo 3: Manual de Usuario AuditaPro"**. Proporciona instrucciones precisas para la correcta utilización del software, garantizando que los usuarios puedan aprovechar todas sus funcionalidades de manera eficiente y efectiva.

El manual de usuario es un componente esencial del programa, ya que facilita la comprensión y aplicación de las herramientas ofrecidas, asegurando que los usuarios puedan llevar a cabo las pruebas, Además, el manual está diseñado para ser intuitivo y accesible, permitiendo a los usuarios de todos los niveles de experiencia tecnológica seguir las instrucciones sin dificultad, lo que contribuye significativamente a la usabilidad y adopción del software en diversas organizaciones. **Ver Anexo 3 Manual de usuario AuditaPro.**

4.2.4 Entorno de desarrollo y herramientas para la Codificación para el software AuditaPro

Este software está basado en PyQt5, que se utiliza para una serie de módulos y pruebas relacionadas con la seguridad y la auditoría de sistemas, la estructura principal se compone de varias ventanas que pueden lanzarse unas desde otras.

Estructura y Navegación

Ventana principal: es la ventana de inicio y permite al usuario a seleccionar entre diferentes módulos como auditoría y otros específicos marcados por el botón correspondiente. Carga su diseño desde un archivo IU y puede lanzar otras ventanas, cada una de estas ventanas representa a un módulo diferente dedicado a un área específica de pruebas o de auditoría estas ventanas permiten realizar pruebas específicas y visualizar los resultados. También pueden volver a la ventana anterior y son nodales lo que significa que bloquea la interacción con otras ventanas hasta que se cierren.

Funcionalidades de pruebas

Cada módulo tiene botones que al ser presionados ejecutar Scripts de Python que llevan a cabo pruebas específicas, los resultados se capturan y se muestran en la interfaz, muchas ventanas incluyen la opción de "Marcar Todos" para seleccionar todas las pruebas y a la vez y un ProgressBar para mostrar el progreso de las pruebas que se están ejecutando.

Gestión de errores y rutas de archivos

Las rutas de los archivos IU se generan dinámicamente usando la ubicación del archivo script actual lo que facilita la adaptabilidad del código a diferentes entornos de ejecución, se maneja los errores de archivos no encontrados especialmente cuando se busca un archivo IU que no existe.

Ejecución de Scripts

La ejecución de scripts se maneja mediante llamadas a Subprocess permitiendo ejecutar scripts externos de Python directamente de la interfaz gráfica y se captura su salida.

Integración y modularidad

La aplicación está diseñada de manera modular, permitiendo fácil adición o

modificación de los módulos sin afectar el resto del sistema, utiliza Pyqt5 para la carga de interfaces de usuario desde archivos .ui lo que facilita el diseño visual sin modificar el código fuente Python.

Entorno de desarrollo

- **Visual Studio Code**: Utilizado como el IDE principal para el desarrollo del código debido a su versatilidad y soporte extensivo para Python y otras tecnologías.

Lenguaje de programación

- **Python 3.10.6**: elegido por su simplicidad y eficacia en el manejo de scripts y automatización de tareas crucial para la validación de estados de seguridad

Diseño de interfaz y gestión de base de datos

- **Qt Designer 5.14.1:** usado para diseñar la interfaz gráfica, facilitando la creación de elementos visuales interactivos.
- **Django 5.0.3** Framework de desarrollo web para implementar la interfaz web del software.
- **SQLite:** Motor de base de datos elegido por su ligereza y capacidad de integrarse fácilmente con aplicaciones de escritorio y web desarrolladas en Python.

Librerías y módulos utilizados

Librerías principales:

- **Socket:** para la comunicación de red y la obtención de información sobre las conexiones.
- **Datetime:** usada para marcar eventos y operaciones con la fecha y hora exacta.
- **Psutil:** proporciona información sobre los procesos y el sistema (como uso de CPU, memoria, discos entre otros) esencial para la monitorización de la salud del sistema.
- **Subprocess:** permite la elección de comandos y procesos del sistema operativo, útil

para pruebas de seguridad y gestión de tareas.

- **Os:** Utilizado para interactuar con el sistema operativo, manejar archivos, directorios y la información del sistema.
- **Secrets, string**: Generación de cadenas seguras, crucial para pruebas que involucren directorios datos sensibles.
- **Re**: para trabajo con expresiones regulares.
- **Winreg, win32com.client**: específicos para interacciones con el registro de Windows y la automatización de tareas en el entorno de Windows.

- **PyQt5:** Utilizada para integrar la interfaz gráfica diseñando con Qt Designer en la aplicación de Windows incluye los módulos
- **Uic:** Carga de archivos .ui diseñados con Qt Designer.
- **QtCore, Qt Widgets:** Básicos para la funcionalidad de la interfaz de usuario, manejo de eventos y widgets.
- **QTimer**: manejo de operaciones basadas en el tiempo dentro de la interfaz gráfica.

4.2.5 Pruebas de funcionalidad del software AuditaPro

Se hace la elección de cada uno de los scripts y se capturan los resultados
Ejecución del primer Script 1 prueba 9.1.2 Acceso a redes y servicios en red.

Fig. No 6 Prueba / 9. Control de Acceso

Fuente: Elaboración propia.

Como se puede observar en la figura 6, la ventana describe el nombre de la prueba, el nombre del equipo, la fecha que se realiza la prueba y el resultado obtenido. En este caso, los puertos que se encuentran abiertos y cerrados. Sí gusta ver la totalidad de las pruebas que se pueden ejecutar con el programa, se recomienda revisar el **"Anexo 3: Manual de Usuario AuditaPro"**, donde se proporciona instrucciones precisas para la correcta utilización del software, garantizando que los usuarios puedan aprovechar todas sus funcionalidades de manera eficiente y efectiva.

4.3 Evaluar la efectividad del software en un entorno real.

Para el "Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real", se propuso crear una lista de chequeo detallada que permita validar las pruebas del software AuditaPro. Esta lista de chequeo será esencial para asegurar que el software cumple con todos los requisitos necesarios para una implementación exitosa en

diferentes entornos de operación. A continuación, se resume el enfoque y los elementos clave de esta lista de chequeo:

Objetivos de la Lista de Chequeo

Validar la Conformidad con ISO 27001: Asegurarse de que todas las funcionalidades del software cumplen con los estándares establecidos en la norma ISO 27001 para la seguridad de la información.

Comprobar la Eficacia del Software: Verificar que el software efectivamente identifica vulnerabilidades de seguridad en diversos entornos de prueba.

Evaluar la usabilidad: Confirmar que el software es fácil de usar para los usuarios finales, independientemente de su nivel de conocimientos técnicos.

Identificar Problemas de Compatibilidad: Detectar cualquier problema de compatibilidad el sistema operativo.

Componentes de la Lista de Chequeo:

Pruebas Funcionales: Revisar que cada módulo (Control de Acceso, Seguridad en las Operaciones, Seguridad de las Comunicaciones, entre otros) funcione según lo previsto.

Pruebas de Estado: Validar que las pruebas de equipo, seguridad y red proporcionan resultados precisos y consistentes.

Evaluación de Seguridad: Confirmar que el software identifica todas las brechas de seguridad conocidas durante las pruebas y que ofrece soluciones o recomendaciones para mitigarlas.

Metodología de Aplicación.

Implementación Sistemática: Aplicar la lista de chequeo en cada uno de los computadores que se van a analizar.

Modelo: Lista de chequeo conforme a la plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)

Reporte de Pruebas Funcionales Conforme a la guía Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)	

Título de la prueba	Prioridad	Numero de la prueba	Fecha de la prueba
Verificación de los módulos de auditoria y estados	Alta	Del nuero 1 a la 31	Día/Mes/año
Descripción de la prueba	**Prueba diseñada por**	**Prueba ejecutada por**	**Fecha de ejecución**
Software AuditaPro	Estudiante: Juan David Argoti Pucha	Estudiante: Juan David Argoti Pucha	Día/Mes/año

Descripción de la prueba

El software AuditaPro está diseñado para validar la seguridad de equipos mediante la ejecución de pruebas en condiciones reales, garantizando así su adecuando funcionamiento				
No Scripts	Descripción	Modulo Perteneciente	Cumple su función	Observación
1	9.1.2 Acceso a redes y servicios en red	Prueba 9.Control de Acceso	SI ☐ NO ☐	
2	9.2.1 Registro y cancelación de registro de usuarios		SI ☐ NO ☐	
3	9.2.2 Suministro de acceso de usuarios		SI ☐ NO ☐	
4	9.4.3 Sistema de gestión de contraseñas		SI ☐ NO ☐	
5	12.3 Copias de respaldo	Pruebas 12.Seguridad en las Operaciones.	SI ☐ NO ☐	
6	12.3.1 Respaldo de la información		SI ☐ NO ☐	
7	12.4 Registro y seguimiento		SI ☐ NO ☐	
8	12.4.1 Registro de eventos		SI ☐ NO ☐	
9	13.1.1 Controles de redes	Pruebas 13.Seguridad en las Comunicaciones	SI ☐ NO ☐	
10	13.1.2 Seguridad de los servicios de red		SI ☐ NO ☐	
11	13.1.3 Separación en las redes		SI ☐ NO ☐	
12	Autenticación De Usuarios Locales	Pruebas de equipo	SI ☐ NO ☐	
13	Listar Controladores Del Sistema		SI ☐ NO ☐	
14	Muestra El Modelo De La Placa Base		SI ☐ NO ☐	
15	Nombre de los programas instalados		SI ☐ NO ☐	
16	Verificar Cuantos Programas Están Instalados		SI ☐ NO ☐	

17	Fecha Última Vez Que Se Inició El Sistema		SI ☐ NO ☐	
18	Listar Tareas De Ejecución		SI ☐ NO ☐	
19	Ver Información Del Sistema		SI ☐ NO ☐	
20	Muestra el número de serie de la BIOS		SI ☐ NO ☐	
21	Verificar Si El Sistema Operativo Está Activo		SI ☐ NO ☐	
22	Muestra La Configuración Del Firewall De Windows	Pruebas de seguridad	SI ☐ NO ☐	
23	Verificar Parches De Seguridad En El Equipo		SI ☐ NO ☐	
24	Ver Actualizaciones Instaladas		SI ☐ NO ☐	
25	Verificación Del Firewall		SI ☐ NO ☐	
26	Verificar Estado del Antivirus		SI ☐ NO ☐	
27	Estado Del Tráfico De Red	Pruebas de red	SI ☐ NO ☐	
28	Mostrar Información De Red		SI ☐ NO ☐	
29	Lista De Las Conexiones De Red Activas		SI ☐ NO ☐	
30	Verificar Restricciones En El Host		SI ☐ NO ☐	
31	Verificar Conectividad a Internet		SI ☐ NO ☐	

_____
Firma Estudiante

_____
Firma con quien se hizo la prueba

Fig. No 7 Formato Lista De Chequeo Pruebas

Para ver los resultados completos registrados en la lista de chequeo se puede revisar el **Anexo 5**

5. Análisis y discusión de resultados

5.1 Análisis Detallado de Resultados: Integrando Objetivos y Antecedentes de Investigación.

Partiendo de lo planteado en el primer objetivo específico referente a la búsqueda, consulta y estudio del arte para analizar las herramientas y técnicas necesarias que permitan comprender los distintos estados de seguridad que afectan a los sistemas informáticos; se llevó a cabo una investigación donde se destaca la importancia de la colaboración entre sectores público y privado en la ciberseguridad. Sobresalen varios estudios y recursos a nivel de Colombia e internacional donde se resalta la importancia del hacking ético, la gestión de vulnerabilidades, las pruebas de penetración y las auditorías de seguridad, así como las iniciativas locales en la región de Nariño, destacando la implementación de sistemas de seguridad de la información basados en normativas ISO, la infraestructura de red segura en empresas y las auditorías enfocadas en fortalecer los procesos de control. Aunque se consideraron metodologías como OSSTMM, ISSAF y NIST SP800-53, no se optó por su implementación directa debido a su enfoque específico y robusto, que no se alinea completamente con los objetivos versátiles del proyecto, el cual se orienta a pequeñas y medianas empresas con usuarios de un nivel técnico en fase de capacitación.

Se determinó la selección de la Norma ISO 27001:2013 como marco de referencia principal en sus dominios y controles, teniendo presente que estos recursos garanticen el alcance del software AuditaPro permitiendo escalar fácilmente a la versión actualizada Norma ISO 27001:2022.

Continuando con el segundo objetivo específico dentro del proyecto de investigación se determinó el uso y aplicación de la metodología Extreme Programming (XP) para garantizar la eficiencia y calidad del software basados en sus principios, valores y prácticas, esta decisión se realizó cuando el grupo investigador estaba conformado por dos integrantes, lo que facilitaba las prácticas primarias de la metodología: Programación de pares, Historias de usuario y ciclo

semanal entre otras, con lo cual se logró avanzar en este tipo de ejecución relacionando un flujo de trabajo constante y con sus respectivos entregables; lamentablemente, al iniciar el semestre del periodo 2024 el grupo se dividió, pero ya se había alcanzado un porcentaje importante en el desarrollo del software AuditaPro. Es en esta parte donde se puede apreciar la versatilidad y eficacia del uso de metodologías ágiles, específicamente de la XP para realizar proyectos con bajos recursos, tiempo limitado y múltiples iteraciones, a su vez y como el proyecto se fundamenta en la Norma ISO 27001 se determinó el diseño de módulos que aborden los controles necesarios para garantizar la revisión de estados de seguridad en entornos reales, priorizando la detección proactiva de vulnerabilidades y amenazas, de tal manera que con esta información permita una buena toma de decisiones en cuanto a buenas prácticas de seguridad.

Finalmente, y después de realizar las pruebas operativas al software AuditaPro verificando que se alcancen los requerimientos funcionales y no funcionales, se procedió al despliegue para poder realizar la ejecución del tercer objetivo, esta fase consiste en validar mediante pruebas de efectividad en diferentes equipos el desempeño del software. Existen metodologías y herramientas ampliamente difundidas para este tipo de ejecución, sin embargo, y continuando con el pensamiento de desarrollo ágil, se optó por el uso de un artefacto de validación de la metodología LINCE (INCIBE – Instituto Nacional de Ciberseguridad España), que consiste en una lista de chequeo que se adapta fácilmente a la aplicación en varios entornos sondeando procesos y estados de seguridad. La lista de chequeo resultó un instrumento de gran apoyo y versatilidad para cubrir de forma rápida y efectiva un número determinado de equipos, ya sea en entornos de trabajo individual o donde se encuentren varios equipos.

Entre los resultados obtenidos en el presente proyecto, vale la pena mencionar que se alcanza la hipótesis principal objeto la investigación; las pruebas realizadas en los equipos de la Empresa Social del Estado Pasto Salud ESE. Permitieron detectar resultados significativos en cuanto a: puertos abiertos, sistemas operativos desactualizados, Backup inactivos, licencias de software vencidas, y otras no conformidades que, por compromiso adquirido previamente con la organización, y en procura de la integridad y confidencialidad no se pueden presentar en este documento. Las vulnerabilidades y amenazas detectadas fueron gestionadas por la oficina de

Comunicaciones y Sistemas, registrando que en la actualidad todos los equipos cubren las normas básicas de seguridad y demostrando la efectividad del software.

Desarrollo del software específico: El texto detalla el desarrollo de un software dedicado a la validación de estados de seguridad en equipos informáticos mediante pruebas en entornos reales. Este enfoque específico sugiere una herramienta adaptada a las necesidades actuales de seguridad informática.

Reducción de riesgos y aumento de la conciencia: Se señala que el uso del software redujo significativamente los riesgos y amenazas cibernéticas para las empresas, además de aumentar la conciencia sobre prácticas de seguridad. Esto sugiere un impacto positivo en la protección de la información y la mejora de la seguridad de los equipos.

Funcionamiento General: La mayoría de los equipos testeados mostraron resultados positivos, indicando que el software funciona adecuadamente en distintas configuraciones y cumple con los objetivos propuestos.

Problemas de Ejecución: Se menciona que en algunos equipos el software no se ejecutó correctamente. Esto indica la necesidad de revisar la compatibilidad del software o posiblemente los requisitos mínimos del sistema.

Impacto y Percepción del Usuario: Las preguntas de la encuesta relacionadas con la percepción de los usuarios sugieren un alto interés y satisfacción con funciones que ayudan a identificar y corregir vulnerabilidades, así como la importancia de seguir normas internacionales como la ISO 27001.

Se anexa acta de verificación de resultados y la lista de chequeo conforme se hicieron las pruebas Anexo 4 y 5

CONCLUSIONES

Con base a los resultados y validación resultada se puede presentar las siguientes conclusiones:

Alta Percepción de la necesidad del software, reveló una fuerte conciencia y reconocimiento entre profesionales técnicos y tecnólogos sobre la importancia de verificar y mejorar la seguridad de los sistemas informáticos. Esta percepción subraya la necesidad y relevancia del software de validación de estados de seguridad, especialmente en entornos reales donde las amenazas son continuas y dinámicas. Los resultados de las pruebas en entorno real indican que el software cumple satisfactoriamente con las expectativas en términos de identificación de vulnerabilidades, conformidad con estándares de seguridad internacionales como ISO 27001. Estos resultados sugieren que el software adecuado para el uso en entornos corporativos que manejan datos sensibles.

Contribución a la Seguridad Mejorada en las Organizaciones: Las pruebas y validaciones realizadas del uso del software ayudó a mejorar significativamente la gestión de la seguridad en sus respectivas pequeñas y medianas empresas. Esto se traduce en una reducción de riesgos y exposición a amenazas cibernéticas, gracias a las capacidades proactivas del software para detectar amenazas de seguridad antes de que estos puedan causar daño significativo.

Impacto Educativo y de Concienciación: El proyecto también tuvo un efecto secundario positivo en términos de educación y concienciación sobre la ciberseguridad. Los participantes en la encuesta y los usuarios del software se volvieron más conscientes de las prácticas de seguridad y la importancia de la vigilancia regular, lo que contribuye a una cultura de seguridad más fuerte dentro de las organizaciones.

RECOMENDACIONES

Recomendaciones y Mejoras Identificadas: A pesar de los resultados positivos, sugirieron algunas áreas de mejora en interfaz, estas sugerencias son cruciales para el desarrollo continuo del software y su adaptación a las necesidades cambiantes de los usuarios finales. Priorizar características que permitan una detección proactiva y corrección continúa de vulnerabilidades en el software de validación de estados.

Ampliar la gama de pruebas: Incluir una diversidad de pruebas de seguridad en el software para garantizar una evaluación exhaustiva en entornos reales, tal como indican las preferencias de los encuestados.

Educación y capacitación: Ofrecer formación y recursos educativos sobre la importancia y el uso del software para maximizar su eficacia y asegurar que los usuarios finales comprendan su funcionamiento y beneficios.

Recomendación final: Integrar el programa a entornos virtuales que permitan un acceso a la información de manera más dinámica.

Bibliografía

[1] Y. C. E. S. Parra Barzola Liliana Milagros, «Repositorio Universidad de Guayaquil,» Octubre 2017. [En línea]. Available: http://repositorio.ug.edu.ec/handle/redug/24003. [Último acceso: 06 Septiembre 2023].

[2] D. Teruel Carrera, «Universitat oberta de catalunya,» Junio 2023. [En línea]. Available: https://openaccess.uoc.edu/handle/10609/148151. [Último acceso: 06 Septiembre 2023].

[3] P. d. i. d. s. l. d. i. 2020, «Programa de ingeniería de sistemas líneas de investigación 2020».

[4] «"BibGuru," Bibguru.com. [Online]. Available: https://app.bibguru.com/p/bc6aeded-28d2-499f-8cd1-ba5ef7fbd735. [Accessed: 10-Mar-2024].,» [En línea].

[5] O. C. S. García, «Universidad Nacional Abierta y a Distancia,» UNAD , 07 Agosto 2021. [En línea]. Available: https://repository.unad.edu.co/handle/10596/43494. [Último acceso: 06 Septiembre 2023].

[6] «[2] Edu.co. [Online]. Available: https://repositorio.itm.edu.co/handle/20.500.12622/5748. [Accessed: 10-Mar-2024].,» [En línea].

[7] G. U. I. Martín, «REPOSITORIO INSTITUCIONAL DE LA UNLP,» SEDICI, 12 Diciembre 2022. [En línea]. Available: http://sedici.unlp.edu.ar/handle/10915/147421. [Último acceso: 06 Septiembre 2023].

[8] r. p. S. P. L. Carolina, «Universidad Estatal Península de Santa Elena,» UPSE, 07 Junio 2022. [En línea]. Available: https://repositorio.upse.edu.ec/handle/46000/7727. [Último acceso: 06 Septiembre 2023].

[9] A. A. D. A. y. B. J. D. Alarcon, «Universidad Tecnológica del Perú,» Repositorio Institucional , 2021. [En línea]. Available: https://hdl.handle.net/20.500.12867/4906. [Último acceso: 07 Septiembre 2023].

[10] P. G. Salazar, «Hacker´s whitebook,» de *Hacker´s whitebook*, Moterrey, Nuevo León, Edición WhiteSuit Hacking, 2019, 2013, p. 563.

[11] F. R. d. l. C. Jo, «Universidad Nacional Santiago Antúnez de Mayolo,» Repositorio

Institucional UNASAM , Octubre 2017. [En línea]. Available: http://repositorio.unasam.edu.pe/handle/UNASAM/2626. [Último acceso: 08 Septiembre 2023].

[12] T. S. Huertas, «Universidad Nacional Abierta y a Distancia,» UNAD, 05 Enero 2023. [En línea]. Available: https://repository.unad.edu.co/handle/10596/54049. [Último acceso: 06 Septiembre 2023].

[13] J. A. C. Borda, «Universidad Nacional Abierta y a Distancia,» UNAD, 16 Octubre 2022. [En línea]. Available: https://repository.unad.edu.co/handle/10596/37182. [Último acceso: 07 Septiembre 2023].

[14] C. Pilay y R. Manuel, «Universidad Estatal Península de Santa Elena,» UPSE, 7 Abril 2021. [En línea]. Available: https://repositorio.upse.edu.ec/handle/46000/5754. [Último acceso: 16 Septiembre 2023].

[15] Willam Alfredo Inampues Villa y Daniel Esteban Lara Rosero, «SIRED,» Universidad de Nariño , 29 mayo 2018. [En línea]. Available: http://sired.udenar.edu.co/id/eprint/7836. [Último acceso: 13 Septiembre 2023].

[16] Christian David Naranjo López y David Esteban Gómez Coral , «Universidad de Nariño,» SIRED, 31 Julio 2017. [En línea]. Available: https://sired.udenar.edu.co/9080/. [Último acceso: 14 Septiembre 2023].

[17] Euler Remigio Basante Mora y Gilberth Andrey Ipaz, «Universidad de Nariño,» SIRED, 10 Julio 2016. [En línea]. Available: http://sired.udenar.edu.co/id/eprint/8594. [Último acceso: 14 Septiembre 2023].

[18] P. C. Borrero Ochoa, «Universidad Nacional Abierta y a Distancia,» UNAD, 17 Enero 2022. [En línea]. Available: https://repository.unad.edu.co/handle/10596/35641. [Último acceso: 06 Septiembre 2023].

[19] E. Moreira Alvarez, «Universidad Casa Grande,» Repositorio Digital , Abril 2023. [En línea]. Available: http://dspace.casagrande.edu.ec:8080/handle/ucasagrande/3965. [Último acceso: 06 Septiembre 2023].

[20] N. I. 27001:2013, «"Information technology - Security techniques - Information security

management systems - Requirements,» ISO , [En línea]. Available: https://www.normas-iso.com/iso-27001/. [Último acceso: 16 Septiembre 2023].

[21] D. M. C. Fauces, «Acerca de los virus informáticos: una amenaza persistente,» SiElo, 2011. [En línea]. Available: http://scielo.sld.cu/scielo.php?pid=S1029-30192011000200018&script=sci_arttext&tlng=pt. [Último acceso: 16 Septiembre 2023].

[22] Ekta Gandotra, Divya Bansal y Sanjeev Sofat, «Malware Analysis and Classification: A Survey,» *Scientific Research Open Access,* vol. 5, nº 2, p. 9, 2014.

[23] A. H. Dominguez, «Sistema para la detección de ataques PHISHING utilizando correo electrónico.,» *Telemática ,* vol. 17, nº 2, p. 11, 2018.

[24] D. R. C. &. N. M. Narváez, «Evaluación de ataques de Denegación de servicio DoS y DDoS, y mecanismos de protección,» *GEEKS DECC-REPORTS,* vol. 2, nº 1, p. 13, 2016.

[25] H. M. M. O. E. A. P. O. D. H. &. C. Ñ. C. M. Domínguez L., «Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple "Contraseñas", pruebas de concepto con software libre y su remediación,» *Revista Científica MASKANA,* vol. 7, nº 4, p. 9, 2016.

[26] P. Fernández Gayol, «Archivo Digital UPM Universidad Politécnica de Madrid,» Junio 2022. [En línea]. Available: https://oa.upm.es/71140/. [Último acceso: 16 Septiembre 2023].

[27] Ernesto Sánchez, Daniel Arias Figueroa, Álvaro Ignacio Gamarra y José Nelson Mayorga , «Implementación de un Servidor DNS Seguro basado en Pi-Hole utilizando,» Mayo 2020. [En línea]. Available: http://sedici.unlp.edu.ar/handle/10915/103557. [Último acceso: 16 Septiembre 2023].

[28] L. M. G.-M. y C. R. , «Universidad de Cordoba,» 2016. [En línea]. Available: http://hdl.handle.net/10396/15775. [Último acceso: 16 Septiembre 2023].

[29] Á. G. Vieites, «Auditoría de Seguridad Informática,» RA-MA, SA EDITORIAL Y PUBLICACIONES , Septiembre 2011. [En línea]. Available: https://books.google.es/books?hl=es&lr=&id=n6W6EAAAQBAJ&oi=fnd&pg=PA5&dq=auditor%C3%ADa+de+seguridad+inform%C3%A1tica+&ots=R2Pc-T5ZEG&sig=Z-eA5n5Rt5DG-

M5tW0RZjEp44KA#v=onepage&q=auditor%C3%ADa%20de%20seguridad%20inform%C3%A1tica&f=false. [Último acceso: 16 Septiembre 2023].

[30] O. D. Arango Gomez, «El ABC de la seguridad informática: guía práctica para entender la seguridad digital,» ITM Institución Universitaria Reacreditada en Alta Calidad , 2023. [En línea]. Available: http://hdl.handle.net/20.500.12622/5901. [Último acceso: 16 Septiembre 2023].

[31] E. M. J. Lenin, «Repositorio Digital,» Universidad Técnica del Norte , 26 Julio 2021. [En línea]. Available: http://repositorio.utn.edu.ec/handle/123456789/11368. [Último acceso: 10 Septiembre 2023].

[32] C. Bracho-Ortega, «Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio,» *Revista Científica MASKANA,* vol. 8, nº Vol. 8 (2017): Actas del V Congreso Ecuatoriano de Tecnologías de la Información y Comunicación - TIC.EC 2017, p. 13, 2017.

[33] I. J. Z. Santos, «Herramienta de armonización entre las normas,» Diciembre 2021. [En línea]. Available: https://repository.ucatolica.edu.co/server/api/core/bitstreams/0449721c-7693-4814-b868-def96fa9d462/content. [Último acceso: 16 Septiembre 2023].

[34] H. R. G. Brito, «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web,» *Revista Cubana de Ciencias Informáticas,* Vols. %1 de %2vol.12 no.4 La Habana oct.-dic. 2018, nº 4, 2018.

[35] M. Á. PÉREZ, «Aplicación de la metodología ITIL,» *Revista Espacios ,* vol. 39, nº 09, p. 17, 2018.

[36] Cárdenas Castillo, Claudia Jannethe y Casalins Jiménez, Juan Roberto, «UNAN Universidad Antonio Nariño,» Automatización de las auditorías , 17 11 2022. [En línea]. Available: http://repositorio.uan.edu.co/handle/123456789/7963. [Último acceso: 16 Septiembre 2023].

[37] M. ATT&CK, «ATT&CK Matrix for Enterprise,» [En línea]. Available: https://attack.mitre.org/. [Último acceso: 23 Septiembre 2023].

[38] O. T. TEN, «Open Web Application Security Project (OWASP). (2023). OWASP Top

Ten.,» (OWASP), [En línea]. Available: https://owasp.org/Top10/es/. [Último acceso: 24 Septiembre 2023].

[39] Sans, « "SysAdmin, Audit, Network, Security," SANS,» [En línea]. Available: https://www.sans.org/. [Último acceso: 24 Octubre 2023].

[40] Shodan, «Search Engine for the Internet of Everything,» [En línea]. Available: https://www.shodan.io/. [Último acceso: 24 Octubre 2023].

[41] NMAP.ORG, «Guía de referencia de Nmap (Página de manual),» [En línea]. Available: https://nmap.org/man/es/index.html. [Último acceso: 24 Octubre 2024].

[42] Metasploit, «The world's most used penetration testing framework,» [En línea]. Available: https://www.metasploit.com/. [Último acceso: 24 Octubre 2023].

[43] Nessus, «El estándar de oro global para la evaluación de vulnerabilidades,» Tenable, [En línea]. Available: https://es-la.tenable.com/products/nessus. [Último acceso: 29 Septiembre 2023].

[44] Wireshark, «The world's most popular network protocol analyzer,» [En línea]. Available: https://www.wireshark.org/. [Último acceso: 24 Octubre 2023].

[45] OpenVAS, «Vulnerability Management:,» [En línea]. Available: https://openwebinars.net/blog/que-es-openvas/. [Último acceso: 24 Setiembre 2023].

[46] «[2] R. G. Sierra, "Inicio," CCN-CERT, 18-Apr-2023. [Online]. Available: https://www.ccn-cert.cni.es/es/. [Accessed: 04-Mar-2024].,» [En línea].

[47] «[1] Cni.es. [Online]. Available: https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/2000-organismo-de-certificacion/4563-ccn-stic-2004-plantilla-del-informe-tecnico-de-evaluacion-de-la-certificacion-nacional-esencial-de-seguridad-lince/file.html.,» [En línea]. [Último acceso: 01 03 2024].

[48] C. Martín, «Esándares y normas ISO para mejorar la Ciberseguridad,» GlobalSuite, 05 Septiembre 2022. [En línea]. Available: https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/. [Último acceso: 10 Septiembre 2023].

[49] «"ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002," Normas ISO. [Online]. Available: https://www.normas-iso.com/iso-27001/.,» [En línea]. [Último acceso:

10 03 2024].

[50] «“Política de Protección de Datos Personales,” Ministerio de Ambiente y Desarrollo Sostenible, 04-Aug-2021. [Online]. Available: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/,» [En línea]. [Último acceso: 10 03 2024].

[51] «“Ley 527 de 1999 - Gestor Normativo,” Gov.co. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276.,» [En línea]. [Último acceso: 10 03 2024].

[52] «“LEY 594 DE 2000,” Gov.co. [Online]. Available: https://normativa.archivogeneral.gov.co/ley-594-de-2000/.,» [En línea]. [Último acceso: 10 03 2024].

[53] «“Ley 1266 de 2008 - Gestor Normativo,” Gov.co. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.,» [En línea]. [Último acceso: 10 03 2024].

[54] «“Ley 1221 de 2008 - Gestor Normativo,” Gov.co. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=31431.,» [En línea]. [Último acceso: 10 03 2024].

[55] «“Ley 1273 de 2009,” Gov.co. [Online]. Available: https://www.secretariajuridica.gov.co/node/279.,» [En línea]. [Último acceso: 10 03 2024].

[56] «“Ley 1341 de 2009 - Gestor Normativo,” Gov.co. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913.,» [En línea]. [Último acceso: 10 03 2024].

[57] «“Ley 1581 de 2012 - Gestor Normativo,” Gov.co. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.,» [En línea]. [Último acceso: 10 03 2024].

[58] «“Ley 1712 de 2014 - Gestor Normativo,” Gov.co. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882.,» [En línea]. [Último acceso: 10 03 2024].

[59] «“Ley 1915 de 2018 - Gestor Normativo,” Gov.co. [Online]. Available:

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87419.,» [En línea]. [Último acceso: 10 03 2024].

[60] «“Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia,” vol. 62, pp. 16–31, 2023.,» [En línea]. [Último acceso: 10 03 2024].

[61] Python, «Python is a programming language,» Guido Van Rossum, Febrero 1989. [En línea]. Available: https://www.python.org/psf-landing/. [Último acceso: 10 Septiembre 2023].

[62] «“socket — interfaz de red de bajo nivel — documentación de Python - 3.10.13,” Python.org. [Online]. Available: https://docs.python.org/es/3.10/library/socket.html.,» [En línea]. [Último acceso: 10 03 2024].

[63] «S. S. C. de 300 P. de R. P. T. U. I. M. el C. L. en el shell Scapy., “a. Comandos básicos,” Www.uv.mx. [Online]. Available: https://www.uv.mx/personal/angelperez/files/2018/09/Actividad-250918.pdf.,» [En línea]. [Último acceso: 10 03 2024].

[64] «Vay3t, “Hacking con Python 3: Capítulo 8 — Entendiendo Scapy,” Medium, 13-Dec-2020. [Online]. Available: https://vay3t.medium.com/hacking-con-python-3-capitulo-8-entendiendo-scapy-8bf619514d04.,» [En línea]. [Último acceso: 10 03 2024].

[65] «“importlib — La implementación de import,” Python documentation. [Online]. Available: https://docs.python.org/es/3/library/importlib.html.,» [En línea]. [Último acceso: 10 03 2024].

[66] «“subprocess — Gestión de subprocesos,” Python documentation. [Online]. Available: https://docs.python.org/es/3/library/subprocess.html.,» [En línea]. [Último acceso: 10 03 2024].

[67] «Juanweb, “Monitoreo del Sistema con Psutil en Python,” Códigos Python, 30-Sep-2023. [Online]. Available: https://codigospython.com/monitoreo-del-sistema-con-psutil-en-python/.,» [En línea]. [Último acceso: 10 03 2024].

[68] K. Beck, «Extreme Programming Explained,» de *Extreme Programming Explained*, Luisiana, Estados Unidos, Addison-Wesley; First Edition (1 Enero 1999), 1999, p. 190.

[69] A. J. Q. Vodniza, «“Guía de investigación parte 1 cuantitativa”,» Pasto Nariño , 1a ed ISBN: 9789588439129, 2009, p. 99.

[70] I. R. R. Crotte, «Tiempo de Educar,» Universidad Autónoma del Estado de México, 24 Diciembre 2011. [En línea]. Available: https://www.redalyc.org/pdf/311/31121089006.pdf. [Último acceso: 01 Octubre 2023].

[71] D. H. Benítez, «método científico y la filosofía como herramientas para generar conocimiento. Revista Filosofía UIS,» *Revista Filosofía UIS,* vol. 19, nº 1, p. 229, 2020.

[72] Raúl J. Martelo, Luis Moncaris y Luis Vélez, «Integración del Ábaco de Régnier, Encuestas y Lluvia de Ideas en la Definición de Variables Claves en Estudios Prospectivos,» *Scielo ,* vol. Inf. tecnol. vol.27 no.5 La Serena 2016, 2016.

[73] «[5] “Política de Protección de Datos Personales,” Ministerio de Ambiente y Desarrollo Sostenible, 04-Aug-2021. [Online]. Available: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/.,» [En línea]. [Último acceso: 10 2024].

Anexos

Anexo 1 Solicitud de encuesta realizada en septiembre del año 2022

San Juan de Pasto 12 de sept. De 22

Ingeniero
HARVEY ALEXIS VALLEJO NARVAEZ
Jefe Oficina Asesora Comunicaciones y Sistemas
Oficina de Comunicaciones
PASTO SALUD ESE

Asunto: Participación de encuesta

Cordial saludo

Con el fin de poder garantizar el trabajo de grado del estudiante Juan David Argoti **Puchana Código estudiantil i026215 del grado noveno titulada "Seguridad Informática Para La Detección De Intrusos Informáticos En Red A Través De Software Libre" solicito si es posible enviar la siguiente encuesta al personal que está bajo su supervisión con el fin de poder recolectar información válida para el desarrollo de la investigación.**

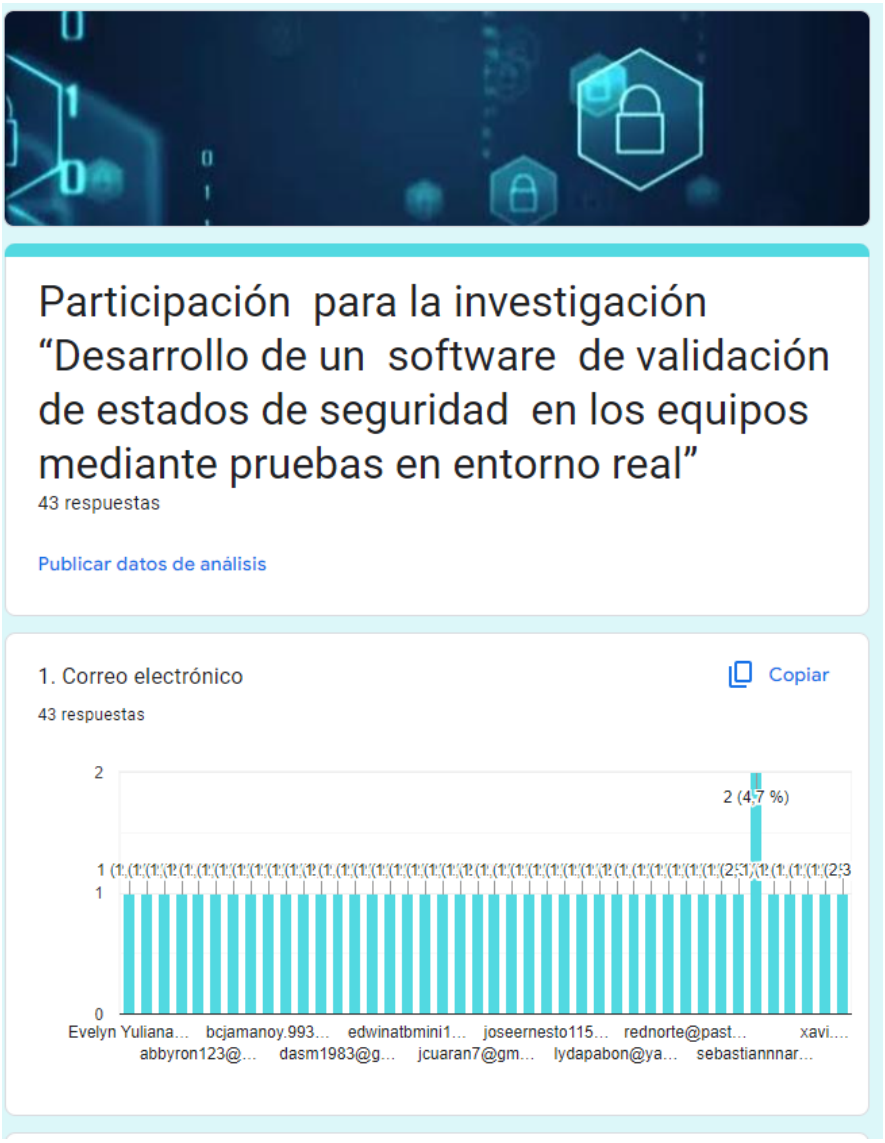
Link de la encuesta: https://docs.google.com/forms/d/e/1FAIpQLSfzRi4Rn-BMKWlEMpB81fjeMG7AOOUtGvXs1IqV5rbZzGJ3zA/viewform?usp=sf_link

Agradezco su participación y colaboración

Atentamente,

Juan David Argoti Puchana
Estudiante Ingeniería de sistemas
Código i026215
Cel. 3044790051
Correo electrónico
juanargoti2015@hotmail.com
juanargoti2020@gmail.com

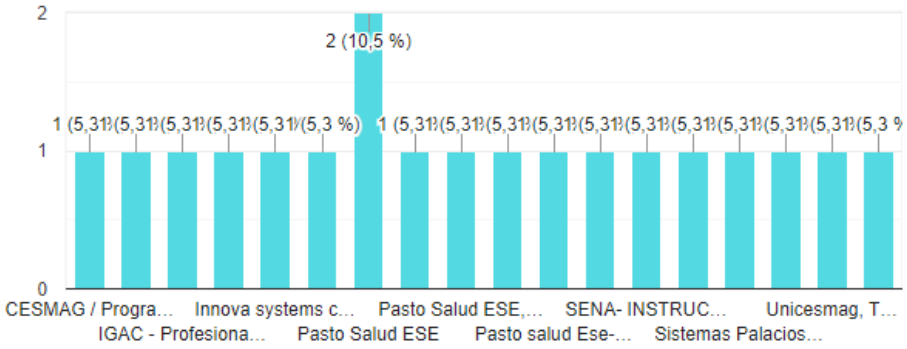
Anexo 2 Participación en la encuesta



3. ¿Actualmente, está empleado o colabora con alguna organización o empresa? En caso afirmativo, por favor, escriba el nombre de la empresa a la que pertenece y la función en el área que se desempeña"

Copiar

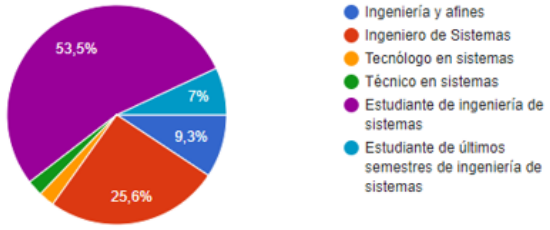
19 respuestas



4. Perfil

Copiar

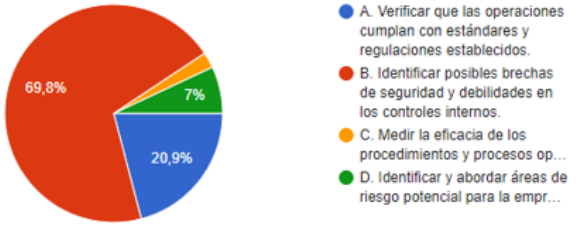
43 respuestas



Participación para la investigación "Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real" Sección sin título

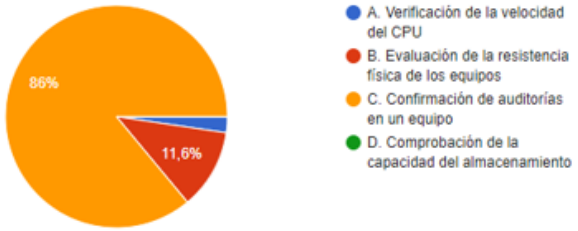
5. ¿Cuál es la importancia de realizar pruebas de auditoría? Copiar

43 respuestas



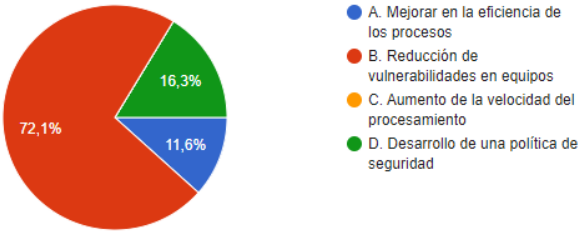
6. ¿Para usted en qué consiste la validación de estados de seguridad en equipos? Copiar

43 respuestas



7. ¿Qué beneficios cree se pueden obtener mediante el uso del software de validación de seguridad? Copiar

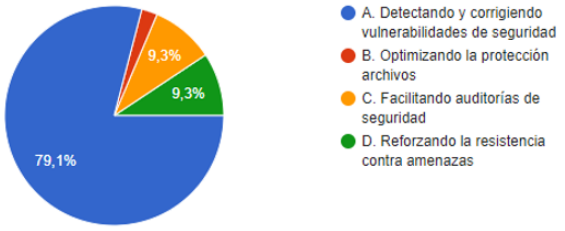
43 respuestas



8. ¿Cómo contribuiría un software de validación de estados con respecto a la ciberseguridad de los equipos?

Copiar

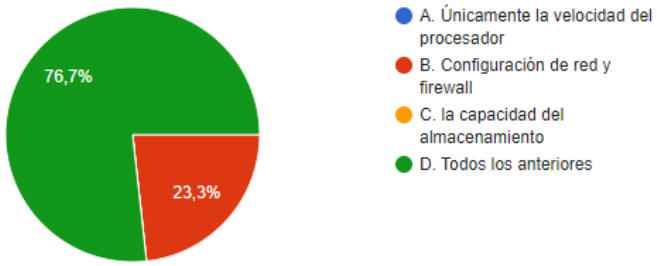
43 respuestas



9. ¿Qué factores se consideran al validar los estados de seguridad en los equipos?

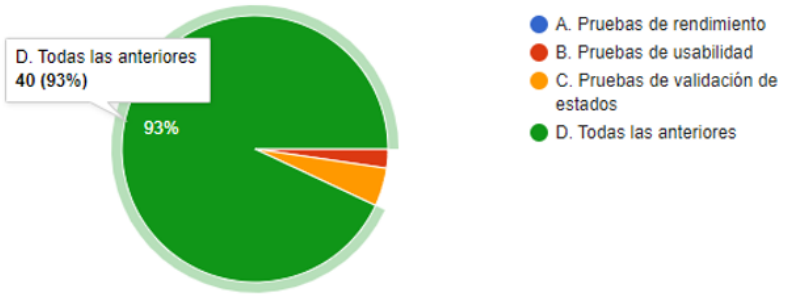
Copiar

43 respuestas



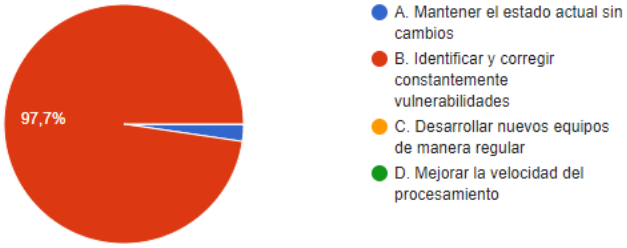
10. ¿Qué tipo de pruebas considera más pertinentes al realizar en un entorno real? Copiar

43 respuestas



11. ¿Qué espera de un software de validación de estados en la mejora continua de la seguridad de los equipos? Copiar

43 respuestas



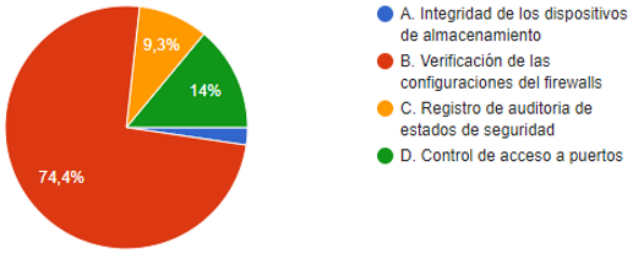
13. ¿Cuál es la principal ventaja de realizar pruebas en entorno real en comparación con pruebas en entornos virtuales? Copiar

43 respuestas

14. ¿Qué componentes a nivel de hardware considera se deben evaluar para garantizar la seguridad de los equipos?

Copiar

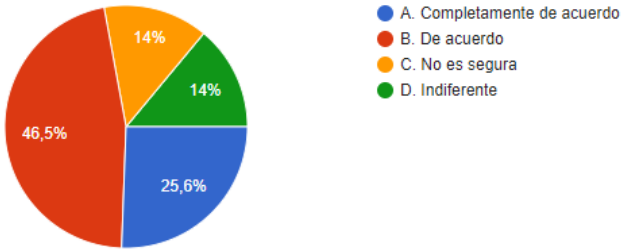
43 respuestas



15.¿Considera la opción de compartir desde servidor el Software a desarrollar para descarga e instalación viable y segura?

Copiar

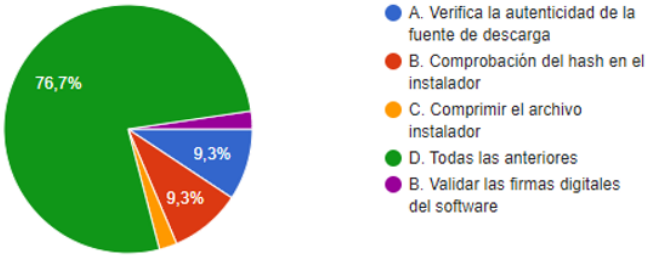
43 respuestas



Copiar

16. ¿Cómo considera usted se puede asegurar la integridad del software de validación de estados de seguridad al descargarlo del servidor.?

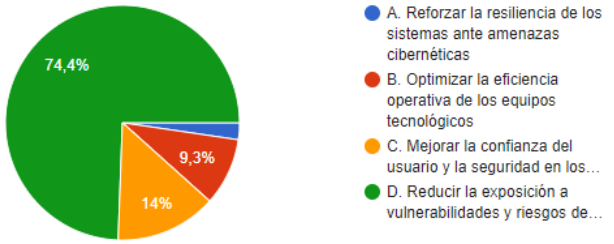
43 respuestas



Copiar

17. ¿Cuál es el impacto potencial de la validación de estados de seguridad en la pequeña y mediana empresa?

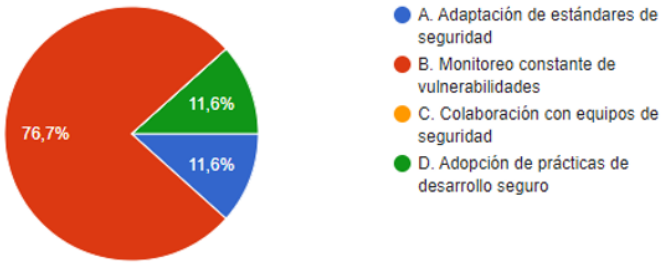
43 respuestas

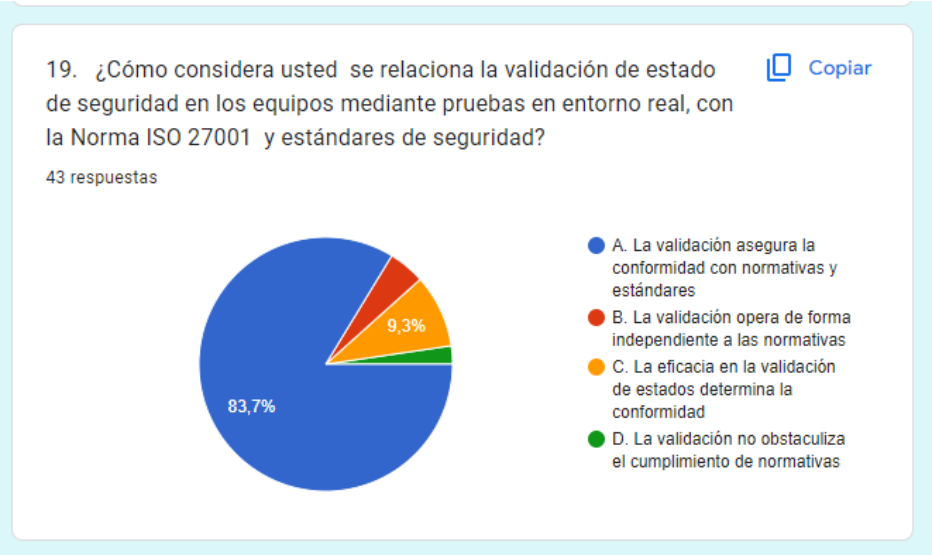


Copiar

18. ¿Cómo considera usted de la manera más efectiva que el software de validación de estados puede colaborar ante las amenazas de seguridad.?

43 respuestas





Anexo 3 Manual de usuario AuditaPro

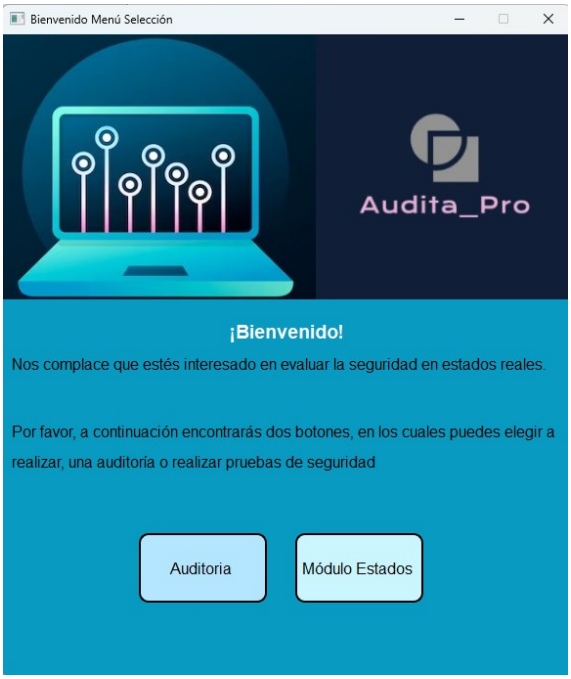


Fig. No 1 Menú selección

1. En esta ventana se encontrar con un enunciado de bienvenida para que al usuario para que lo pueda guiar en las actividades que él quiera realizar, en el primer botón llamado "Auditoría" que son unas actividades conforme a la norma ISO 27001 – 2013 y en el segundo botón "Módulo Estados" se encuentra una variedad de pruebas diseñadas para que el usuario pueda validar el estado de seguridad de su equipo.

- **Ventana Módulo auditoría de Pruebas ISO 27001 -2013**

En esta ventana se despliega la opción de cuatro botones:

Botón1. 9. Controles de acceso

Botón 2. 12. Seguridad de las operaciones,

Botón 3. 13. Seguridad de las Telecomunicaciones

Botón 4. Módulo de reportes

Fig. No 02 Selección de pruebas ISO 27001 – 2013

2. Ventana de Pruebas No 9 ISO 27001 -2013

Se despliega la ventana llamada control de acceso donde esta ubicados en cuatros botones para que el usuario pueda hacer las pruebas que puede realizar el usuario el objetivo es garantizar la seguridad de la información y la integridad de los sistemas informáticos en una organización a través de la implementación de los controles efectivos, esto se logra mediante la gestión adecuada de la identificación de las posibles riesgos y así poder cumplir con los estándares establecidos. [49]

- **A 9.CONTROL DE ACCESO.**
- 9.1.2 Acceso a redes y servicios en red.

- 9.2.1 Registro y cancelación de registro de usuarios
- 9.2.2 Suministro de acceso de usuarios
- 9.4.3 Sistema de gestión de contraseñas

Fig. 03 Ventana Pruebas No 9 Control de acceso

3. Ventana Pruebas No / 12 Pruebas seguridad en las operaciones ISO 27001 -2013

Se despliega la ventana llamada control seguridad en las operaciones donde esta ubicados en cuatros botones para que el usuario pueda realizar las pruebas su objetivo es garantizar la seguridad de la información de la organización a través de la relación de pruebas accesibles a los usuarios y la promoción de una cultura de seguridad sólida y proactiva. [49]

- **A 12. SEGURIDAD EN LAS OPERACIONES.**
- 12.3 Copias de respaldo
- 12.3.1 Respaldo de la información

- 12.4 Registro y seguimiento
- 12.4.1 Registro de eventos

Fig. 04 Ventana Pruebas No 12 Seguridad de las Operaciones

4. Ventana Pruebas No / 13 Seguridad de las Comunicaciones

Se despliega la ventana llamada Seguridad de las comunicaciones control seguridad donde esta ubicados en cuatros botones para que el usuario pueda realizar las pruebas que puede realizar el usuario, su objetivo proteger la confidencialidad, integridad y disponibilidad de la información transmitida a través de redes y sistemas de comunicaciones en un entorno donde cada vez es más interconectado y digitalizado [49].

- **A 13 SEGURIDAD DE LAS COMUNICACIONES**
- 13.1.1 Controles de redes
- 13.1.2 Seguridad de los servicios de red

- 13.1.3 Separación en las redes

Fig. 5 A 13 Seguridad de las comunicaciones

5. Ventana Módulo Estados

Se despliega la ventana llamada pruebas de estados les que se encuentran separadas en tres categorías pruebas de equipo, pruebas de seguridad y pruebas de red.

Fig. 6 Módulo Estados

1. Descripción Pruebas de Equipo

- **Autenticación De Usuarios Locales**

  Verificar la capacidad del sistema para autenticar usuarios locales y garantizar la seguridad de las cuentas de usuario con el fin de verificar si los usuarios que fueron asignados tienen el acceso autorizado.

- **Fecha Última Vez Que Se Inició El Sistema**

  Determinar cuándo se inició el sistema por última vez.

- **Listar Controladores Del Sistema**

  Identifica los controladores de hardware y software instalados en el sistema, se proporciona una lista de los contadores que pueden ser útil para garantizar que todos estén actualizados y funcionando correctamente.

- **Listar Tareas De Ejecución**

Enumera las tareas en ejecución en el sistema para supervisar el rendimiento y la utilización de recursos lo que ayuda a identificar posibles problemas de rendimiento.

- **Muestra El Modelo De La Placa Base**
  Se proporciona el modelo de la placa base, lo que puede ser útil para futuras actualizaciones.

- **Muestra el número de serie de la BIOS**
  Se proporciona el número de serie de la BIOS que es importante para el soporte técnico y la gestión del hardware.

- **Nombre de los programas instalados**
  Se mostrará una lista de programas instalados, lo que es útil para la gestión del software y la seguridad.

- **Ver Información Del Sistema**
  Obtener información general sobre el sistema como el hardware, el sistema operativo y otros detalles relevantes, lo que es útil para el mantenimiento y la administración.

- **Verificar Cuántos Programas Están Instalados**
  Su principal función es contar la cantidad de programas instalados en el sistema lo que es útil para el soporte técnico y la seguridad del equipo.

- **Verificar Si El Sistema Operativo Está Activo**
  Determinar si es sistema operativo está activo lo que es crucial para el funcionamiento general del sistema.

Las pruebas mencionadas están relacionadas con la evaluación y el análisis de un sistema informático o una computadora.

Fig. 7 Pruebas de Equipo

2. Descripción pruebas de Seguridad

- **Muestra La Configuración Del Firewall De Windows**

  El objetivo es asegurarse de que las reglas de seguridad estén correctamente establecidas.

- **Ver Actualizaciones Instaladas**.

  Proporciona una lista de las actualizaciones, lo que es importante para garantizar que el sistema esté al día en términos de seguridad, funcionalidad y protegido.

- **Verificación Del Firewall**

  Realizar la verificación del Firewall para asegurar que esté habilitado y funcionando correctamente, lo que es esencial para la seguridad del sistema.

- **Verificar Estado del Antivirus**

- Se enfoca en obtener información sobre la protección antivirus incluyendo el nombre del producto y el estado de la protección.

- **Verificar Parches De Seguridad En El Equip**o
  Verificar si se han aplicado todos los parches de seguridad necesarios en el sistema para protegerlo contra vulnerabilidades conocidas.

Estas pruebas están diseñadas para evaluar la seguridad y el estado de un sistema informático, estas pruebas ayudarán a garantizar que el sistema esté protegido contra amenazas de seguridad, esté al día en términos de actualizaciones y tenga una configuración adecuada para mantener un nivel adecuado de seguridad

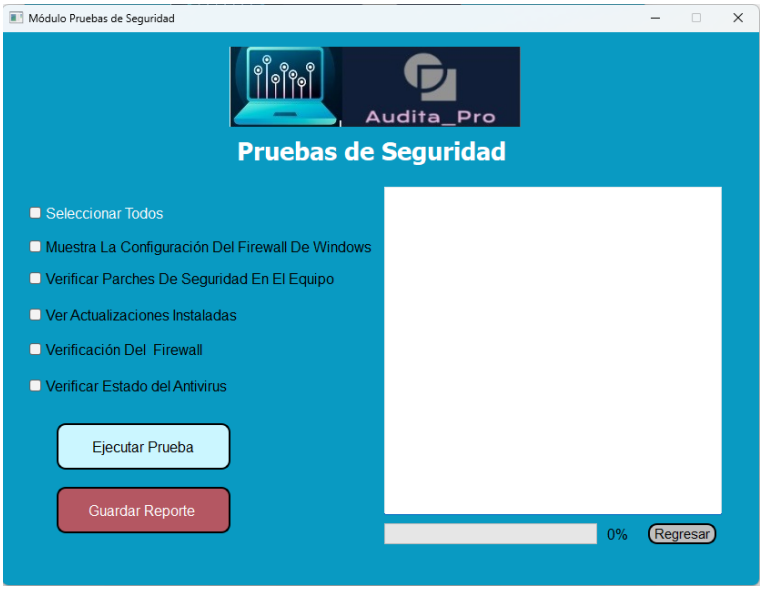


Fig. 8 Pruebas de seguridad

3. Descripción Pruebas de Red

- **Estado Del Tráfico De** Red

Evaluar el estado actual del tráfico de red, el fin de verificar patrones de tráfico sospechoso, el tráfico de red puede ser útil para identificar problemas de congestión o actividad no autorizada en red.

- **Lista De Las Conexiones De Red Activas**
  Se enumeran las conexiones de red activas en el sistema para identificar quién está accediendo a la red.

- **Mostrar Información De Red**
  Obtiene información detallada sobre la configuración y el estado de la red, como dirección IP entre otros, lo que es importante para la configuración y la solución de problemas de red.
- **Verificar Restricciones En El Host**

  Verifica si existen restricciones de acceso en el host que puedan afectar la conectividad o la seguridad de la red.

- **Verificar Conectividad a Internet**
  Verifica una conexión a un sitio web conocido y verificar si la conexión se establece correctamente

Estas pruebas se centran en la seguridad y el monitoreo de la red, así como la evaluación del estado del software antivirus en el sistema, estas pruebas ayudarán a garantizar que la red y las conexiones estén protegida, y que el sistema esté bien defendido contra amenazas de seguridad

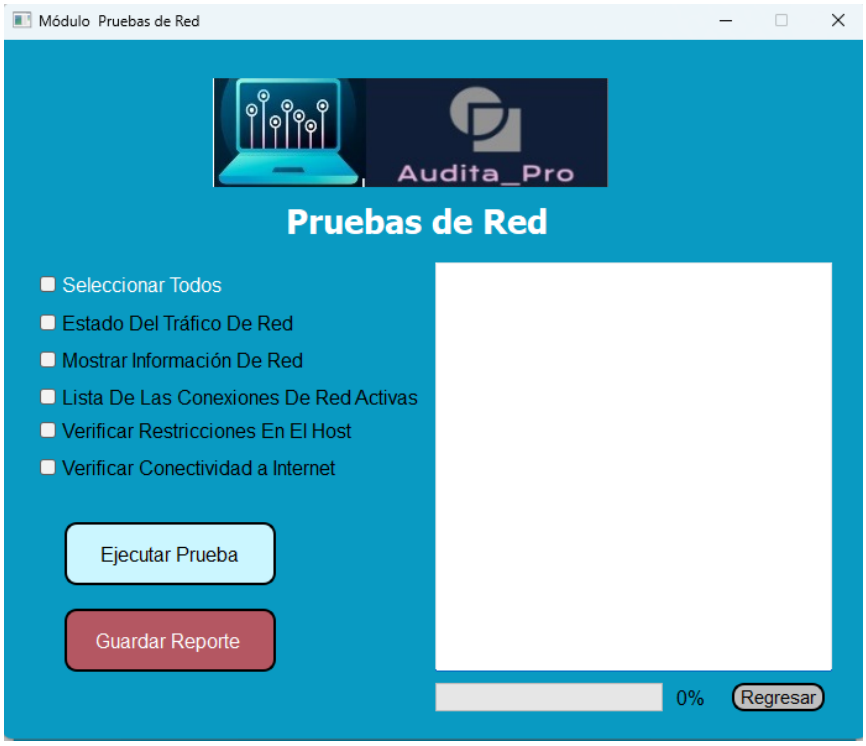


Fig. 9 Pruebas de Red

4. Descripción del Módulo Reportes

En este módulo se almacena los reportes que el software realice con fin de llevar un control conforme se haga las pruebas en diferentes fechas.

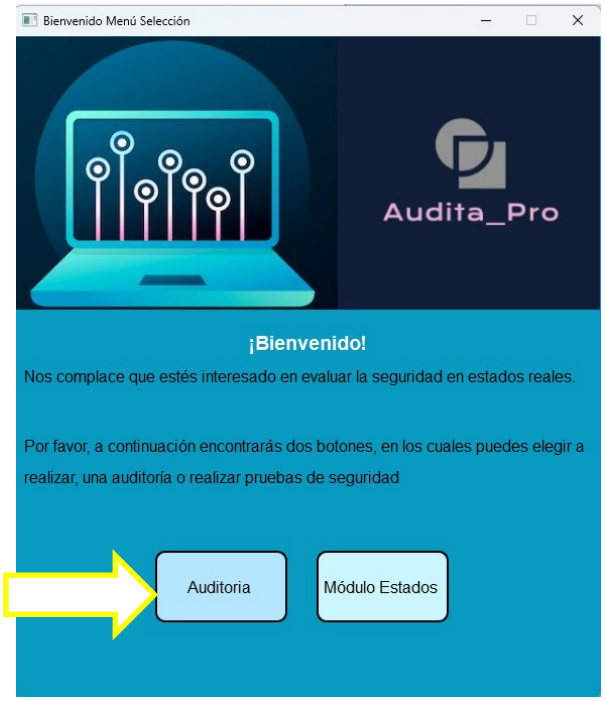
Prueba	Resultado	
Resultado de	Prueba 1	{'Puerto 80': 'Closed'}
	Prueba 1	{'Puerto 80': 'Closed', 'Puerto 8000': 'Open'}
	Prueba 2	{'Puerto 80': 'Closed', 'Puerto 8000': 'Open'}
	Prueba 1	{'prueba_id': '1', 'Puerto 80': 'Closed', 'Puerto 8000': 'Open'}
	Prueba 2	{'prueba_id': '2', 'Puerto 80': 'Closed', 'Puerto 8000': 'Open'}
	Prueba 3	{'prueba_id': '3', 'Puerto 80': 'Closed', 'Puerto 8000': 'Open'}
	Prueba 4	{'prueba_id': '4', 'Puerto 80': 'Closed', 'Puerto 8000': 'Open'}

Fig.10 Módulo Reportes

5. Prueba piloto

En este espacio es para el desarrollo de las pruebas en un computador para validar el correspondiente funcionamiento del software se utilizara un Hash de verificación con el

propósito de que el software no sea modificado al momento de realizar la descarga del producto y poder realizar las pruebas.

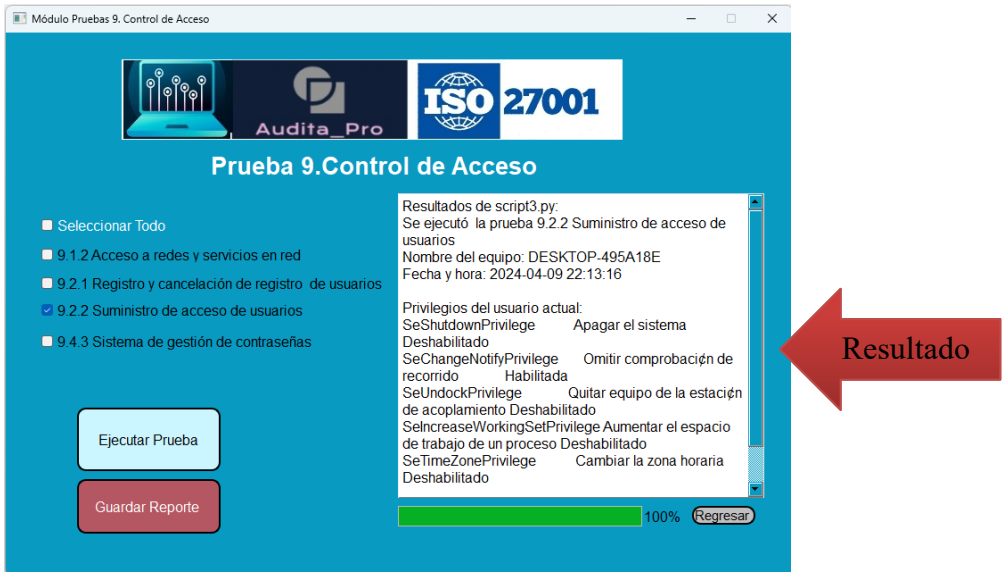


Se selecciona la opción en el botón Auditoría y seleccionamos la opción A9 Control de acceso

A 9.Control De Acceso.

9.1.2 Acceso a redes y servicios en red.

- **9.2.1 Registro y cancelación de registro de usuarios**

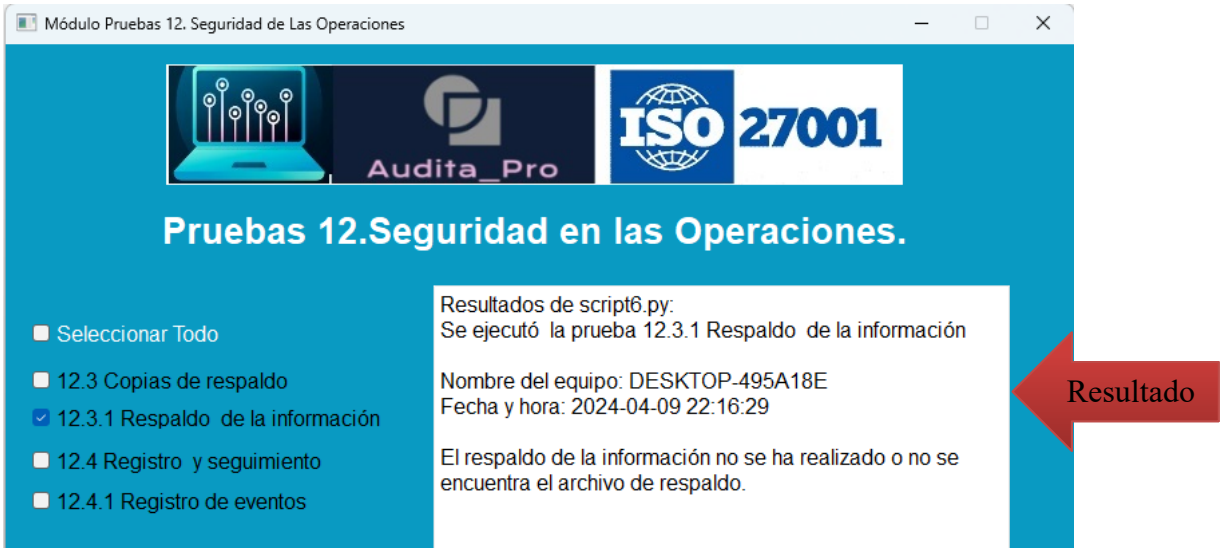


- **9.2.2 Suministro de acceso de usuarios**

- **9.4.3 Sistema de gestión de contraseñas**

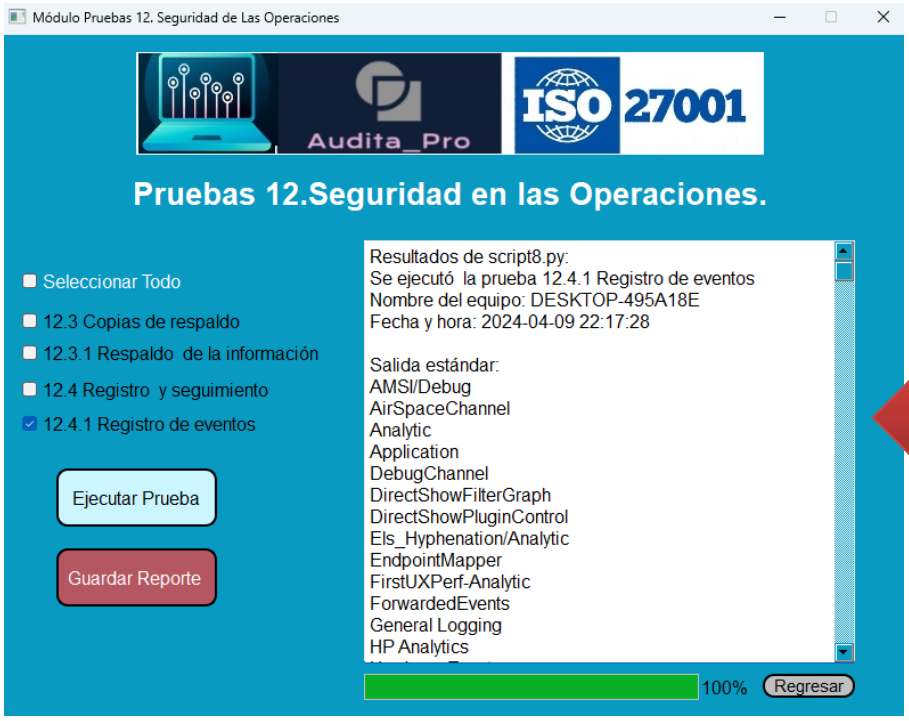
- **A 12. SEGURIDAD EN LAS OPERACIONES.**

- **12.3 Copias de respaldo**



- **12.3.1 Respaldo de la información**

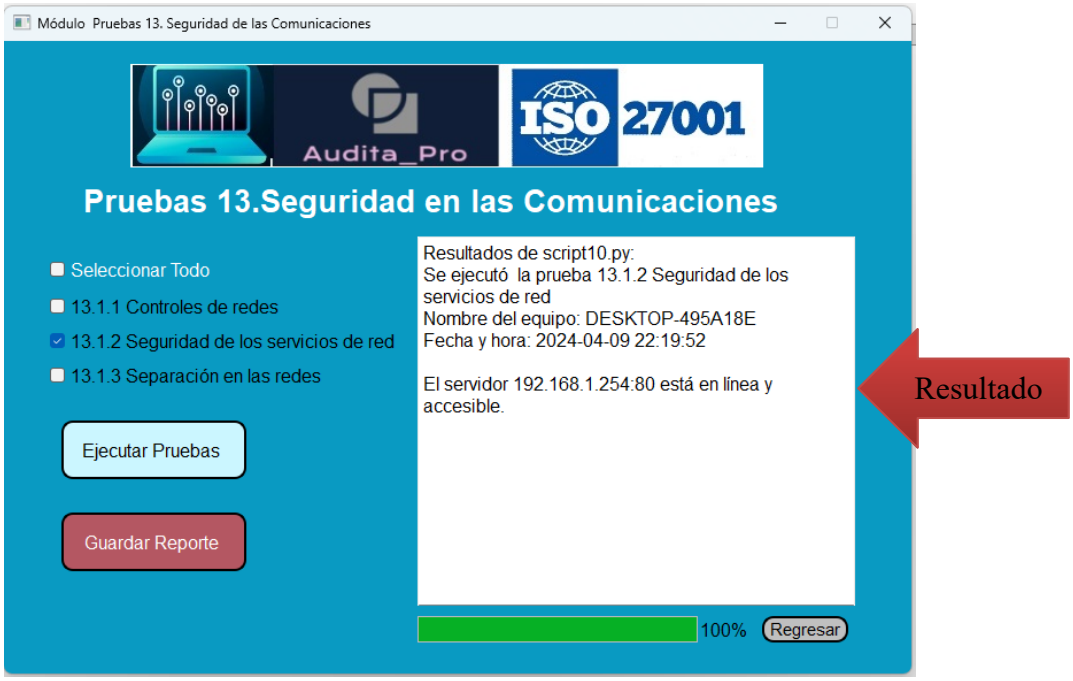
- **12.4 Registro y seguimiento**



- **12.4.1 Registro de eventos**

- **A 13 SEGURIDAD DE LAS COMUNICACIONES**

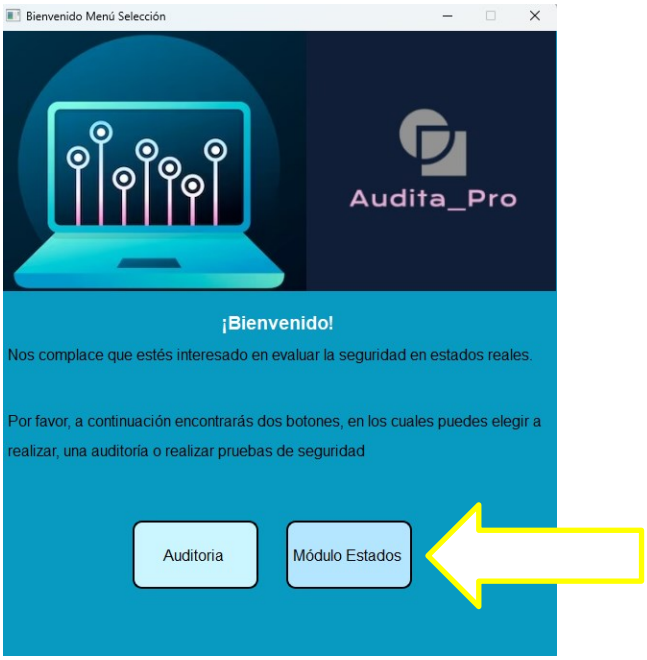
- **13.1.1 Controles de redes**



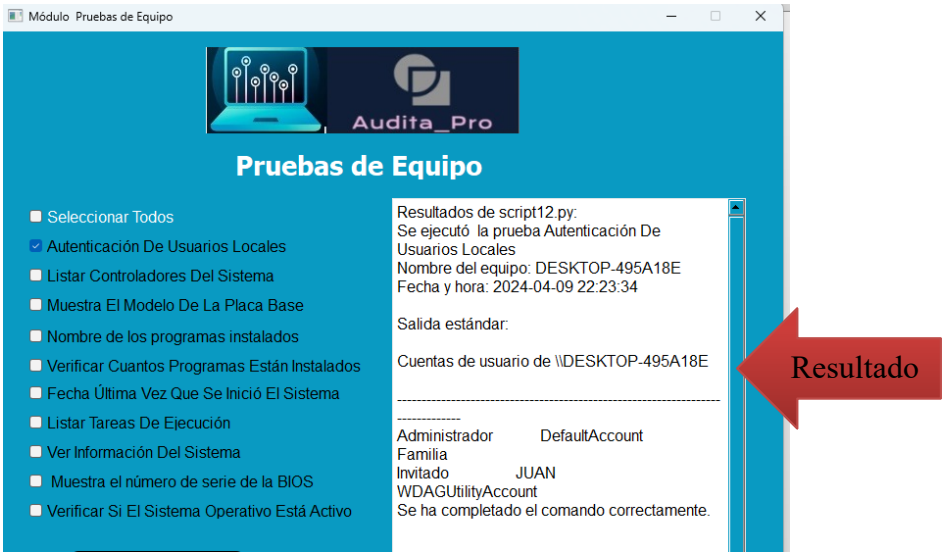
- **13.1.2 Seguridad de los servicios de red**

- **13.1.3 Separación en las redes**

Se selecciona la opción en el botón Ventana Módulo Estados

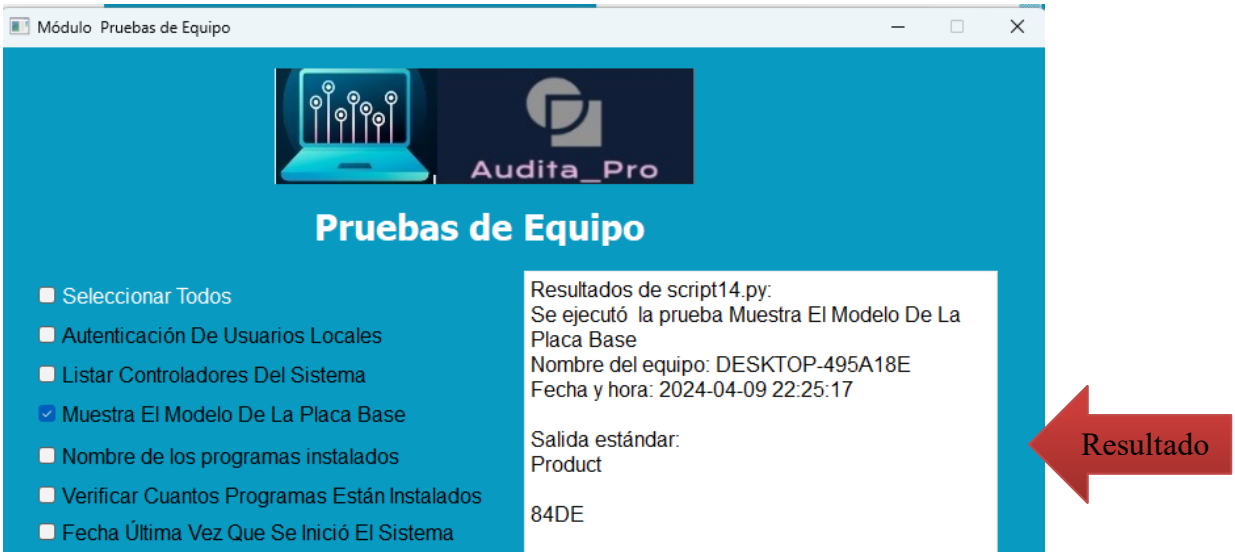


Se selecciona la opción Pruebas en equipos y tenemos los siguientes resultados



- **Autenticación De Usuarios Locales**

- **Listar Controladores Del Sistema**

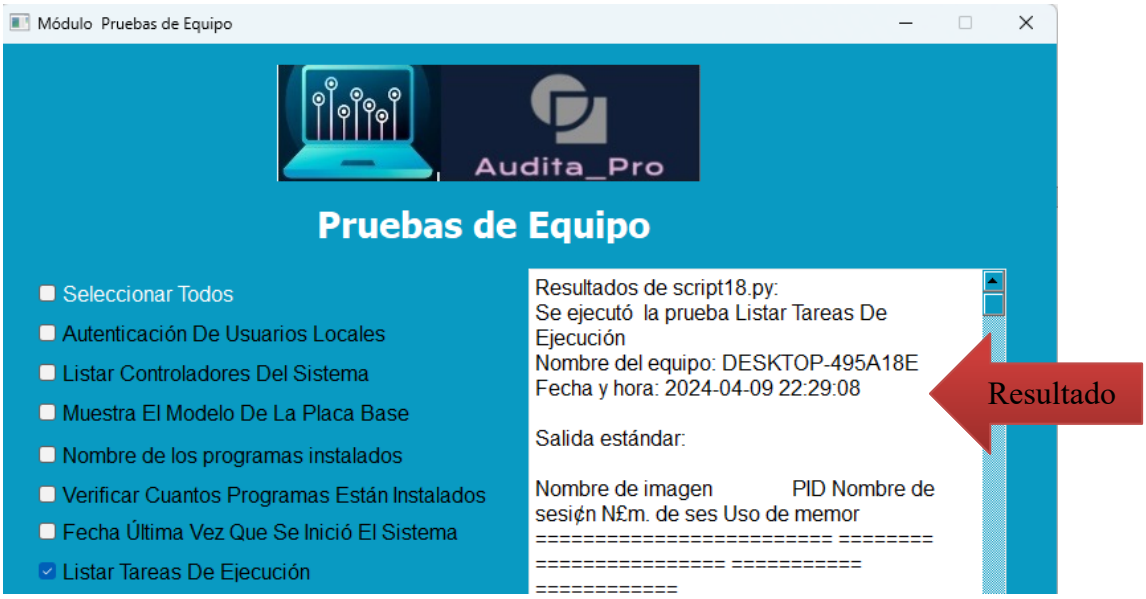


- **Muestra El Modelo De La Placa Base**

- **Nombre de los programas instalados**

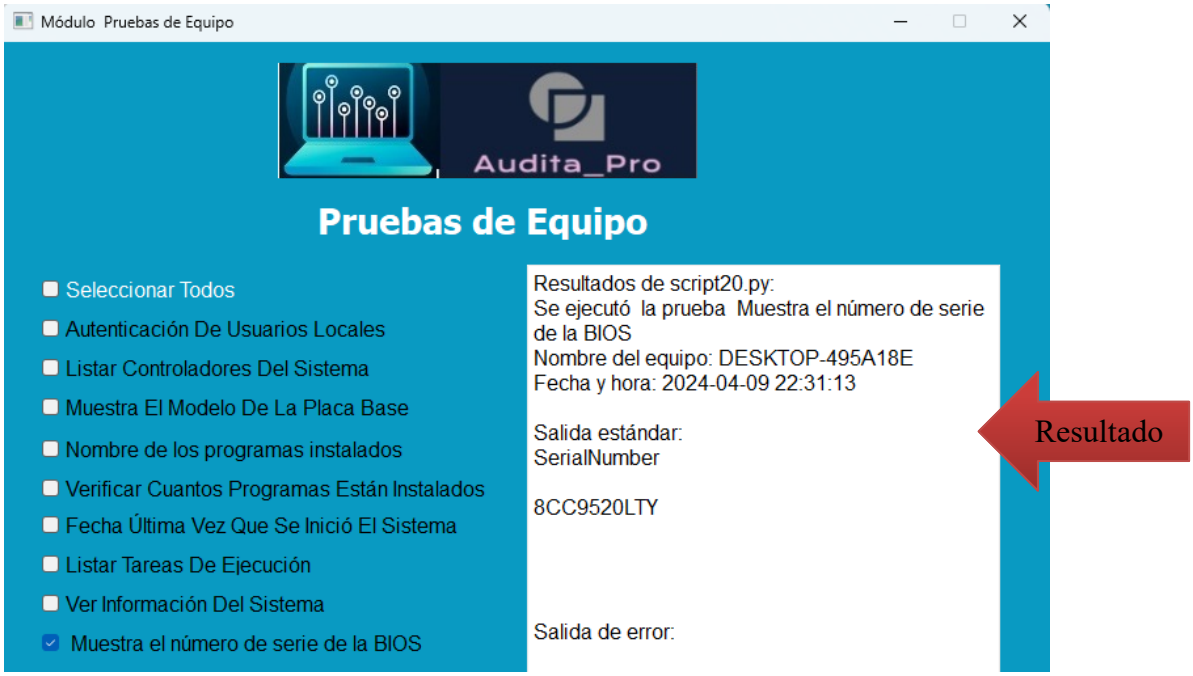
- **Verificar Cuántos Programas Están Instalados**

- **Fecha Última Vez Que Se Inició El Sistema**



- **Listar Tareas De Ejecución**

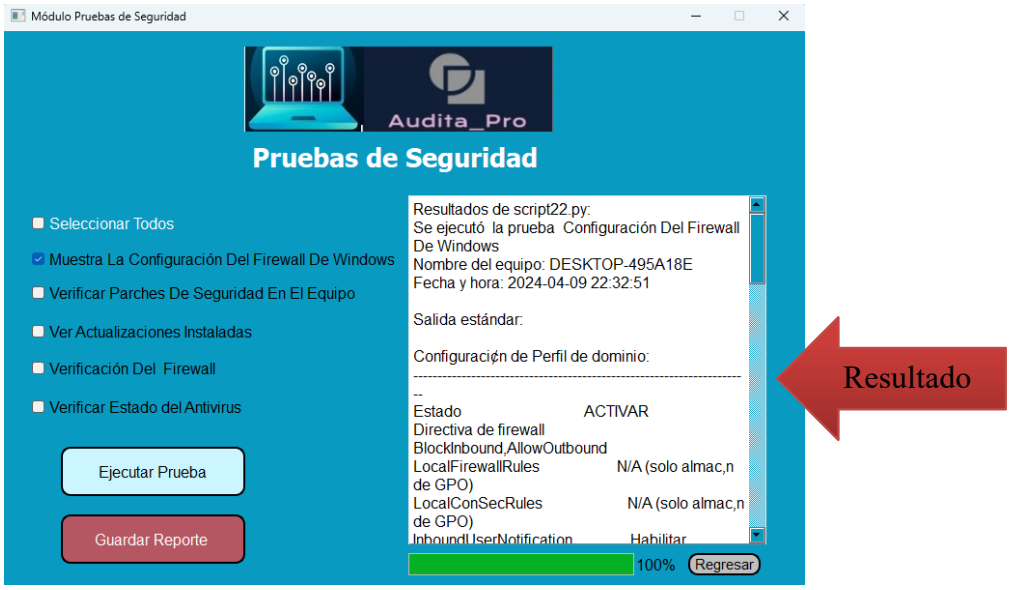
- **Ver Información Del Sistema**



- **Muestra el número de serie de la BIOS**

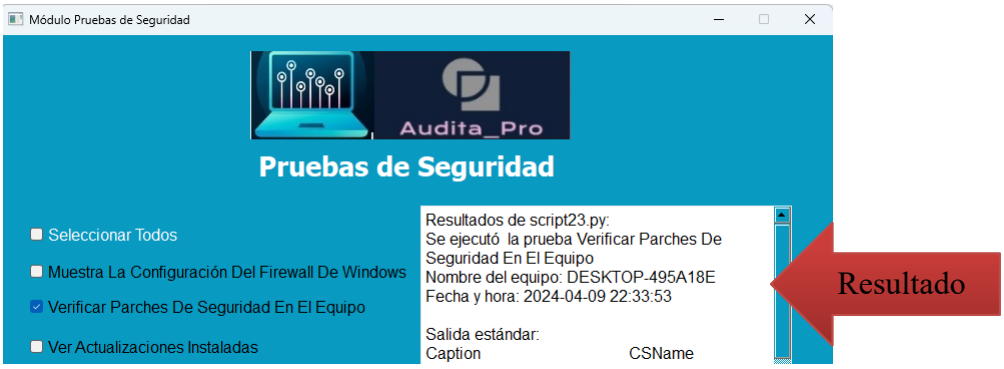
- **Verificar Si El Sistema Operativo Está Activo**

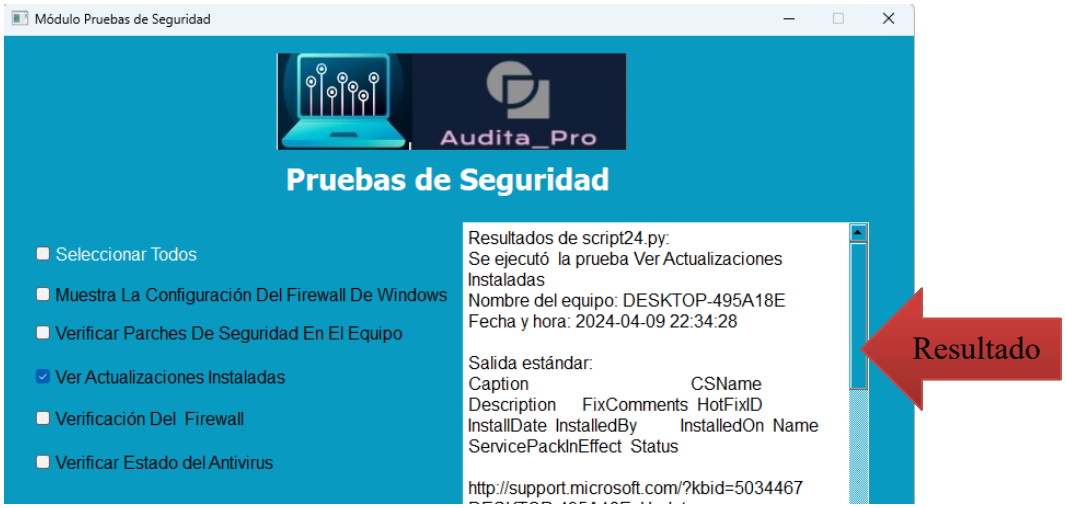
2. Pruebas de Seguridad



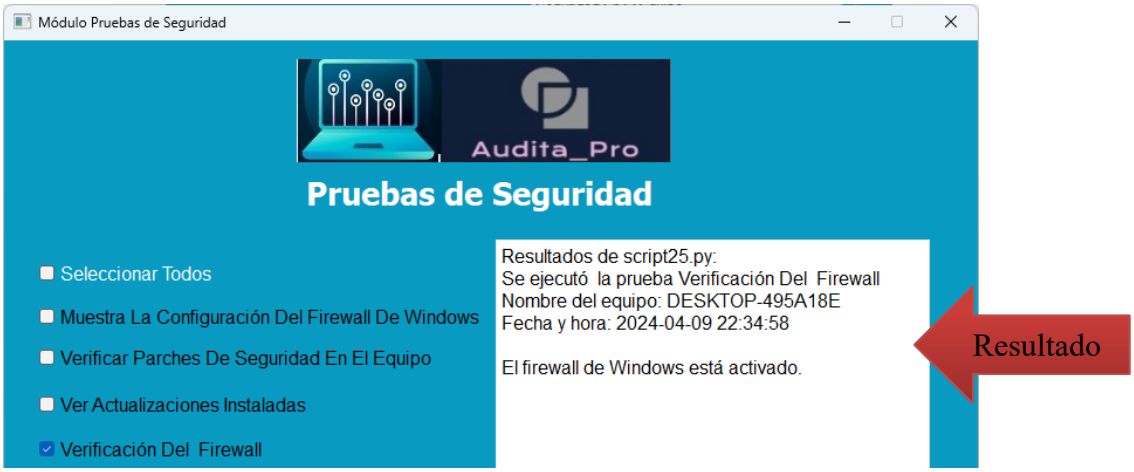
- **Muestra La Configuración Del Firewall De Windows**

- **Verificar Parches De Seguridad En El Equipo**

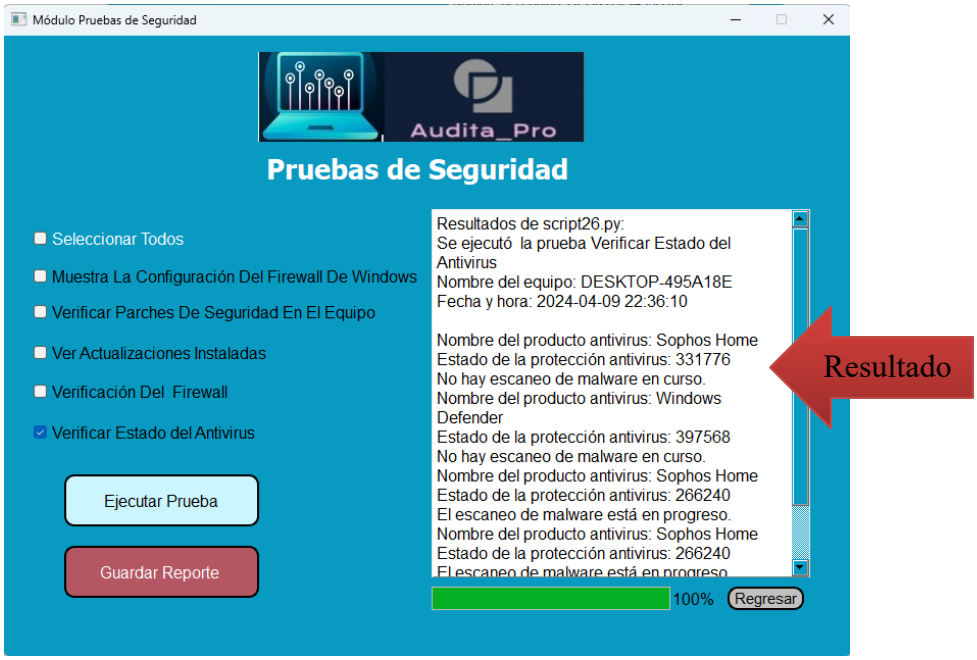




- **Ver Actualizaciones Instaladas**



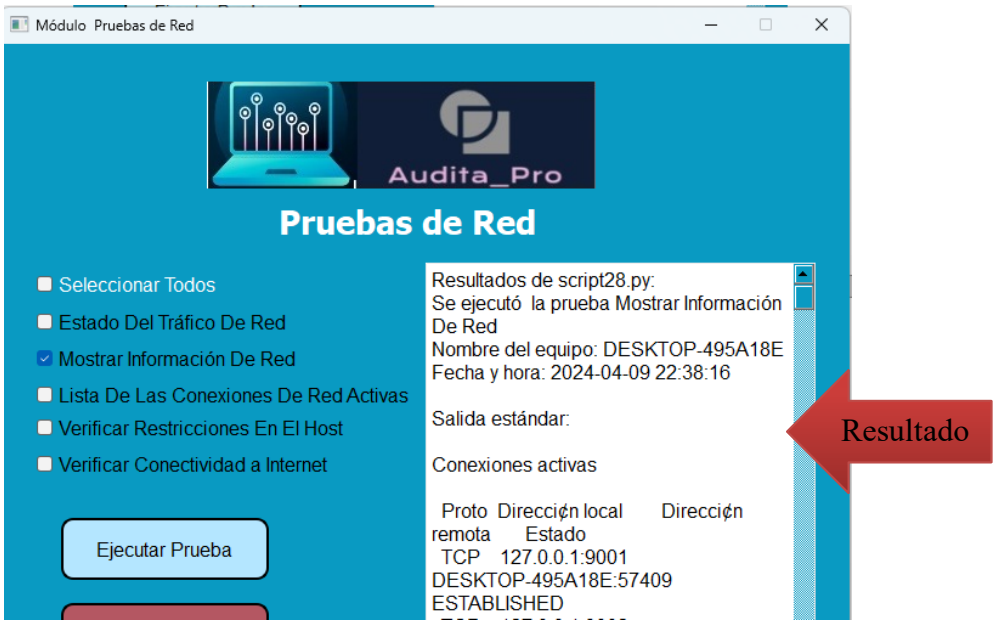
- **Verificación Del Firewall**



- **Verificar Estado del Antivirus**

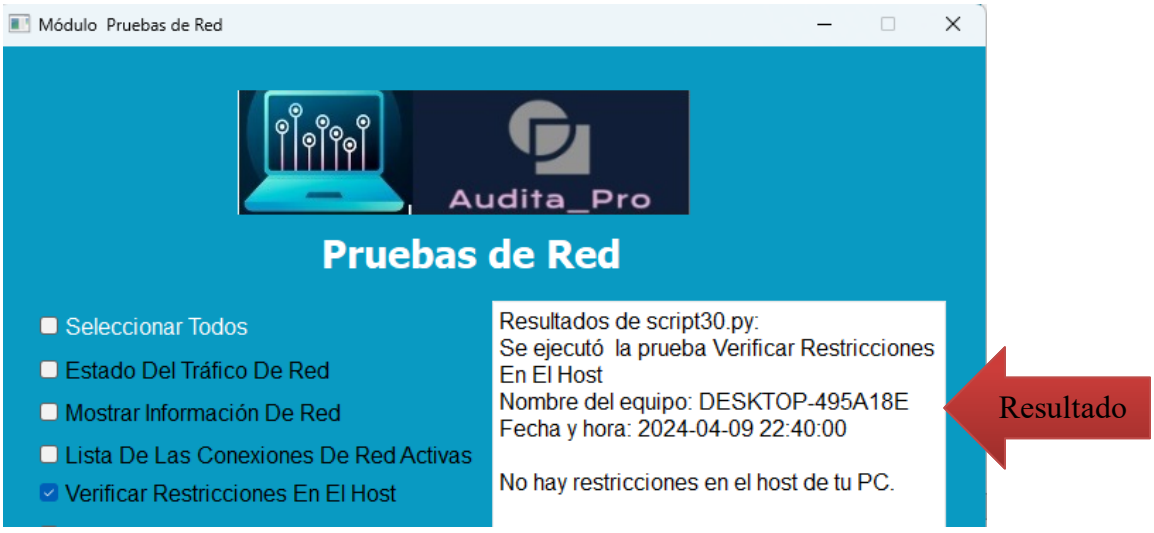
3. Pruebas de Red

- **Estado Del Tráfico De Red**



- **Mostrar Información De Red**

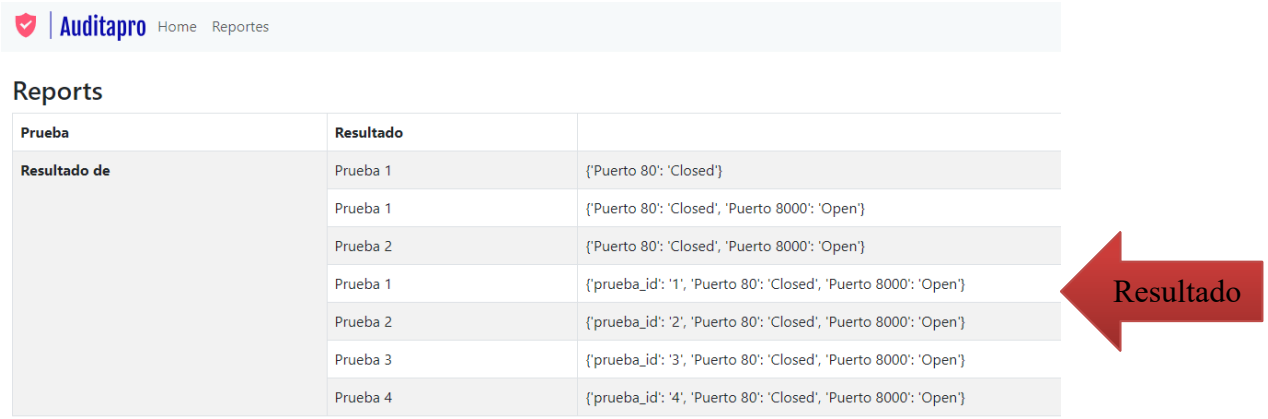
- **Lista De Las Conexiones De Red Activas**



- **Verificar Restricciones En El Host**

- **Verificar Conectividad a Internet**

4. Módulo Reportes



- **Módulo Reportes**

Anexo 4 Formato acta 022 de Pasto Salud Socialización del software

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	ACTA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-A	022

Diligenciar en medio digital o a mano alzada Válida con firmas

FECHA	DIA	MES	AÑO	HORA INCIO	HORA FINAL	ACTA No.
	01	04	2024	8:00 AM	12:00 PM	1

TEMA DE REUNION:	Socialización del software AuditaPro y solicitud para realizar pruebas
LUGAR:	Oficina de comunicaciones y sistemas Sede administrativa Pasto Salud E.S.E

ASISTENTES

NOMBRES Y APELLIDOS	CARGO	DEPENDENCIA	FIRMA
LIDA PABÓN LÓPEZ	Jefe Oficina Asesora de comunicaciones y sistemas	Oficina Asesora de comunicaciones y Sistemas	
Juan David Argoti Puchana	Estudiante de Ingeniería de sistemas	Universidad Cesmag	

Cuando se trate de un grupo de asistentes superior a cinco personas, es válido adjuntar firmas de asistentes a la reunión en Registros de Asistencia, que forman parte integral del acta

ORDEN DEL DIA

1. Verificación de la documentación
2. Socialización del software AuditaPro
3. Prueba piloto
4 solicitud de hacer pruebas en diferentes equipos
5. Conclusiones

DESARROLLO

Se da el inicio con el numeral 1

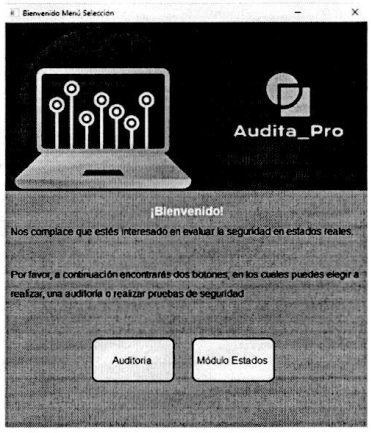
1. Verificación de la documentación

En este punto el estudiante indica la documentación pertinente con respecto al desarrollo de trabajo de grado titulado

Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real

2. Socialización del software AuditaPro

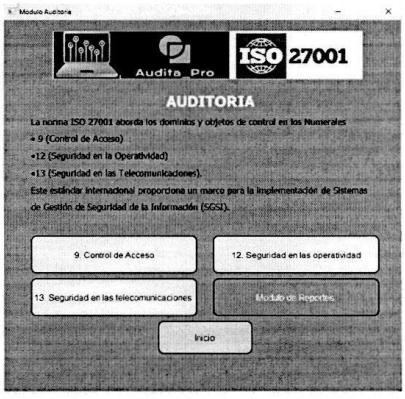
Se indica el diseño del software AuditaPro



Interfaz Menú selección

Una vez dado clic en el botón auditorio se despliega la otra ventana con la opción de cuatro botones:

Botón1. / 9. Controles de acceso
Botón 2. / 12. Seguridad de las operaciones,
Botón 3. /13. Seguridad de las Telecomunicaciones
Botón 4 / Módulo de reportes



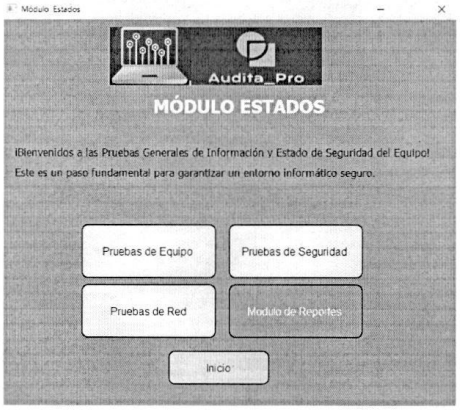
Interfaz Modulo de auditoria

Para regresar al menú se da clic en el botón inicio que nos devuelve a la anterior interfaz donde se

encontrara en la ventana módulo estados

Ventana Módulo Estados

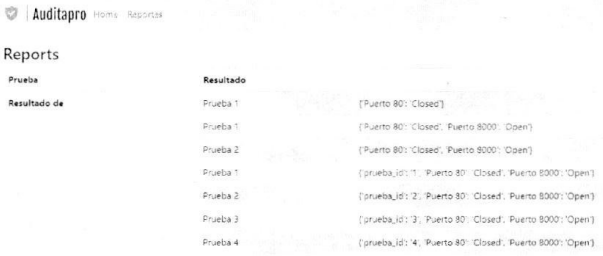
Se despliega la ventana llamada pruebas de estados les que se encuentran separadas en tres categorías pruebas de equipo, pruebas de seguridad y pruebas de red.



Interfaz Módulo Estados

Para ir al menú de reportes se puede dar clic en el botón modulo reportes que lo dirigirá a la venta reportes

Ventana módulo reportes



Interfaz módulo reportes

3. Prueba piloto se solicita hacer una prueba piloto para ver el funcionamiento del software y se diligencia la lista de chequeo

4. Solicitud de hacer pruebas en diferentes equipos

la ingeniera me da el visto bueno de hacer las pruebas con el compromiso de que los reportes que se encuentren sean de reserva por la confidencialidad de la información

5. Conclusiones

El desarrollo del software de validación de estados de seguridad ha mostrado ser una herramienta crucial

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	ACTA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-A	022

en entornos reales. Se recomienda continuar con su desarrollo y adopción, teniendo en cuenta las áreas de mejora identificadas y las necesidades cambiantes del entorno de seguridad cibernética.

Desarrollo e Implementación: Siguiendo una metodología rigurosa que incluye el análisis de requisitos, diseño, implementación y evaluación, el software se diseñó para simular condiciones de operación reales y evaluar la seguridad de los equipos frente a posibles amenazas.

Se realizaron pruebas en diferentes configuraciones de sistema para garantizar la efectividad del software bajo diversos escenarios de uso.

Resultados

El uso del software contribuyó significativamente a la gestión de la seguridad, disminuyendo los posibles riesgos y amenazas cibernéticas para las pequeñas y medianas empresas se observó un incremento en la concienciación sobre prácticas de seguridad entre los usuarios, fortaleciendo la cultura de seguridad

Recomendaciones

Para la mejora Continua en el desarrollo enfocado en vulnerabilidades, priorizar características para una detección y corrección proactiva de vulnerabilidades. Asegurar la conformidad continua del software con normativas de seguridad internacionales. Para mejorar el enfoque de las pruebas

Educación Continua: Ofrecer formación y recursos educativos para maximizar la eficacia del software y el entendimiento de los usuarios.

COMPROMISOS
El estudiante se compromete hacer las pruebas en diferentes equipos de la sede administrativa, garantizando que la información que se obtenga no salga de la entidad

PROXIMA CONVOCATORIA					
LUGAR	HORA	FECHA	DIA	MES	AÑO

ANEXOS AL ACTA	1 lista de chequeo
RESPONSABLE DEL ACTA	

Anexo 5 lista de chequeo de pruebas

Reporte de Pruebas Funcionales Conforme a la guía Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)	

Título de la prueba	Prioridad	Numero de la prueba	Fecha de la prueba
Verificación de los módulos de auditoria y estados	Alta	Del nuero 1 a la 31	Día/Mes/año 01-04-2024
Descripción de la prueba	**Prueba diseñada por**	**Prueba ejecutada por**	**Fecha de ejecución**
Software AuditaPro	Estudiante: Juan David Argoti Pucha	Estudiante: Juan David Argoti Pucha	Día/Mes/año 01-04-2024

Descripción de la prueba

El software AuditaPro está diseñado para validar la seguridad de equipos mediante la ejecución de pruebas en condiciones reales, garantizando así su adecuando funcionamiento

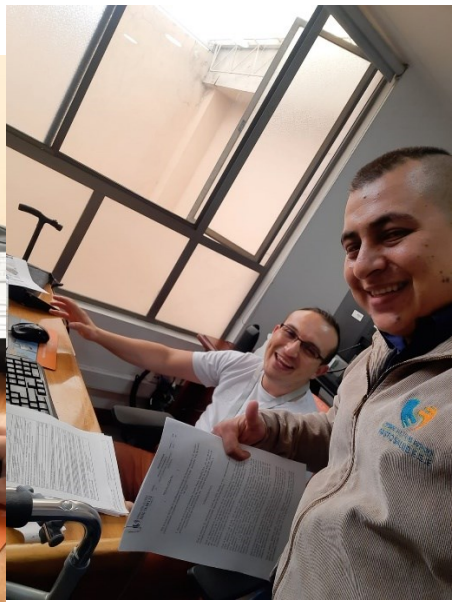
No Scripts	Descripción	Modulo Perteneciente	Cumple su función	Observación
1	9.1.2 Acceso a redes y servicios en red	Prueba 9.Control de Acceso	SI ☑ NO ☐	
2	9.2.1 Registro y cancelación de registro de usuarios		SI ☑ NO ☐	
3	9.2.2 Suministro de acceso de usuarios		SI ☑ NO ☐	
4	9.4.3 Sistema de gestión de contraseñas		SI ☑ NO ☐	
5	12.3 Copias de respaldo	Pruebas 12.Seguridad en las Operaciones.	SI ☑ NO ☐	
6	12.3.1 Respaldo de la información		SI ☑ NO ☐	
7	12.4 Registro y seguimiento		SI ☑ NO ☐	
8	12.4.1 Registro de eventos		SI ☑ NO ☐	
9	13.1.1 Controles de redes	Pruebas 13.Seguridad en las Comunicaciones	SI ☐ NO ☑	
10	13.1.2 Seguridad de los servicios de red		SI ☑ NO ☐	
11	13.1.3 Separación en las redes		SI ☑ NO ☐	
12	Autenticación De Usuarios Locales	Pruebas de equipo	SI ☐ NO ☑	
13	Listar Controladores Del Sistema		SI ☐ NO ☑	
14	Muestra El Modelo De La Placa Base		SI ☑ NO ☐	
15	Nombre de los programas instalados		SI ☑ NO ☐	
16	Verificar Cuantos Programas Están Instalados		SI ☑ NO ☐	

17	Fecha Última Vez Que Se Inició El Sistema		SI ☐ NO ☑	
18	Listar Tareas De Ejecución		SI ☐ NO ☑	
19	Ver Información Del Sistema		SI ☑ NO ☐	
20	Muestra el número de serie de la BIOS		SI ☑ NO ☐	
21	Verificar Si El Sistema Operativo Está Activo		SI ☑ NO ☐	
22	Muestra La Configuración Del Firewall De Windows	Pruebas de seguridad	SI ☑ NO ☐	
23	Verificar Parches De Seguridad En El Equipo		SI ☑ NO ☐	
24	Ver Actualizaciones Instaladas		SI ☐ NO ☑	
25	Verificación Del Firewall		SI ☑ NO ☐	
26	Verificar Estado del Antivirus		SI ☑ NO ☐	
27	Estado Del Tráfico De Red	Pruebas de red	SI ☐ NO ☑	
28	Mostrar Información De Red		SI ☐ NO ☑	
29	Lista De Las Conexiones De Red Activas		SI ☑ NO ☐	
30	Verificar Restricciones En El Host		SI ☑ NO ☐	
31	Verificar Conectividad a Internet		SI ☑ NO ☐	

Oscar David Argote Pachon
Firma Estudiante

Firma con quien se hizo la prueba

Anexo 6 Registros fotográficos



UNIVERSIDAD CESMAG NIT: 800.109.387-7 VIGILADA MINEDUCACIÓN	**CARTA DE ENTREGA TRABAJO DE GRADO O TRABAJO DE APLICACIÓN – ASESOR(A)**	**CÓDIGO:** AAC-BL-FR-032
		VERSIÓN: 1
		FECHA: 09/JUN/2022

San Juan de Pasto, 18 de junio de 2024

Biblioteca
REMIGIO FIORE FORTEZZA OFM. CAP.
Universidad CESMAG
Pasto

Saludo de paz y bien.

Por medio de la presente se hace entrega del Trabajo de Grado / Trabajo de Aplicación denominado Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real, presentado por el autor Juan David Argoti Puchana del Programa Académico Ingeniería de sistemas al correo electrónico biblioteca.trabajosdegrado@unicesmag.edu.co. Manifiesto como asesor, que su contenido, resumen, anexos y formato PDF cumple con las especificaciones de calidad, guía de presentación de Trabajos de Grado o de Aplicación, establecidos por la Universidad CESMAG, por lo tanto, se solicita el paz y salvo respectivo.

Atentamente,

(Firma del Asesor)

LUIS ARNOBY ESCOBAR HERNÁNDEZ
C.C. 98.388.299
Facultad Ingeniería de Sistemas
315 4671444
laescobar@unicesmag.edu.co

INFORMACIÓN DEL (LOS) AUTOR(ES)	
Nombres y apellidos del autor: JUAN DAVID ARGOTI PUCHANA	**Documento de identidad:** 1085.304.462
Correo electrónico: Juanargoti2015@hotmail.com	**Número de contacto:** 1085304462
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del asesor: Luis Arnoby Escobar Hernández	**Documento de identidad:** 98.388.299
Correo electrónico: laescobar@unicesmag.edu.co	**Número de contacto:** 315 4671444
Título del trabajo de grado: Desarrollo de un software de validación de estados de seguridad en los equipos mediante pruebas en entorno real	
Facultad y Programa Académico: Ingeniería de Sistemas	

En mi (nuestra) calidad de autor(es) y/o titular (es) del derecho de autor del Trabajo de Grado o de Aplicación señalado en el encabezado, confiero (conferimos) a la Universidad CESMAG una licencia no exclusiva, limitada y gratuita, para la inclusión del trabajo de grado en el repositorio institucional. Por consiguiente, el alcance de la licencia que se otorga a través del presente documento, abarca las siguientes características:

a) La autorización se otorga desde la fecha de suscripción del presente documento y durante todo el término en el que el (los) firmante(s) del presente documento conserve (mos) la titularidad de los derechos patrimoniales de autor. En el evento en el que deje (mos) de tener la titularidad de los derechos patrimoniales sobre el Trabajo de Grado o de Aplicación, me (nos) comprometo (comprometemos) a informar de manera inmediata sobre dicha situación a la Universidad CESMAG. Por consiguiente, hasta que no exista comunicación escrita de mi(nuestra) parte informando sobre dicha situación, la Universidad CESMAG se encontrará debidamente habilitada para continuar con la publicación del Trabajo de Grado o de Aplicación dentro del repositorio institucional. Conozco(conocemos) que esta autorización podrá revocarse en cualquier momento, siempre y cuando se eleve la solicitud por escrito para dicho fin ante la Universidad CESMAG. En estos eventos, la Universidad CESMAG cuenta con el plazo de un mes después de recibida la

petición, para desmarcar la visualización del Trabajo de Grado o de Aplicación del repositorio institucional.

b) Se autoriza a la Universidad CESMAG para publicar el Trabajo de Grado o de Aplicación en formato digital y teniendo en cuenta que uno de los medios de publicación del repositorio institucional es el internet, acepto(amos) que el Trabajo de Grado o de Aplicación circulará con un alcance mundial.
c) Acepto (aceptamos) que la autorización que se otorga a través del presente documento se realiza a título gratuito, por lo tanto, renuncio(amos) a recibir emolumento alguno por la publicación, distribución, comunicación pública y/o cualquier otro uso que se haga en los términos de la presente autorización y de la licencia o programa a través del cual sea publicado el Trabajo de grado o de Aplicación.
d) Manifiesto (manifestamos) que el Trabajo de Grado o de Aplicación es original realizado sin violar o usurpar derechos de autor de terceros y que ostento(amos) los derechos patrimoniales de autor sobre la misma. Por consiguiente, asumo(asumimos) toda la responsabilidad sobre su contenido ante la Universidad CESMAG y frente a terceros, manteniéndose indemne de cualquier reclamación que surja en virtud de la misma. En todo caso, la Universidad CESMAG se compromete a indicar siempre la autoría del escrito incluyendo nombre de(los) autor(es) y la fecha de publicación.
e) Autorizo(autorizamos) a la Universidad CESMAG para incluir el Trabajo de Grado o de Aplicación en los índices y buscadores que se estimen necesarios para promover su difusión. Así mismo autorizo (autorizamos) a la Universidad CESMAG para que pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

NOTA: En los eventos en los que el trabajo de grado o de aplicación haya sido trabajado con el apoyo o patrocinio de una agencia, organización o cualquier otra entidad diferente a la Universidad CESMAG. Como autor(es) garantizo(amos) que he(hemos) cumplido con los derechos y obligaciones asumidos con dicha entidad y como consecuencia de ello dejo(dejamos) constancia que la autorización que se concede a través del presente escrito no interfiere ni transgrede derechos de terceros.

Como consecuencia de lo anterior, autorizo(autorizamos) la publicación, difusión, consulta y uso del Trabajo de Grado o de Aplicación por parte de la Universidad CESMAG y sus usuarios así:

- Permito(permitimos) que mi(nuestro) Trabajo de Grado o de Aplicación haga parte del catálogo de colección del repositorio digital de la Universidad CESMAG por lo tanto, su contenido será de acceso abierto donde podrá ser consultado, descargado y compartido con otras personas, siempre que se reconozca su autoría o reconocimiento con fines no comerciales.

En señal de conformidad, se suscribe este documento en San Juan de Pasto a los 18 días del mes de Junio del año 2024

Juan David Argoti Puchana Firma del autor:	Firma del autor
Nombre del autor: Juan David Argoti Puchana	Nombre del autor:
Firma del autor	Firma del autor
Nombre del autor:	Nombre del autor:

Nombre del asesor: Luis Arnoby Escobar H.