

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

CIS CRITICAL SECURITY CONTROLS (CIS CONTROLS) PARA LA MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD EN LA INFRAESTRUCTURA DE RED DE LA UNIDAD EDUCATIVA GENERAL ELOY ALFARO DE LA CIUDAD DE SALCEDO

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información

ÁREA: Seguridad y Redes

LÍNEA DE INVESTIGACIÓN: Software, Tecnologías de la Información y Ciencias de Datos

AUTOR: Carlos David Quispe Silva

TUTOR: Ing. David Omar Guevara Aulestia, Mg.

Ambato - Ecuador

enero - 2026

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: CIS CRITICAL SECURITY CONTROLS (CIS CONTROLS) PARA LA MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD EN LA INFRAESTRUCTURA DE RED DE LA UNIDAD EDUCATIVA GENERAL ELOY ALFARO DE LA CIUDAD DE SALCEDO, desarrollado bajo la modalidad Proyecto de Investigación por el señor Carlos David Quispe Silva estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, enero 2026.

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA
Validar únicamente con FirmaEC

Ing. David Omar Guevara Aulestia, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: CIS CRITICAL SECURITY CONTROLS (CIS CONTROLS) PARA LA MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD EN LA INFRAESTRUCTURA DE RED DE LA UNIDAD EDUCATIVA GENERAL ELOY ALFARO DE LA CIUDAD DE SALCEDO es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, enero 2026.

Firmado electrónicamente por:
CARLOS DAVID QUISPE SILVA
Validar únicamente con FirmaEC

Carlos David Quispe Silva

C.C. 1850130152

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, enero 2026.



Carlos David Quispe Silva

C.C. 1850130152

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Carlos David Quispe Silva, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado CIS CRITICAL SECURITY CONTROLS (CIS CONTROLS) PARA LA MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD EN LA INFRAESTRUCTURA DE RED DE LA UNIDAD EDUCATIVA GENERAL ELOY ALFARO DE LA CIUDAD DE SALCEDO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor presidente del tribunal.

Ambato, enero 2026.

Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA
Validar únicamente con FirmaEC

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
DANIEL ALEJANDRO MALDONADO RUIZ
Validar únicamente con FirmaEC

Ing. Daniel Maldonado Ruiz, PhD.
PROFESOR CALIFICADOR

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA
Validar únicamente con FirmaEC

Ing. Vicente Morales Lozada, PhD.
PROFESOR CALIFICADOR

DEDICATORIA

Dedico este logro a mi familia, amigos y a todas las personas que día a día estuvieron apoyándome en esta etapa de mi vida.

AGRADECIMIENTO

Agradezco a mi familia y amigos, por el apoyo y comprensión constante a lo largo de este trayecto.

A mi tutor el ing. David Guevara por su invaluable guía y compromiso para que este proyecto sea realizado con éxito.

A las autoridades de la Unidad Educativa General Eloy Alfaro, por la confianza depositada y la apertura brindada en la elaboración de este proyecto.

Finalmente, extiendo mi gratitud a la Universidad Técnica de Ambato por haberme brindado la oportunidad de formarme como profesional. Un reconocimiento a los docentes de la carrera, por su invaluable dedicación y por ser fuente constante de apoyo e inspiración a lo largo de toda mi trayectoria académica.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... **iv**

APROBACIÓN DEL TRIBUNAL DE GRADO ..... **v**

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE GENERAL DE CONTENIDOS ..... **viii**

ÍNDICE DE TABLAS ..... **xi**

ÍNDICE DE FIGURAS ..... **xii**

ÍNDICE DE ANEXOS ..... **xv**

RESUMEN EJECUTIVO ..... **xvi**

ABSTRACT ..... **xvii**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 2

1.3 Fundamentación teórica 6

1.3.1 Tecnologías de la Información (TI) 6

1.3.2 Seguridad Informática 6

1.3.3 Marco de Seguridad 6

1.3.4 CIS Critical Security Controls (CIS Controls) 7

1.3.5 Unidad educativa 9

1.3.6 Infraestructura tecnológica 9

1.3.7 Componentes de red 9

1.3.8 Vulnerabilidad 10

1.4 Objetivos 10

1.4.1 Objetivo general 10

1.4.2 Objetivos específicos 10

CAPÍTULO II. METODOLOGÍA 12

2.1 Materiales 12

2.1.1 Encuesta dirigida a docentes 12

2.1.2 Encuesta dirigida a estudiantes 12

2.1.3 Entrevista al docente encargado del área de TI de la Unidad Educativa 12

2.1.4 Ficha de observación 13

2.2 Métodos 14

2.2.1 Modalidad de la investigación 14

2.2.2 Población y muestra 15

2.2.3 Recolección de información 16

2.2.4 Procesamiento y análisis de datos 32

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 34

3.1 Análisis y discusión de resultados 34

3.2 Aplicación del marco de ciberseguridad de los CIS Controls 34

3.2.1 Fase 1: Evaluación el estado de seguridad actual 34

3.2.2 Fase 2: Priorización de los controles según las necesidades 54

3.2.3 Fase 3: Planificación y Preparación 54

3.2.4 Fase 4: Implementación 56

3.2.5 Fase 5: Monitorización, revisión y actualización 71

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 72

4.1 Conclusiones 72

4.2 Recomendaciones 73

REFERENCIAS BIBLIOGRÁFICAS 75

ANEXOS 77

ÍNDICE DE TABLAS

Tabla 1. Cadenas de búsqueda en bases de datos científicas. 2

Tabla 2. Criterios de inclusión y exclusión. 3

Tabla 3. Pasos de la metodología de los CIS Controls. 7

Tabla 4. CIS Controls básicos. 8

Tabla 5. CIS Controls funcionales. 8

Tabla 6. CIS Controls organizativos. 9

Tabla 7. Ficha de Observación 13

Tabla 8. Población de estudio. 15

Tabla 9. Entrevista al encargado de TI de la institución. 16

Tabla 10. Activos empresariales de la unidad educativa General Eloy Alfaro 36

Tabla 11. Inventario y control de activos empresariales. 38

Tabla 12. Inventario de software instalado. 39

Tabla 13. Resumen de vulnerabilidades encontradas. 52

Tabla 14. Evaluación de riesgos. 53

Tabla 15. Controles seleccionados. 54

Tabla 16. Cronograma o plan de acción 55

Tabla 17. Resumen de Controles y salvaguardas implementadas. 70

ÍNDICE DE FIGURAS

Figura 1. Datos de la pregunta 1. 18

Figura 2. Datos de la pregunta 2. 19

Figura 3. Datos de la pregunta 3. 19

Figura 4. Datos de la pregunta 4. 20

Figura 5. Datos de la pregunta 5. 21

Figura 6. Datos de la pregunta 6. 21

Figura 7. Datos de la pregunta 7. 22

Figura 8. Datos de la pregunta 8. 23

Figura 9. Datos de la pregunta 9. 23

Figura 10. Datos de la pregunta 10. 24

Figura 11. Datos de la pregunta 1. 25

Figura 12. Datos de la pregunta 2. 25

Figura 13. Datos de la pregunta 3. 26

Figura 14. Datos de la pregunta 4. 27

Figura 15. Datos de la pregunta 5. 27

Figura 16. Datos de la pregunta 6. 28

Figura 17. Datos de la pregunta 7. 29

Figura 18. Datos de la pregunta 8. 30

Figura 19. Datos de la pregunta 9. 31

Figura 20. Datos de la pregunta 10. 31

Figura 21. Topología de red de la unidad educativa General Eloy Alfaro. 35

Figura 22. Descubrimiento de host's en laboratorio – red 1. 37

Figura 23. Descubrimiento de host's en laboratorio – red 2. 37

Figura 24. Descubrimiento de host's en rectorado – red 3. 38

Figura 25. Desinstalación de software no autorizado. 41

Figura 26. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC01. 42

Figura 27. Resultados del escaneo de vulnerabilidades del pc UEGEA_PC02. 43

Figura 28. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC03. 44

Figura 29. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC04. 44

Figura 30. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC05. 45

Figura 31. Resultados del escaneo de vulnerabilidades del pc UEGEA_PC06. 45

Figura 32. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC07. 46

Figura 33. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC08. 47

Figura 34. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC09. 48

Figura 35. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC10. 48

Figura 36. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC11. 49

Figura 37. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC12. 50

Figura 38. Resultado del escaneo de vulnerabilidades del pc UEGEA_Rector. 50

Figura 39. Resultado del escaneo de vulnerabilidades del pc UEGEA_Vicerrector. 51

Figura 40. Resultado del escaneo de vulnerabilidades del pc UEGEA_Secretaria. .. 51

Figura 41. Activación de firewall de windows defender. 56

Figura 42. Configuración de contraseña en dispositivos de la institución. 57

Figura 43. Otorgación de permisos de administrador y usuario a cuentas de los activos empresariales. 58

Figura 44. Identificación del servicio de la vulnerabilidad encontrada. 59

Figura 45. Exportación del certificado. 60

Figura 46. Selección de la ruta de descarga del certificado. 60

Figura 47. Contenido del certificado. 61

Figura 48. Certificado vinculado a nessus. 61

Figura 49. Reinicio del servicio de nessus. 62

Figura 50. Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre). 62

Figura 51. Habilitación del servicio: Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre). 63

Figura 52. Confirmación de habilitación del servicio: Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre). 63

Figura 53. Regla que permite el escaneo desde la ip de nessus. 64

Figura 54. Ejecución de reglas para la mitigación de la vulnerabilidad. 65

Figura 55. Resultado de la mitigación de vulnerabilidades. 66

Figura 56. Resultado de la mitigación de vulnerabilidades. 66

Figura 57. Instalación de Avast Free Antivirus. 67

Figura 58. Tríptico usado en la capacitación. 81

Figura 59. Tríptico usado en la capacitación. 82

ÍNDICE DE ANEXOS

Anexo A. Encuesta a docentes de la Unidad Educativa General Eloy Alfaro. 77

Anexo B. Encuesta a estudiantes de la Unidad Educativa General Eloy Alfaro. 79

Anexo C. Tríptico sobre ingeniería social usado en la capacitación..... 81

RESUMEN EJECUTIVO

La creciente dependencia tecnológica en las instituciones educativas ha convertido a los sistemas de información en activos críticos, lo que subraya la necesidad de implementar estrategias sólidas de ciberseguridad para proteger datos confidenciales y garantizar la continuidad operativa. El propósito del presente trabajo se enfoca en la unidad educativa General Eloy Alfaro de la ciudad de Salcedo, que enfrenta importantes amenazas cibernéticas y físicas debido a los recursos limitados que posee y a la falta de prácticas de seguridad definidas.

La investigación inició con el levantamiento de los activos críticos y el análisis del estado actual de la red institucional. Seguidamente, se ejecutó el diagnóstico de la red mediante la herramienta de análisis de vulnerabilidades Nessus, los resultados obtenidos fueron clasificados bajo el marco de referencia de los CIS Controls, y a través de una matriz de riesgos cualitativa, se pudo medir el grado de exposición de la unidad educativa ante amenazas, sentando las bases para la propuesta de remediación.

Los resultados del diagnóstico revelaron que los riesgos más significativos se deben a la falta de controles esenciales como la firma SMB, Para mitigar estas deficiencias, se implementó una selección de los Controles CIS, escogidos y adaptados acorde a la infraestructura y recursos de la unidad educativa. Como resultado se aumentó la madurez en ciberseguridad de la unidad educativa proporcionando un modelo replicable y sostenible que fomente la cultura proactiva de la gestión de riesgos a pesar de las limitaciones presupuestarias.

Palabras claves: Ciberseguridad, CIS Controls, mitigación de vulnerabilidades, seguridad informática, unidades educativas.

ABSTRACT

The growing technological dependence in educational institutions has turned information systems into critical assets, which underscores the need to implement robust cybersecurity strategies to protect confidential data and ensure operational continuity. The purpose of this work focuses on the General Eloy Alfaro educational unit in the city of Salcedo, which faces significant cyber and physical threats due to its limited resources and the lack of defined security practices.

The research began with the identification of critical assets and the analysis of the institutional network's current status. Subsequently, a network diagnosis was carried out using the Nessus vulnerability analysis tool. The results obtained were classified under the CIS Controls framework, and through a qualitative risk matrix, the educational unit's degree of exposure to threats was measured, laying the foundation for the remediation proposal.

The diagnostic results revealed that the most significant risks were due to the lack of essential controls such as SMB signing. To mitigate these deficiencies, a selection of the CIS Controls was implemented, chosen and adapted according to the educational unit's infrastructure and resources. As a result, the cybersecurity maturity of the educational unit was increased, providing a replicable and sustainable model that promotes a proactive culture of risk management despite budgetary limitations.

Keywords: Cybersecurity, CIS Controls, vulnerability mitigation, information security, educational institutions.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

CIS CRITICAL SECURITY CONTROLS (CIS CONTROLS) PARA LA MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD EN LA INFRAESTRUCTURA DE RED DE LA UNIDAD EDUCATIVA GENERAL ELOY ALFARO DE LA CIUDAD DE SALCEDO.

1.1.1 Planteamiento del problema

A nivel mundial, la ciberseguridad se ha convertido en una de las principales preocupaciones debido al aumento de amenazas cibernéticas. En el 2024, los costos globales de los delitos cibernéticos alcanzaron los 9.5 billones de dólares y se espera que para el año 2025 esta cifra llegue a los 10.5 billones de dólares [1]. Además, se reportaron más de 30000 nuevas vulnerabilidades en el 2024, lo que representa un aumento del 17% respecto al año 2023 [2]. Estos datos muestran la escala de problemas y la necesidad urgente de realizar una intervención efectiva para reducir el riesgo cibernético en la infraestructura de redes.

En el contexto latinoamericano, la región ha experimentado un aumento significativo en los ciberataques. En el segundo trimestre de 2024, América Latina registró un aumento del 53% en los ataques cibernéticos, en comparación con el mismo período del año 2023. Siendo esta región la de mayor aumento a nivel mundial [3]. Este crecimiento resalta la urgente necesidad de fortalecer la infraestructura de ciberseguridad en la región, adoptando marcos y controles efectivos, como los propuestos por el Center for Internet Security (CIS).

Ecuador enfrenta desafíos significativos en materia de ciberseguridad. Según el informe mundial sobre ciberdelincuencia del año 2024 la capacidad del país para resistir incidentes cibernéticos sigue siendo limitada, lo cual se evidencia en sus bajos resultados en los distintos indicies internacionales. Con un Índice Nacional de Ciberseguridad de 53,25, un Índice de Exposición a la Ciberseguridad de 34,8, un Índice Global de Ciberseguridad de 26,3 y un Índice de Ciberresiliencia de 73,89 [4],

Ecuador enfrenta vulnerabilidades significativas a las ciberamenazas, teniendo en cuenta que las puntaciones son sobre 100 y que una mayor puntuación indica mejor preparación y madurez en ciberseguridad. Además, un informe de Kaspersky indicó que, entre agosto de 2022 y agosto de 2023, Ecuador fue el tercer país de América Latina con mayor número de ciberataques, solo superado por Brasil y México [5].

Dentro de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo, se evidencia la falta de una gestión adecuada de la seguridad informática. Esta situación puede generar efectos negativos en el funcionamiento diario de la institución, afectando su imagen institucional y provocando costos inesperados derivados de incidentes tecnológicos o fallas en los sistemas.

1.2 Antecedentes investigativos

Para la elaboración del presente proyecto, se llevó a cabo una revisión de la literatura mediante la exploración de varias fuentes de información certificadas, como el caso de Scielo, IEEE Xplore, Scopus y Google Scholar, las cuales son 4 de las fuentes de información académica más confiables. Las cadenas de búsqueda fueron establecidas utilizando palabras clave como: “CIS Controls”, “Mitigación de vulnerabilidades”, “Escuela”. Como resultado la Tabla 1 muestra los resultados obtenidos.

Tabla 1. Cadenas de búsqueda en bases de datos científicas.

Base de datos	Cadenas de búsqueda	Número de artículos
Scielo	("CIS Controls") Filtros activados: 2020 - 2024	1
IEEE Xplore	("All Metadata":"cis controls") AND ("All Metadata":"mitigation") Filters Applied: 2020 - 2025	4
Scopus	(ALL ("cis controls") AND TITLE-ABS-KEY ("mitigation") OR TITLE-ABS-KEY ("school")) AND PUBYEAR > 2019 AND PUBYEAR < 2026	23
Google Scholar	"CIS Controls" and ("vulnerability mitigation" or "school") 2020-2025	15
Total:		43

Esta revisión bibliográfica permitió realizar un análisis de los antecedentes pertinentes sobre la aplicación de un marco de ciberseguridad basado en los CIS Controls, en el ámbito de la educación y la infraestructura de red, Se utilizaron criterios de inclusión y exclusión detallados en la Tabla 2. Como resultado de este proceso se identificaron 5 artículos que cumplen con los criterios establecido para fundamentar el marco teórico que conlleva la presente investigación.

Tabla 2. Criterios de inclusión y exclusión.

Inclusión	• Estudios que evalúan la efectividad de las mitigaciones cibernéticas utilizando los CIS Controls. • Estudios que analizan los CIS Controls en entornos educativos u organizaciones similares en términos de infraestructura.
Exclusión	• Estudios que no estén relacionados con los CIS Controls. • Investigaciones orientadas a entornos grandes, cuya escala no es comparable a una unidad educativa. • Estudios anteriores al año 2019.

Honeres Chauca [6] diseñó e implementó un sistema de seguridad basado en los CIS Controls, para mitigar vulnerabilidades en la red Local Area Network (LAN) del Instituto Nacional de Evaluación Educativa (INEVAL), que incluye entornos educativos de nivel secundario. El estudio utilizó la herramienta InsightVM de Rapid7 para escanear vulnerabilidades en equipos críticos, detectando 58 vulnerabilidades, de las cuales 12 fueron críticas, 11 severas y 15 moderadas. La implementación se centró en aplicar controles como inventario de hardware y software, gestión de parches y configuraciones seguras, logrando una reducción significativa de las vulnerabilidades explotables. El proyecto se desarrolló con infraestructura que incluyó servidores Dell y sistemas operativos Windows Server 2019, demostrando que la adopción de los CIS Critical Security Controls (CIS Controls) es efectiva para fortalecer la seguridad en instituciones educativas con recursos limitados y redes complejas.

Pardo Sarango [7] buscó establecer un marco referencial para la implementación de controles de seguridad en la red de Minervilla, dentro del Grupo Chevez. Se utilizó como estándar los CIS Controls, que son un conjunto de mejoras prácticas en seguridad cibernética y acciones defensivas reconocidas a nivel mundial, destinadas a ayudar a los profesionales a administrar medidas de seguridad. El análisis inicial de la seguridad

informática de la empresa determinó que las medidas de seguridad existentes no garantizaban la protección de la red LAN contra ataques externos, haciendo necesaria la implementación de controles dictados por algún estándar. El trabajo adoptó los Controles CIS para proveer a la organización pautas claras, gestionando así su ciberseguridad con formalidad. La investigación incluyó una simulación práctica en la que se instaló y configuró un Firewall Sophos junto con Windows Server 2012 R2, y se generaron tres tipos de ataques para verificar la efectividad del firewall. Finalmente, el estudio recomendó realizar un análisis periódico de vulnerabilidades en los equipos de la red LAN para remediar las brechas de seguridad de forma proactiva, evitando la pérdida de información o fallos en los sistemas.

Según Ancajima Mendoza en [8] detalla la propuesta de implementación de seguridad informática aplicada en la Institución Educativa San Miguel Arcángel, Catacaos – Piura en Perú, donde se implementaron controles alineados con CIS para mitigar vulnerabilidades en equipos compartidos por 350 estudiantes. La investigación, desarrollada en 2023, utilizó servidores HP ProLiant DL380 con procesadores Intel Xeon E5-2650, 32 Gigabyte (GB) de Random Access Memory (RAM) y sistemas Windows Server 2022, implementando configuraciones seguras (CIS Control 4) mediante CIS-CAT Lite para endurecer 45 estaciones de trabajo. Los resultados mostraron una reducción del 68% en incidentes de malware tras aplicar políticas de control de acceso (CIS Control 14) y parches automatizados (CIS Control 7), validados mediante pruebas de penetración con Metasploit Framework 6.0 en laboratorios de informática. La metodología incluyó encuestas a 60 usuarios (docentes, administrativos y estudiantes), revelando que el 82% de las brechas se originaban en dispositivos Universal Serial Bus (USB) no autorizados, mitigadas mediante protección de puertos USB (CIS Control 9). El proyecto demostró que la implementación escalonada de IG1 permite a instituciones con presupuestos limitados alcanzar el 74% de cumplimiento con NIST SP 800-171 en 6 meses, priorizando controles como inventario de activos (CIS Control 1) y monitorización continua (CIS Control 8)

Santana Páez y Zurita Morales [9] se aplicó la metodología Top-Down Network Design junto con los controles CIS para rediseñar y fortalecer la red de datos de la institución, que atiende a una comunidad de aproximadamente 3 000 estudiantes y 135

docentes y administrativos. El análisis inicial identificó problemas de conectividad, cableado estructurado deficiente, distribución inadecuada de equipos inalámbricos y falta de medidas de seguridad tanto a nivel de hardware como de software. La implementación de los CIS Controls, especialmente en áreas como inventario y control de activos, gestión de parches y protección de la red, permitió mejorar la confidencialidad y disponibilidad de la información, así como optimizar el rendimiento de la red en un 63.3%, según simulaciones realizadas con Riverbed. Este caso demuestra cómo los CIS Controls pueden ser adaptados efectivamente para mejorar la seguridad y operación en instituciones educativas con infraestructura limitada.

Según se detalla en [10] el caso del Distrito Escolar de Hillsboro-Deering en New Hampshire, Neal Richardson, Director de Tecnología, implementó con éxito CIS Controls para mejorar la ciberseguridad y cumplir con las regulaciones estatales de privacidad estudiantil. Ante el desafío de priorizar las acciones de ciberseguridad en un entorno con recursos limitados y poca documentación, Richardson utilizó el Grupo de Implementación 1 (IG1) de los CIS Controls, que incluye 43 salvaguardas básicas como el inventario de activos, control de privilegios administrativos y protección de datos. Esta estrategia permitió al distrito escolar establecer una base sólida de seguridad durante 2019, facilitando la comprensión y aceptación de las medidas por parte de autoridades educativas y municipales. Posteriormente, el distrito planea avanzar hacia los grupos Grupo de Implementación 2 (IG2) y Grupo de Implementación 3 (IG3) para madurar su postura de ciberseguridad. A finales de 2019, Richardson recibió el Premio SANS Difference Maker por sus logros, dedicación y profesionalismo, tras implementar con éxito los Controles CIS del grupo IG1 en la red escolar y lograr que el distrito cumpla con la ley de privacidad estudiantil de New Hampshire.

1.3 Fundamentación teórica

1.3.1 Tecnologías de la Información (TI)

Las TI, o Tecnologías de la Información comprenden el estudio, diseño, desarrollo, implementación, soporte y gestión de sistemas informáticos, particularmente aplicaciones de software y hardware. Implican la utilización de computadoras y software para convertir, almacenar, proteger, procesar, transmitir y recuperar información de manera segura. Las TI abarcan no solo la infraestructura tecnológica en sí misma, sino también la forma en que esta tecnología se aplica y gestiona para resolver problemas y crear valor en diversos contextos organizacionales y sociales [11].

1.3.2 Seguridad Informática

La seguridad informática es un campo multidisciplinario que engloba la protección de los activos de información en el ciberespacio, incluyendo sistemas informáticos, redes de comunicación, datos almacenados y en tránsito, así como las personas involucradas en su uso y gestión. Implica la implementación de estrategias, políticas, procesos y tecnologías para garantizar la confidencialidad (previniendo la divulgación no autorizada), la integridad (asegurando la exactitud y completitud de la información) y la disponibilidad (garantizando el acceso oportuno y confiable a los recursos) frente a una variedad de amenazas, vulnerabilidades y riesgos cibernéticos. Además, considera aspectos como la autenticación, la autorización y la rendición de cuentas para asegurar un entorno digital seguro y confiable [12].

1.3.3 Marco de Seguridad

Un marco de seguridad es un conjunto estructurado de directrices, estándares, mejores prácticas y procesos diseñados para ayudar a las organizaciones a gestionar y reducir los riesgos de seguridad de la información. Proporciona una hoja de ruta y un lenguaje común para abordar la seguridad de manera integral y sistemática, facilitando la

planificación, implementación, evaluación y mejora continua de las defensas de seguridad [13].

a. Marco de ciberseguridad de los CIS Controls

El marco de los CIS Controls es un conjunto de mejores prácticas técnicas para reforzar la seguridad; estos controles proporcionan una hoja de ruta para que los administradores de TI mejoren la postura de seguridad de sus entornos de manera efectiva [12]. En la Tabla 3, se enumeran los pasos para implementar este marco en un entorno educativo.

Tabla 3. Pasos de la metodología de los CIS Controls.

Número	Pasos
1	Evaluar el estado de seguridad actual.
2	Priorizar los controles según las necesidades específicas.
3	Planificar y prepararse.
4	Implementación.
5	Monitorear, revisar y actualizar.

1.3.4 CIS Critical Security Controls (CIS Controls)

Los CIS Critical Security Controls (CIS Controls) son un conjunto priorizado de acciones de defensa contra los ciberataques más frecuentes y peligrosos. Proporcionan un punto de partida enfocado y procesable para mejorar la postura de ciberseguridad de una organización. Los CIS Controls están organizados en una estructura que va desde los controles fundamentales hasta los controles de implementación y gestión, reflejando una progresión para implementar y administrar la seguridad de manera efectiva. Están desarrollados y mantenidos por una comunidad global de expertos en seguridad, aprovechando el conocimiento de ataques del mundo real y contramedidas efectivas [14].

a. Controles básicos

Los controles básicos representan un conjunto de 6 controles fundamentales que cualquier organización debe implementar para asegurar la disponibilidad de sus

sistemas y establecer una defensa primaria contra ataques de ciberseguridad. Estos controles se detallan en la Tabla 4.

Tabla 4. CIS Controls básicos.

Control	Título del Control
CIS Control 1	Inventario y control de los activos empresariales.
CIS Control 2	Inventario y control de activos de software.
CIS Control 3	Protección de datos.
CIS Control 4	Configuración segura de activos y software empresarial.
CIS Control 5	Administración de cuentas.
CIS Control 6	Gestión de control de accesos.

b. Controles funcionales

Los controles funcionales representan un conjunto de 10 controles enfocados a la seguridad de la información. Su propósito es asegurar una protección adecuada contra las amenazas cibernéticas, contribuyendo cada uno a la estrategia integral de ciberseguridad. Estos controles se detallan en la Tabla 5.

Tabla 5. CIS Controls funcionales.

Control	Título del Control
CIS Control 7	Gestión continua de vulnerabilidades.
CIS Control 8	Gestión de registros de auditoría.
CIS Control 9	Protección del correo electrónico y navegador web.
CIS Control 10	Defensas contra malware.
CIS Control 11	Recuperación de datos.
CIS Control 12	Gestión de la infraestructura de red.
CIS Control 13	Monitoreo y defensa de la red.
CIS Control 14	Concientización en seguridad y formación de habilidades.
CIS Control 15	Gestión de proveedores de servicios.
CIS Control 16	Seguridad en el software de aplicación.

c. Controles organizativos

Los controles organizativos buscan establecer una cultura de seguridad robusta. Están diseñados para integrar prácticas seguras en todos los procesos y áreas de la organización con el fin de salvaguardar la información. Estos controles se detallan en la Tabla 6.

Tabla 6. CIS Controls organizativos.

Control	Título del Control
CIS Control 17	Gestión de respuesta a incidentes.
CIS Control 18	Pruebas de penetración.

1.3.5 Unidad educativa

Una unidad educativa es una institución o establecimiento organizado para proporcionar educación formal a estudiantes en diferentes niveles, estos pueden abarcar desde la educación inicial hasta la educación secundaria. Estas unidades están diseñadas para facilitar el proceso enseñanza-aprendizaje, fomentando el desarrollo integral de los estudiantes en aspectos académicos, sociales, emocionales y, en algunos casos, vocacionales. Suelen estar gestionados por entidades gubernamentales, privadas o religiosas y operan bajo las regulaciones del sistema educativo de un país o región.

1.3.6 Infraestructura tecnológica

La infraestructura tecnológica comprende los recursos físicos (hardware, redes, instalaciones) y los servicios (software, sistemas operativos, almacenamiento de datos) compartidos que proporcionan una plataforma para las aplicaciones de sistemas de información de una empresa. Es la base sobre la cual se construyen y operan los sistemas de información [15].

1.3.7 Componentes de red

Los componentes de red son las entidades físicas y lógicas necesarias para establecer la comunicación y el intercambio de datos entre dispositivos en una red de computadoras. Estos incluyen el medio de transmisión (alámbrico o inalámbrico), los dispositivos de interconexión (como routers y switches que dirigen el tráfico) y los dispositivos finales (como computadoras y servidores) que se comunican a través de la red [16].

1.3.8 Vulnerabilidad

Aplicar Una vulnerabilidad representa una flaqueza inherente en un sistema de información, ya sea en su diseño arquitectónico, la manera en que fue implementado a través de software o hardware, o en cómo está configurado para operar. Esta debilidad se convierte en un punto de entrada potencial para una amenaza, que puede ser un individuo malintencionado, un grupo organizado o incluso un proceso automatizado. La explotación exitosa de una vulnerabilidad puede tener diversas consecuencias perjudiciales, incluyendo el acceso no autorizado a información sensible, la interrupción de los servicios que el sistema proporciona, la alteración o destrucción de datos, o la capacidad de utilizar el sistema comprometido para lanzar ataques contra otros objetivos. La identificación y mitigación de estas vulnerabilidades es un aspecto fundamental de la ciberseguridad para proteger los activos digitales y garantizar la continuidad de las operaciones [17].

1.4 Objetivos

1.4.1 Objetivo general

Aplicar los CIS Critical Security Controls (CIS Controls) como estrategia de mitigación contra vulnerabilidades de seguridad en la infraestructura de red de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo.

1.4.2 Objetivos específicos

- Analizar el estado actual de la infraestructura de red de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo para identificar vulnerabilidades presentes.
- Escanear las vulnerabilidades de los equipos tecnológicos utilizando el marco de ciberseguridad de los CIS Critical Security Controls (CIS Controls) en la

infraestructura de red de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo.

- Implementar las acciones de mitigación proporcionadas por los CIS Critical Security Controls (CIS Controls) de acuerdo a las vulnerabilidades encontradas en la infraestructura de red de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para el presente proyecto de investigación dentro de la Unidad Educativa General Eloy Alfaro se emplearon herramientas que facilitaron una mejor comprensión del panorama dentro de la red institucional, primero se realizó una encuesta a los docentes y estudiantes, y una entrevista al docente responsable del área de TI de la Unidad Educativa. Finalmente, se utilizó una ficha de observación para registrar información relevante durante el proceso de desarrollo del proyecto.

2.1.1 Encuesta dirigida a docentes

Con el propósito de conocer el nivel de conocimiento y las percepciones de los docentes de la unidad educativa General Eloy Alfaro en relación a la seguridad informática, se diseñó y aplicó una encuesta, como se detalla en el Anexo A.

2.1.2 Encuesta dirigida a estudiantes

Con el propósito de conocer el nivel de conocimiento y las percepciones de los docentes de la unidad educativa General Eloy Alfaro en relación a la seguridad informática, se diseñó y aplicó una encuesta, como se detalla en el Anexo B.

2.1.3 Entrevista al docente encargado del área de TI de la Unidad Educativa

Con el propósito de conocer la gestión informática de la institución se llevó a cabo una entrevista semiestructurada con el encargado de TI de la unidad educativa, siendo esta una técnica clave para conocer la situación actual de la seguridad informática. Los temas centrales incluyeron la gestión de datos, las prioridades de ciberseguridad, la disponibilidad de recursos, y el registro de incidentes. También se evaluaron las medidas de seguridad existentes, los procesos de auditoría, la conciencia de riesgo de la comunidad y la sostenibilidad económica de las mejoras propuestas. Las respuestas obtenidas, que se presentan de forma tabulada en la Tabla 9, permitieron establecer un

diagnóstico claro sobre el nivel de seguridad de la institución y sus principales vulnerabilidades.

2.1.4 Ficha de observación

Se utilizó una ficha de observación como se detalla en la Tabla 7, como instrumento de validación, enfocada en la inspección directa de los componentes de hardware y software que conforman la infraestructura de red.

Tabla 7. Ficha de Observación

N° Ficha: F01		Ubicación: Laboratorio de computación de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo	
		Fecha: 14/10/2025	
Responsable: Carlos David Quispe Silva		Hora: 10:00 AM.	
ASPECTOS POR OBSERVAR	SI	NO	OBSERVACIÓN
Observar si las áreas donde se encuentran los equipos tecnológicos se encuentran restringidas a personal autorizado mediante controles físicos.		X	No se observan controles de acceso adecuados, el laboratorio es accesible únicamente con un llave que se entrega en rectorado.
Verificar si existen medidas de seguridad contra incendios, humedad u otros daños físicos.		X	Debido a la falta de presupuesto, no se cuenta con conexiones eléctricas adecuadas, además, debido al uso intensivo de dispositivos y herramientas en otros laboratorios, en ocasiones las computadoras se apagan repentinamente
Observar si los equipos tienen pantallas de inicio de sesión con contraseña obligatoria.		X	Los equipos inician sesión con el usuario por defecto.
Observar si existe un software antivirus/antimalware activo y actualizado.		X	No se observa la instalación de un software de protección de virus, lo que deja expuesto a los dispositivos a infecciones por malware y virus, comprometiendo la integridad de la información.
Observar si los puertos USB de los equipos se encuentran controlados.		X	Los puertos USB de las estaciones de trabajo no presentan controles de acceso, tanto físicas como de software, lo que permite la conexión de dispositivos

			externos desconocidos y la posible introducción de malware.
Verificar si los datos de los estudiantes, docentes y personal administrativo se encuentran respaldados de manera segura.		X	La mayoría de la información de los estudiantes se guarda en memorias USB y en discos duros de las computadoras del laboratorio y laptops personales de los docentes, lo que representa un riesgo significativo para la seguridad y la integridad de los datos.
Verificar si los equipos de red están etiquetados y sus contraseñas por defecto han sido modificadas.	X		Las contraseñas de defecto de los dispositivos de red fueron cambiadas y se encuentran bajo supervisión de la secretaria de la institución.
Observar si existe información sensible (por ejemplo, contraseñas) visible en el área de trabajo.		X	No existe evidencia de información sensible cerca del área de trabajo.
Observar si existen avisos que recuerden a los usuarios políticas básicas sobre seguridad informática (por ejemplo, no abrir correos sospechosos o no conectar dispositivos USB desconocidos).		X	No existe programa de concientización lo que aumenta la probabilidad de incidentes derivados al error humano.
Conclusiones: La institución presenta deficiencia en las medidas de seguridad tanto físicas como lógicas como actualización de antivirus, políticas de respaldo y control de acceso a los equipos, lo que aumenta el riesgo de explotación de vulnerabilidades. Es importante resolver estas falencias para garantizar un entorno seguro y funcional.			

2.2 Métodos

2.2.1 Modalidad de la investigación

La presente investigación se centra en la modalidad de investigación de campo y bibliográfica-documental.

Investigación de campo

Se enfocó en la recopilación de información directa en el entorno institucional mediante la evaluación del estado actual de la red, incluyendo una entrevista al

encargado de TI, así encuestas al personal decente y estudiantil de la unidad educativa General Eloy Alfaro, esto permitió tomar decisiones fundamentales para mejorar la seguridad de la red institucional.

Investigación bibliográfica-documental

La investigación se apoyó en la modalidad bibliográfica-documental, ya que parte del análisis de libros, artículos científicos, informes especializados, guías técnicas y documentos institucionales relacionados con la gestión de la seguridad informática, se sustenta en la revisión de fuentes académicas, técnicas y normativas que aborda la ciberseguridad, las vulnerabilidades en infraestructura de red y la implementación de los CIS Controls.

2.2.2 Población y muestra

La población con la cual se trabajó en el proyecto está conformada principalmente por el personal que participa directa o indirectamente en el manejo, administración y uso de la infraestructura tecnológica de la Unidad Educativa General Eloy Alfaro de la ciudad de Salcedo, provincia de Cotopaxi, tal y como se muestra en la Tabla 8.

Tabla 8. Población de estudio.

Población	Número	Porcentaje
Administrativos	5	2.44 %
Docentes	20	9.76 %
Estudiantes	180	87.80 %
Total	205	100%

Para el grupo de estudiantes al tener una población mayor a 100, se aplicó la siguiente fórmula para determinar una muestra significativa de estudiantes, para aquello se estableció, un nivel de confianza de 1,96 y un error de estándar de 0,09:

$$\mathrm{n} = \frac{N\sigma^2\mathrm{Z}^2}{(N-1)e^2 + \sigma^2\mathrm{Z}^2}$$

Donde:

- n = tamaño de la muestra
- N = tamaño de la población = 180 o 205
- σ^2 = desviación estándar = 0,5
- Z = Nivel de confianza 95% = 1,96
- e = Error estándar del 9% = 0.09

$$n = \frac{(180)\ (0{,}5)^2(1{,}96)^2}{(180-1)(0{,}09)^2 + \ (0{,}5)^2(1{,}96)^2}$$

$$n = 71{,}72$$

Dando como resultado que la muestra corresponde a 72 estudiantes.

Respecto a los demás grupos como el personal de rectorado, personal administrativo y personal docente estos no superan los 100 individuos, por lo tanto, se incluye a toda la población en el estudio. En total se determina, 97 individuos, a quienes se les aplicarán los métodos de recolección de datos.

2.2.3 Recolección de información

Entrevista al encargado de TI de la institución

Se realizó una entrevista docente encargado de TI de la institución para conocer aspectos relevantes de la seguridad informática de la red de la unidad educativa General Eloy Alfaro.

Tabla 9. Entrevista al encargado de TI de la institución.

Datos Personales Institución: Unidad Educativa General Eloy Alfaro Entrevistado: Ing. Lenin Ortíz Cargo: Docente de Computación y encargado de TI Fecha: 03/10/2025			
N°	Pregunta	Respuesta	Observación
1	¿Cuál es el estado actual de la red de la unidad educativa en términos de seguridad?	Mala no existe un sistema de protección hacia los equipos de la institución.	No consta con ningún sistema dirigido a seguridad.

2	¿Ha enfrentado incidentes de seguridad? En caso de ser afirmativo, ¿cuál es el más grave que ha sufrido la unidad educativa?	No	
3	¿Con qué frecuencia realiza evaluaciones de la seguridad en la infraestructura de red de la unidad educativa?	Muy poca, no existe ningún plan de seguridad a ejecutarse.	
4	¿Cómo gestiona la unidad educativa el acceso a la red para el personal administrativo, docente y estudiantes?	La generación de claves	Se cambia cada cierto tiempo
5	¿La institución cuenta con un inventario de activos? En caso de ser afirmativo, ¿cómo lo mantiene?	Sí, la institución cuenta con un inventario de activos, el cual se mantiene de manera actualizada mediante registros digitales y físicos.	
6	¿Existe algún proceso para garantizar que los sistemas operativos y aplicaciones de la red se encuentren actualizados?	No, actualmente la institución no cuenta con un proceso formal para garantizar que los sistemas operativos y aplicaciones de la red se mantengan actualizados. Las actualizaciones se realizan de manera eventual y sin un seguimiento sistemático,	
7	¿La unidad educativa cuenta con políticas sobre el uso de contraseñas o la instalación de software?	No, la unidad educativa no cuenta con políticas establecidas sobre el uso de contraseñas ni sobre la instalación de software. Esta ausencia de normas dificulta el control y la seguridad en el manejo de los equipos y sistemas	
8	¿Con qué frecuencia se realizan copias de seguridad de los datos sensibles (calificaciones, registros de estudiantes y personal docente y administrativo) y como verifica la integridad de los mismos?	Solo cuando es datos importantes y se solicite que existan respaldos.	
9	¿La unidad educativa realiza charlas o existe un programa de formación o concientización en ciberseguridad para el personal	La unidad educativa no realiza charlas ni cuenta con un programa de formación o	

	docente, administrativo y estudiantes?	concientización en ciberseguridad dirigido al personal docente, administrativo o a los estudiantes.	
10	¿Qué tan factible ve la implementación de controles y buenas prácticas de seguridad estandarizados como los CIS Critical Security Controls (CIS Controls)?	La implementación de controles y buenas prácticas de seguridad estandarizados como los CIS Critical Security Controls es factible, porque la institución cuenta con la infraestructura.	Sin embargo, la infraestructura todavía en la institución es insuficiente.

Encuesta realizada a docentes

Pregunta 1: ¿Sabe usted si la Unidad Educativa cuenta con un inventario de activos informáticos?

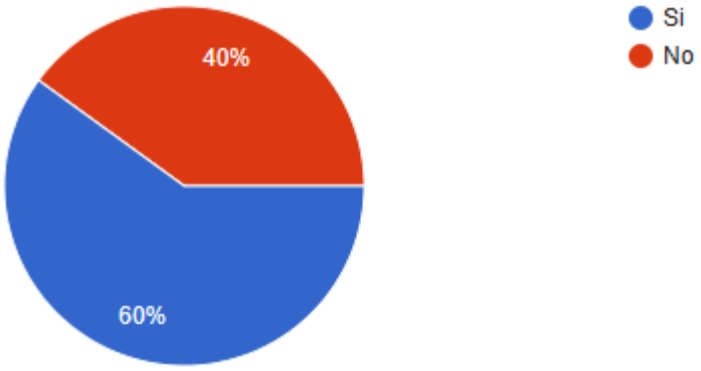


Figura 1. Datos de la pregunta 1.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 1, el 60% de los docentes indicó que tiene conocimiento de que la unidad educativa cuenta con un inventario de activos informáticos, mientras que el 40% señaló que no tiene conocimiento del mismo, lo que indica una brecha crítica en la gestión de activos dentro de la institución.

Pregunta 2: ¿Con qué frecuencia utiliza los equipos y la red de la Unidad Educativa?

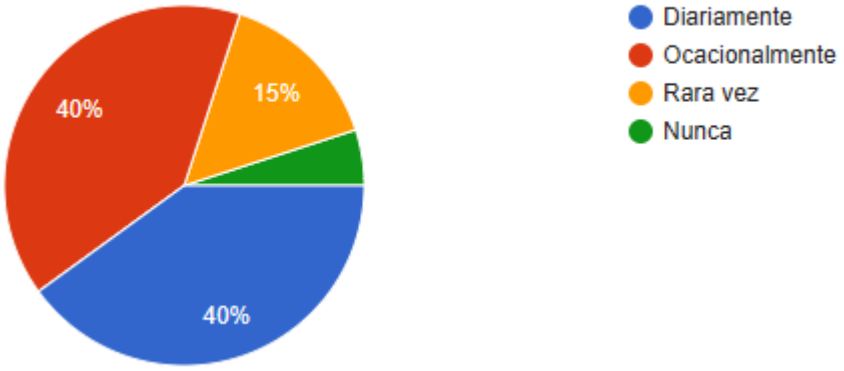


Figura 2. Datos de la pregunta 2.

Análisis e interpretación de resultados

Según los resultados mostrados en la figura 2, un 40% de los docentes utilizan diariamente los equipos y la red de la institución, de la misma manera un 40% de los docentes los utilizan de manera ocasional, mientras que el 15% de los docentes los utilizan rara vez, y un 5% indicó que nunca han usado los equipos ni la red de la institución, lo que señala la criticidad de la infraestructura de red para las operaciones diarias y corrobora la urgencia de mitigar vulnerabilidades.

Pregunta 3: ¿Qué tan segura considera que es la red de la unidad educativa para proteger su información personal e institucional?

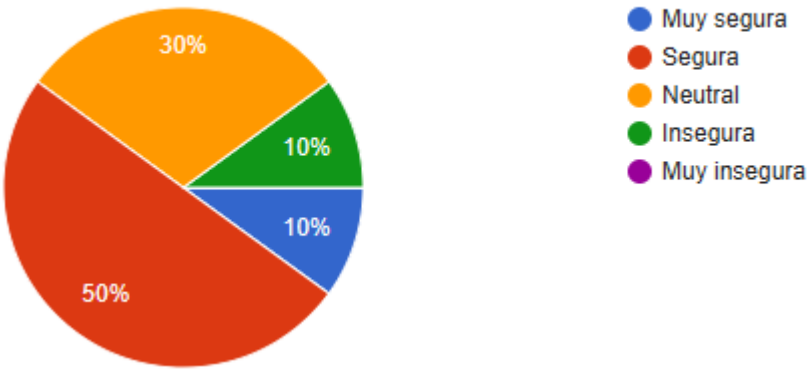


Figura 3. Datos de la pregunta 3.

Análisis e interpretación de resultados

En base a los resultados obtenidos en la figura 3, la mayoría de los encuestados perciben una seguridad aceptable: el 50% la considera segura y un 10% muy segura, sumando un 60% de percepción positiva. Sin embargo, es notable que un 30% se mantiene neutral y un 10% la percibe como insegura, lo que totaliza un 40% de incertidumbre o percepción negativa. Lo que demuestra una falta de confianza o conocimiento sobre las medidas de protección existentes.

Pregunta 4: ¿Alguna vez ha notado problemas de rendimiento al momento de utilizar la red de la unidad educativa?

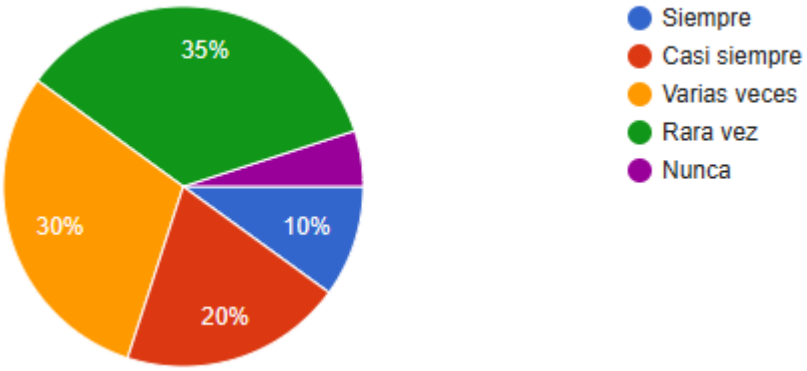


Figura 4. Datos de la pregunta 4.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 4, existe una alta incidencia de problemas de rendimiento en la red: el 10% reporta problemas siempre, el 20% casi siempre, y el 30% varias veces, lo que suma un 60% de encuestados que experimentan fallos de rendimiento de forma recurrente. Si bien un 35% señala rara vez, la minoría que nunca los ha notado es solo del 5%. Lo que indica la existencia de vulnerabilidades de estabilidad y disponibilidad que deben ser mitigadas. Los problemas de rendimiento suelen ser síntomas de una mala gestión de la red, congestión, o incluso la presencia de malware

Pregunta 5: A recibido correos sospechosos (phishing) en sus cuentas de correos electrónicos?

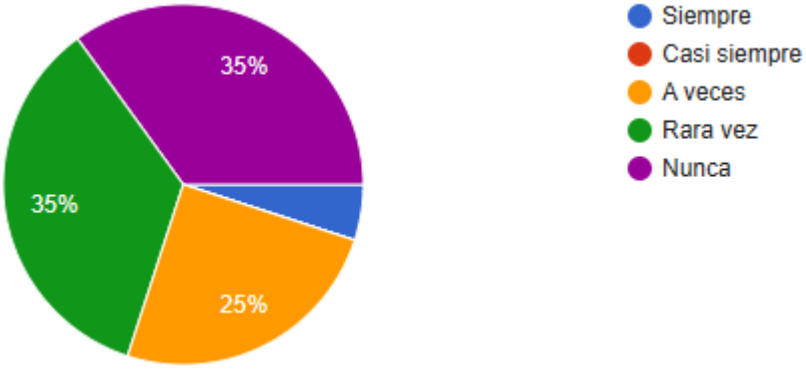


Figura 5. Datos de la pregunta 5.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura, una mayoría significativa del 65% de los encuestados ha recibido correos sospechosos (phishing): el 5% reporta recibirlos siempre, el 35% rara vez, y el 25% a veces. Solo un 35% afirma nunca haberlos recibido. Estos datos indican que phishing es una vulnerabilidad crítica que explota el factor humano, ya que el correo electrónico es una vía primaria de infección de la red y robo de credenciales.

Pregunta 6: ¿Qué tan familiarizado se encuentra respecto a medidas de prevención y mitigación de vulnerabilidades de seguridad?

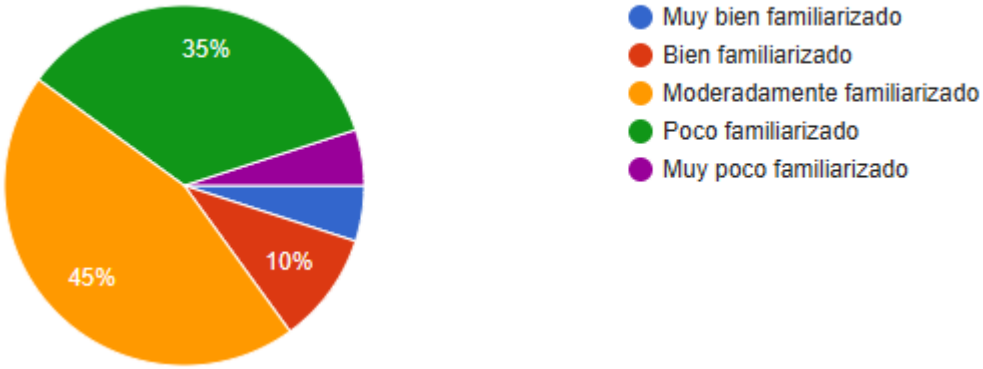


Figura 6. Datos de la pregunta 6.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 6, el conocimiento sobre medidas de seguridad es predominantemente bajo a moderado. Un 45% se siente moderadamente familiarizado, un 35% poco familiarizado y un 5% muy poco familiarizado, sumando un 85% de encuestados que no tienen un alto nivel de confianza en su conocimiento de seguridad. Solo el 10% se siente bien familiarizado y el 5% muy bien familiarizado. Estos resultados sugieren que existe una gran área de mejora en cuanto a medidas de prevención y mitigación de vulnerabilidades de seguridad.

Pregunta 7: ¿Estaría de acuerdo en recibir capacitación sobre ciberseguridad para ayudar a proteger su información y la de la Unidad Educativa?

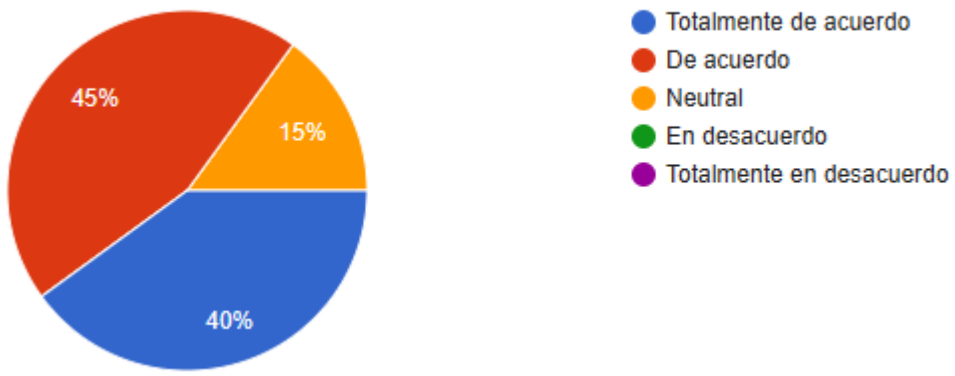


Figura 7. Datos de la pregunta 7.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 7, existe una voluntad abrumadora y positiva para recibir formación en ciberseguridad: el 40% está totalmente de acuerdo y el 45% está de acuerdo, sumando un 85% de aprobación. Solo un 15% se mantuvo en una postura neutral. Estos resultados ofrecen una validación social y operativa crucial para la implementación de acciones de mitigación.

Pregunta 8: ¿Considera que la implementación de medidas adicionales de seguridad (por ejemplo, doble autenticación) mejorará la seguridad de acceso a las cuentas?

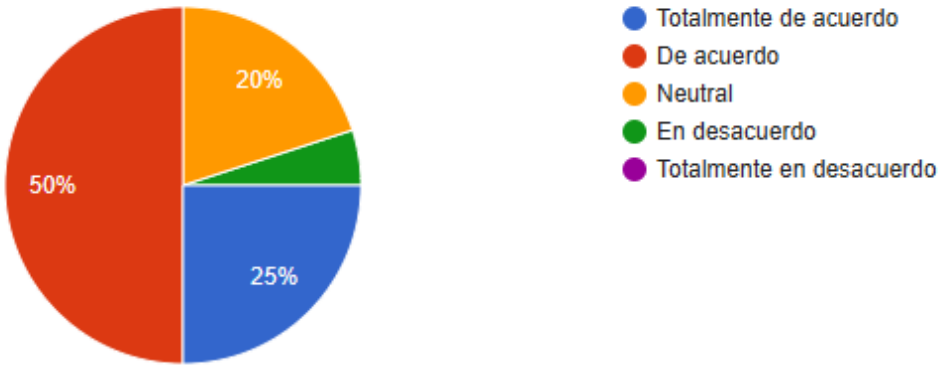


Figura 8. Datos de la pregunta 8.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 8, existe un fuerte consenso en que las medidas adicionales de seguridad son beneficiosas: el 25% está totalmente de acuerdo y el 50% está de acuerdo, sumando un 75% de aprobación. Solo un 5% se encuentra en desacuerdo, siendo el 20% restante neutral. Lo que indica que el personal está preparado para aceptar la implementación de controles que añadan fricción al acceso, como la autenticación multifactor (MFA)

Pregunta 9: ¿Cree que la unidad educativa es vulnerable a ataques de seguridad?

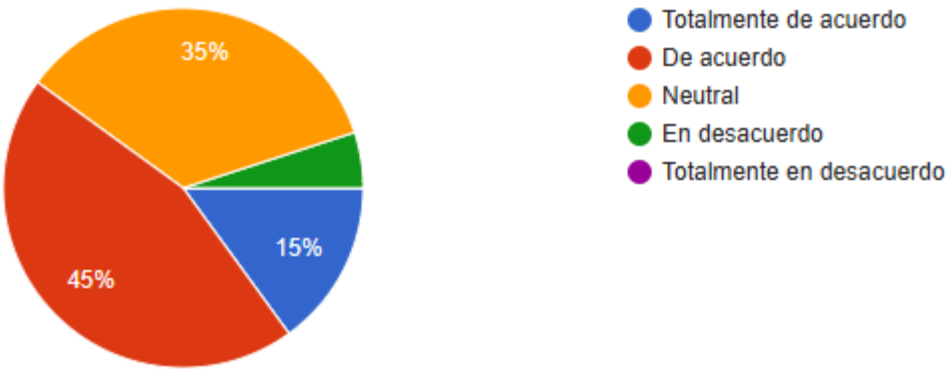


Figura 9. Datos de la pregunta 9.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 9, existe una percepción mayoritaria de vulnerabilidad entre los encuestados: el 45% está de acuerdo y el 15% está totalmente de acuerdo, sumando un 60% que reconoce el riesgo de ataque. Un 35% se mantiene neutral, y solo un 5% está en desacuerdo. Lo que señala que el personal es consciente de que la infraestructura es un blanco potencial. Este reconocimiento facilita la justificación para la implementación de acciones de mitigación.

Pregunta 10: ¿Cree que la implementación de un conjunto priorizado de mejores prácticas de ciberseguridad como los CIS Critical Security Controls (CIS Controls) será beneficioso para la Unidad Educativa?

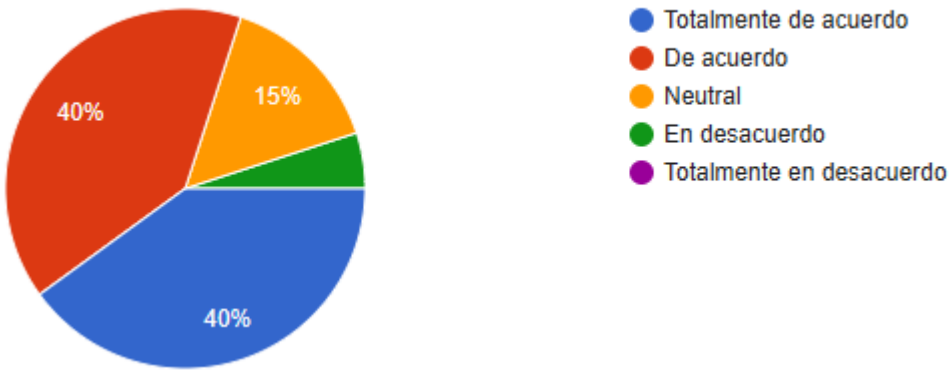


Figura 10. Datos de la pregunta 10.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 10, existe un apoyo masivo: el 40% está totalmente de acuerdo y otro 40% está de acuerdo, sumando un 80% de aprobación. Solo un 5% se encuentra en desacuerdo, siendo el 15% restante neutral. Estos datos indican que el personal percibe la necesidad de un marco estructurado y priorizado como los CIS Controls para solucionar las vulnerabilidades.

Encuesta realizada a estudiantes

Pregunta 1: ¿Con qué frecuencia utiliza los equipos y la red de la Unidad Educativa?

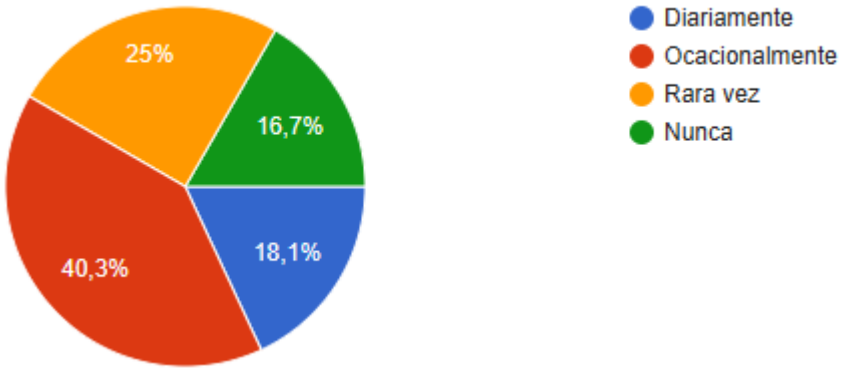


Figura 11. Datos de la pregunta 1.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 11, la mayoría de los estudiantes utiliza la red y los equipos de la Unidad Educativa de forma frecuente, diariamente lo utilizan el 18.1%, ocasionalmente lo utiliza el 40.3%, un 25% los utiliza rara vez, y un 16.7% reporta nunca utilizarlos. Lo que sugiere que la exposición al riesgo no es constante, pero sí masiva e indica que cualquier vulnerabilidad técnica o humana tiene un alto potencial de propagación debido al volumen de usuarios.

Pregunta 2: ¿Ha notado mal funcionamiento en los equipos de la Unidad Educativa?

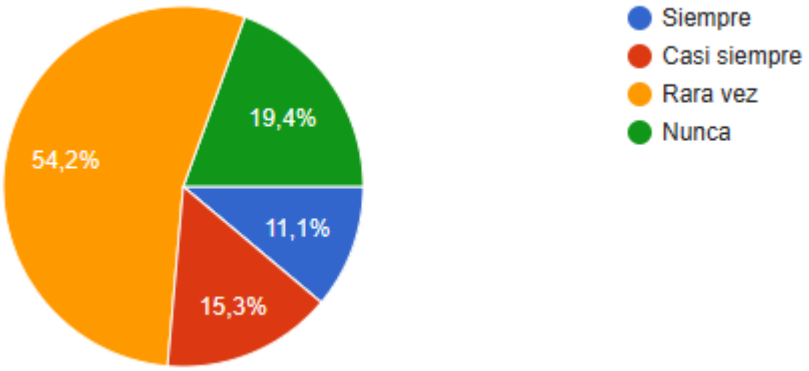


Figura 12. Datos de la pregunta 2.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 12, una abrumadora mayoría de los estudiantes ha experimentado mal funcionamiento en los equipos de la Unidad Educativa: el 11.1% reporta problemas siempre, el 15.3% casi siempre, y un 54.2% rara vez, lo que suma un 80.6% de incidencias de fallos. Solo el 19.4% nunca ha notado un mal funcionamiento. Estos datos señalan que los problemas recurrentes en los equipos son un síntoma claro de vulnerabilidades no mitigadas, que pueden incluir software desactualizado, configuraciones inseguras, o la presencia de malware.

Pregunta 3: ¿Qué tan seguro se siente al utilizar la red de la Unidad Educativa?

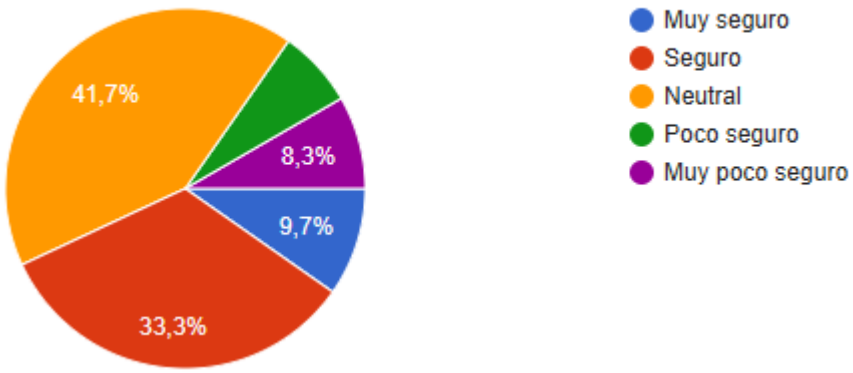


Figura 13. Datos de la pregunta 3.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 13, existe una gran incertidumbre en la percepción de seguridad de los estudiantes. El 41.7% se siente neutral respecto a la seguridad de la red. Al sumar este grupo al 15% (Poco Seguro + Muy Poco Seguro) que tiene una percepción negativa, se obtiene un 56.7% de estudiantes sin confianza o con dudas sobre la seguridad de la red. Solo el 43% (9.7% Muy Seguro + 33.3% Seguro) tiene una percepción positiva. Estos datos señalan la necesidad de implementar acciones de mitigación que sean visibles y comunicadas para mejorar la protección y luego difundir que estas medidas estén activas.

Pregunta 4: ¿Qué tan informado está sobre la importancia de utilizar una contraseña segura y por qué es importante?

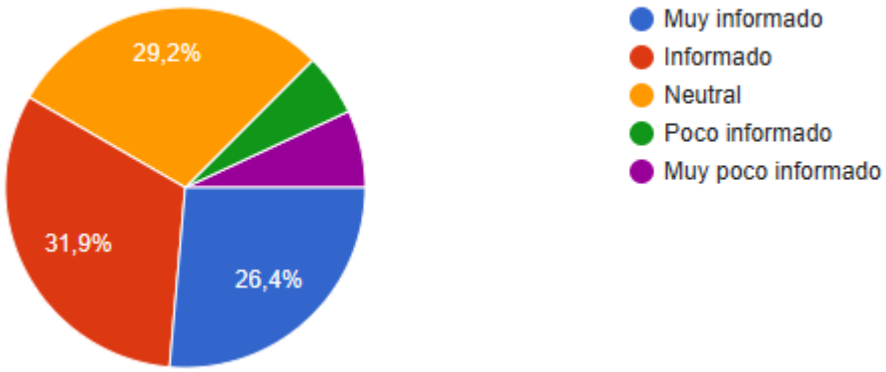


Figura 14. Datos de la pregunta 4.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 14, existe una distribución de conocimiento sobre contraseñas, pero una alta proporción de estudiantes no está completamente informada: un 29.2% es neutral, un 5.6% poco informado y un 5.6% muy poco informado sumando un 40.4% con bajos conocimientos, aunque un 58.3% (26.4% Muy informado + 31.9% Informado) tiene una noción positiva. Lo que indica la falta de conocimiento en un 40% de la población estudiantil sobre la creación y uso de contraseñas seguras representa una vulnerabilidad crítica de credenciales.

Pregunta 5: ¿Alguna vez ha tenido dificultad en descargar archivos o en acceder a sitios web desde los equipos de la Unidad Educativa?

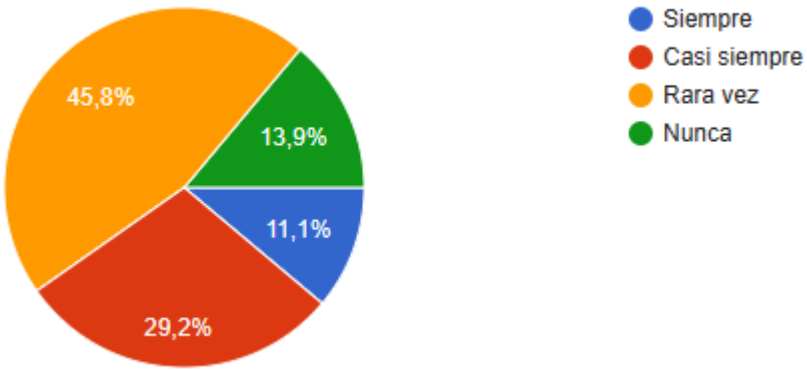


Figura 15. Datos de la pregunta 5.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 15, una abrumadora mayoría de los estudiantes ha experimentado dificultades con las descargas o el acceso a sitios web: el 45.8% reporta problemas rara vez, el 29.2% casi siempre, y el 11.1% siempre, sumando un 86.1% de incidencia. Solo el 13.9% nunca ha tenido dificultad. Estos datos señalan que los problemas para descargar o acceder a sitios pueden ser causados por una congestión de red, políticas de filtrado mal configuradas o la presencia de malware afectando la conexión.

Pregunta 6: ¿Confía en que los trabajos y archivos que guarda en los equipos de la Unidad Educativa están seguros y no se perderán?

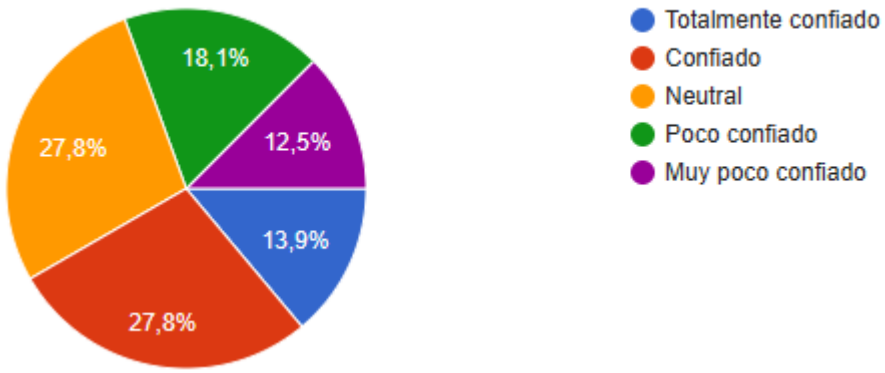


Figura 16. Datos de la pregunta 6.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 16, existe una división de confianza con una inclinación significativa hacia la incertidumbre. La confianza total y parcial suma un 41.7% (13.9% Totalmente Confiado y 27.8% Confiado). Sin embargo, el 27.8% tiene una postura neutral, el 18.1% Poco Confiado y el 12.5% muy poco confiado lo que expresa duda o desconfianza en la seguridad y permanencia de sus archivos. Lo que señala que la preocupación por la pérdida de trabajos escolares sugiere fallas en las políticas de backup y la gestión de la integridad de los equipos.

Pregunta 7: ¿Cree que los equipos de la Unidad Educativa se encuentran protegidos contra programas maliciosos o virus?

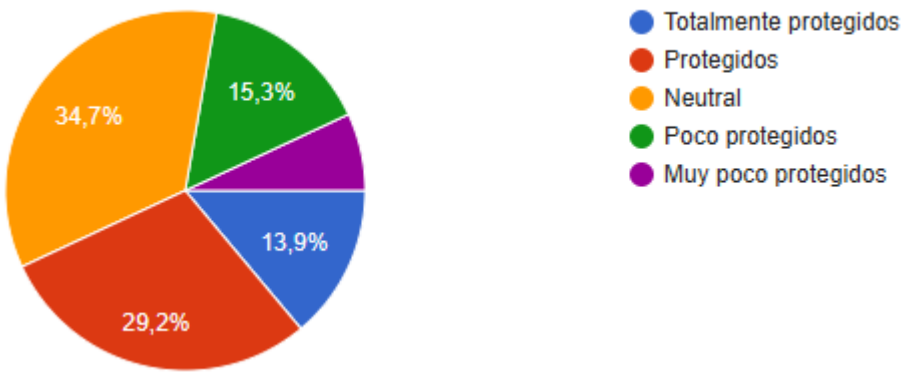


Figura 17. Datos de la pregunta 7.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 17, existe una gran incertidumbre y desconfianza en la protección de los equipos. Un notable 34.7% se mantiene neutral. Al sumar aquellos que se sienten poco protegidos 15.3% y muy poco protegidos 7.0%, se obtiene un 57% de estudiantes con duda o baja percepción de protección contra malware. Solo el 43.1% (13.9% Totalmente protegidos + 29.2% Protegidos) tiene una percepción positiva. Lo que sugiere que la alta tasa de duda y desconfianza valida la necesidad de aplicar una defensa contra malware que sea visible, efectiva y conocida por los usuarios para mitigar el riesgo de infecciones y mejorar la confianza en la infraestructura.

Pregunta 8: ¿Con qué frecuencia ha accedido a cuentas personales desde los equipos de la Unidad Educativa?

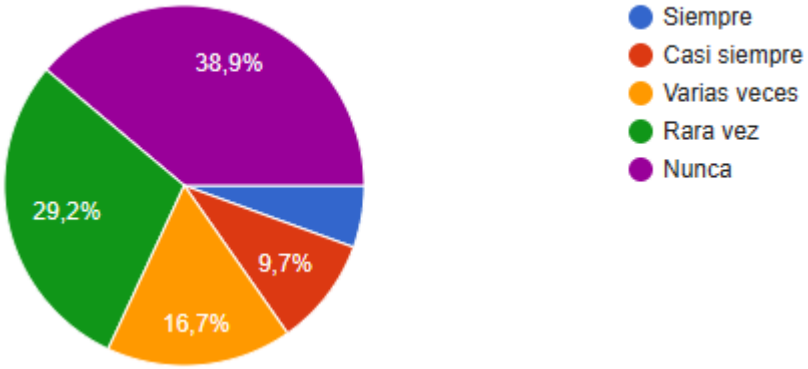


Figura 18. Datos de la pregunta 8.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 18, una mayoría del 68.1% de los estudiantes accede a cuentas personales (sumando Siempre, Casi Siempre, Varias Veces y Rara Vez). Aunque la frecuencia es baja para muchos ("Rara vez" con 29.2%), es significativo que el 31.4% (9.7% Casi Siempre, 16.7% Varias Veces, 5% Siempre) acceda a sus cuentas personales con cierta regularidad. Solo el 38.9% reporta no haber accedido nunca. Según los datos recolectados se puede indicar que el hecho de que una parte significativa de la población estudiantil utilice equipos compartidos de la institución para acceder a cuentas personales genera un alto riesgo de fuga de datos o robo de credenciales, de igual manera indica la necesidad de fortalecer el control de cuentas de acceso.

Pregunta 9: ¿Estaría de acuerdo en seguir normas más estrictas en el uso de la red de la Unidad Educativa con el fin de tener una red más segura?

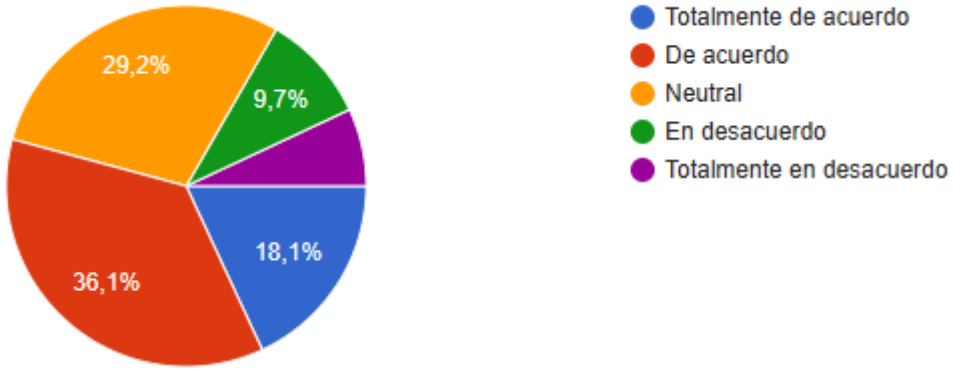


Figura 19. Datos de la pregunta 9.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 19, existe una mayoría dispuesta a aceptar medidas de seguridad más estrictas: el 18.1% está totalmente de acuerdo y el 36.1% está de acuerdo, un 29.2% se mantiene Neutral, y solo el 16.9% (9.7% En Desacuerdo y 7.2% Totalmente en Desacuerdo) se opone. Lo que indica una validación social crucial para la implantación de acciones de mitigación. Esta disposición facilita la aplicación de políticas más rígidas inherentes al marco CIS Controls, asegurando que la propuesta de mitigación no genere un conflicto operativo significativo.

Pregunta 10: ¿Estaría de acuerdo con tener una red más segura en la Unidad Educativa, aunque esto signifique tener una mayor restricción sobre la navegación y descarga de archivos o software?

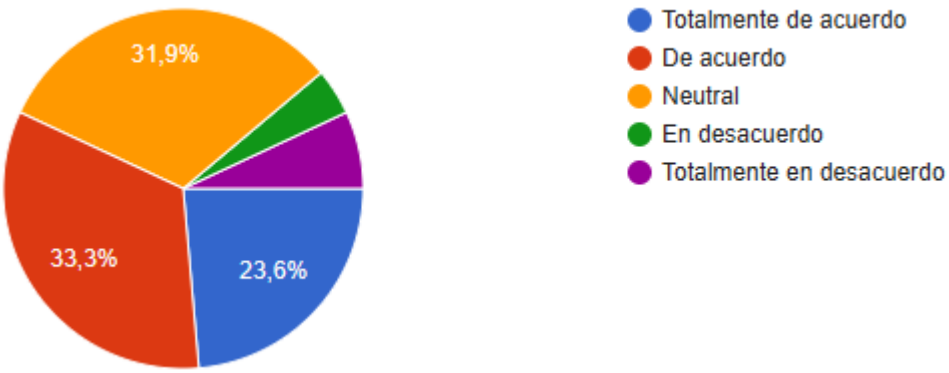


Figura 20. Datos de la pregunta 10.

Análisis e interpretación de resultados

De acuerdo con los resultados de la figura 20, existe un fuerte apoyo a la seguridad, incluso a costa de la restricción: el 23.6% está totalmente de acuerdo y el 33.3% está de acuerdo, sin embargo, un 31.9% se mantuvo neutral, y solo el 11.2% (En desacuerdo con un 4.2% y totalmente en desacuerdo con un 6.9%) se opuso a las restricciones. Según los datos recolectados se puede indicar que la propuesta de mitigar vulnerabilidades mediante políticas de restricción será efectiva y viable.

2.2.4 Procesamiento y análisis de datos

Estos resultados confirman la necesidad de priorizar la concienciación y formación dentro del plan de mitigación, utilizando el apoyo institucional como un factor clave de éxito.

La encuesta a estudiantes revela que la principal problemática radica en la inestabilidad y la desconfianza en la infraestructura técnica, según la pregunta 2 un abrumador 80.6% de los estudiantes reporta mal funcionamiento recurrente de los equipos, lo que es síntoma de vulnerabilidades no mitigadas en la configuración y defensa contra malware. Además, en la pregunta 6 el 58.4% de los estudiantes desconfía de la integridad y permanencia de sus archivos, señalando fallas en las políticas de backup.

Los estudiantes demuestran pragmatismo, ya que en la pregunta 10 el 56.9% acepta la implementación de mayores restricciones (navegación y descarga) a cambio de una red más segura. Esto valida la necesidad de que el proyecto se centre en la mejora técnica y operativa de la red y garantiza que las medidas estrictas propuestas serán bien recibidas por los usuarios.

El análisis de la Ficha de Observación confirma que las vulnerabilidades críticas de la infraestructura son tanto técnicas como físicas/operacionales. Se determinó la ausencia de medidas fundamentales de seguridad física, como conexiones eléctricas adecuadas y controles de acceso, lo que expone directamente los activos al riesgo de pérdida total o acceso no autorizado.

A nivel de configuración, la falta de software antivirus activo y actualizado y el descontrol en puertos USB demuestran que los equipos no se encuentran protegidos contra malware, lo que corrobora la alta tasa de mal funcionamiento y desconfianza reportada en las encuestas. La falta de evidencia de respaldos de datos y la ausencia de avisos de concienciación cierran el ciclo de vulnerabilidad, demostrando que la falta de procedimientos formales y la debilidad en los controles técnicos elementales son el principal foco de riesgos para la unidad educativa.

El análisis integral de los datos recopilados establece que la unidad educativa General Eloy Alfaro presenta un alto grado de vulnerabilidad de seguridad que afecta tanto a los activos tecnológicos como a la continuidad operativa. Permitiendo realizar un enfoque de solución con una propuesta clara y consistente en el siguiente capítulo.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de resultados

El presente capítulo se centrará en la ejecución de un diagnóstico técnico y sistemático de la infraestructura de red de la unidad educativa General Eloy Alfaro, El enfoque integral se orientará a analizar la postura de seguridad de los componentes de red. Mediante herramientas de escaneo y la aplicación de los CIS Controls, se proyectarán reportes de las vulnerabilidades detectadas. Este análisis permitirá la identificación precisa de las gestiones sospechosas o configuraciones inseguras. Finalmente, con base en los resultados visualizados y alineados con el Grupo de Implementación 1 (IG1) de los CIS Controls, se gestionará un diseño de remediación que implica obtener un detalle de mayor seguridad informática dentro del sistema de trabajo, protegiendo así al personal y los datos de la organización educativa.

3.2 Aplicación del marco de ciberseguridad de los CIS Controls

La implantación del marco de ciberseguridad de los CIS Controls se estructurará a través de un ciclo de vida continuo que asegura no solo la mitigación inicial de vulnerabilidades sino también la sostenibilidad del programa de seguridad. Este proceso se desglosa en las siguientes etapas clave:

3.2.1 Fase 1: Evaluación el estado de seguridad actual

Esta fase inicial requiere una evaluación exhaustiva de la postura de seguridad actual de la institución, con el objetivo de identificar las vulnerabilidades inherentes a la infraestructura de red.

a. Topología de red

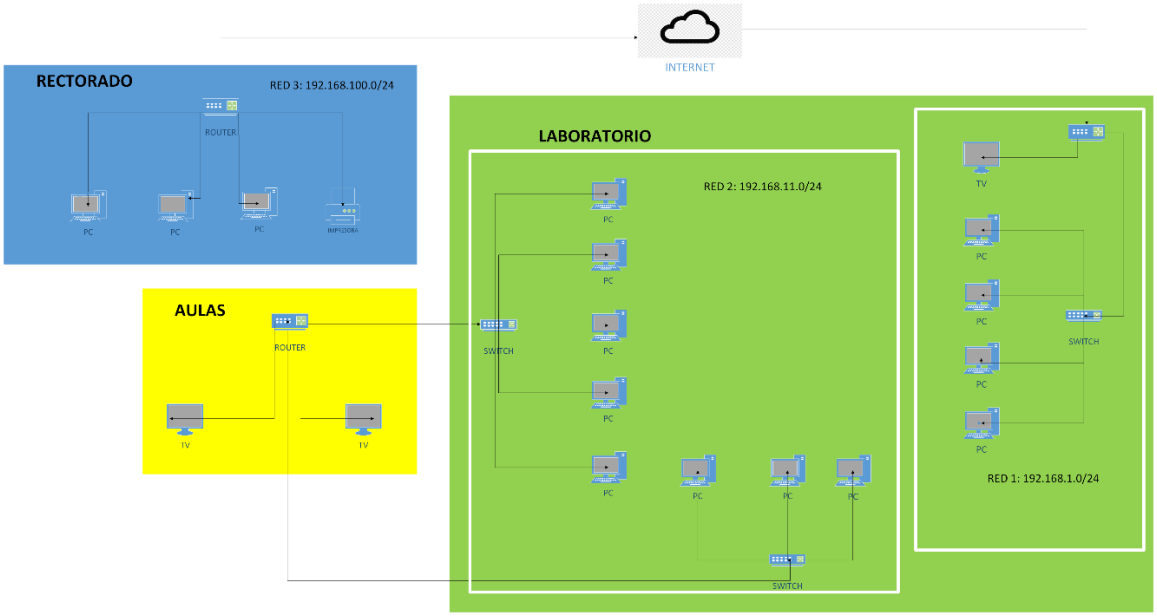


Figura 21. Topología de red de la unidad educativa General Eloy Alfaro.

La Figura 21, muestra la topología de la red de la unidad educativa General Eloy Alfaro la cual consta de 3 bloques fácilmente identificables:

- Laboratorio: Red 1 – 192.168.1.0/24

  Este bloque cuenta con 1 router, 1 switch, 1 televisor y 5 pc's.

- Laboratorio: Red 2 – 192.168.11.0/24

  Este bloque cuenta con 1 router, 2 switchs, 2 televisores y 8 pc's.

- Rectorado: Red 3 – 192.168.100.0/24

  Este bloque cuenta con 1 router, 1 impresora y 3 pc's.

b. Inventario de activos

Inventario y control de los activos empresariales (CIS Control 1)

Este control se enfoca en la gestión del inventario y control de activos empresariales, destacando la importancia de mantener un inventario actualizado de hardware para

mejorar la seguridad y la eficiencia en la gestión de activos Los activos empresariales de muestran en la Tabla 10.

Salvaguarda: Establecer y mantener un inventario detallado de activos empresariales.

Tabla 10. Activos empresariales de la unidad educativa General Eloy Alfaro

8	KIT GARRA
4	CABLE DE AUDIO
2	KIT EK 230
1	CIRCUITO EN SERIE
2	PISTOLAS DE SILICONA
1	PAR DE GAFAS DE PROTECCION
1	DRON
1	KIT HERRAMIENTAS IMPRESORA
2	TALADROS DE MANO
1	KIT BOXING BOT ABIERTO
1	CONTROL
1	SMALL SIX SIN BRAZO
1	CARRITO
2	CPU COER I5
9	CPU CORE 2 DUO
4	CPU VANTEC
12	MOUSE
14	TECLADOS
15	PANTALLAS
2	TELEVISORES LG

Salvaguarda: Utilice una herramienta de descubrimiento activo.

Mediante la herramienta Advanced IP Scanner se realizó un análisis de dispositivos que se encuentran conectados a la red de la institución.

Laboratorio – Red 1

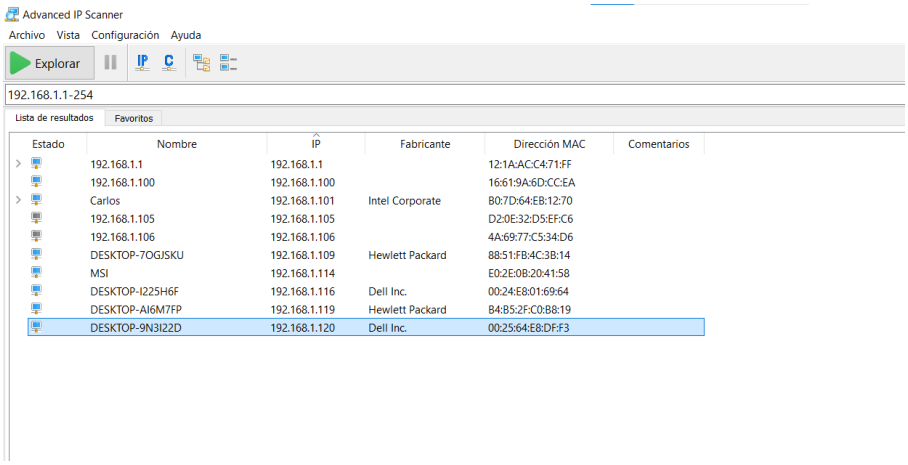


Figura 22. Descubrimiento de host's en laboratorio – red 1.

Laboratorio – Red 2

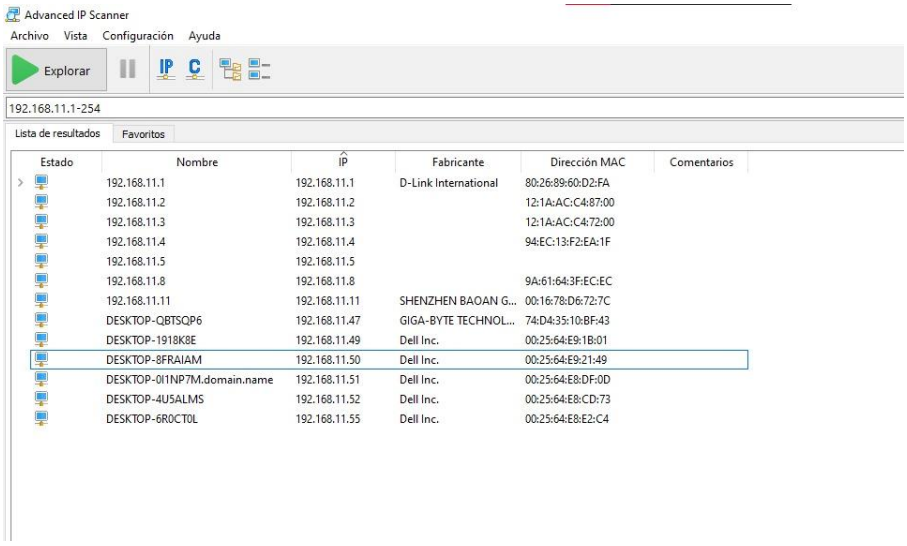


Figura 23. Descubrimiento de host's en laboratorio – red 2.

Rectorado – Red 3

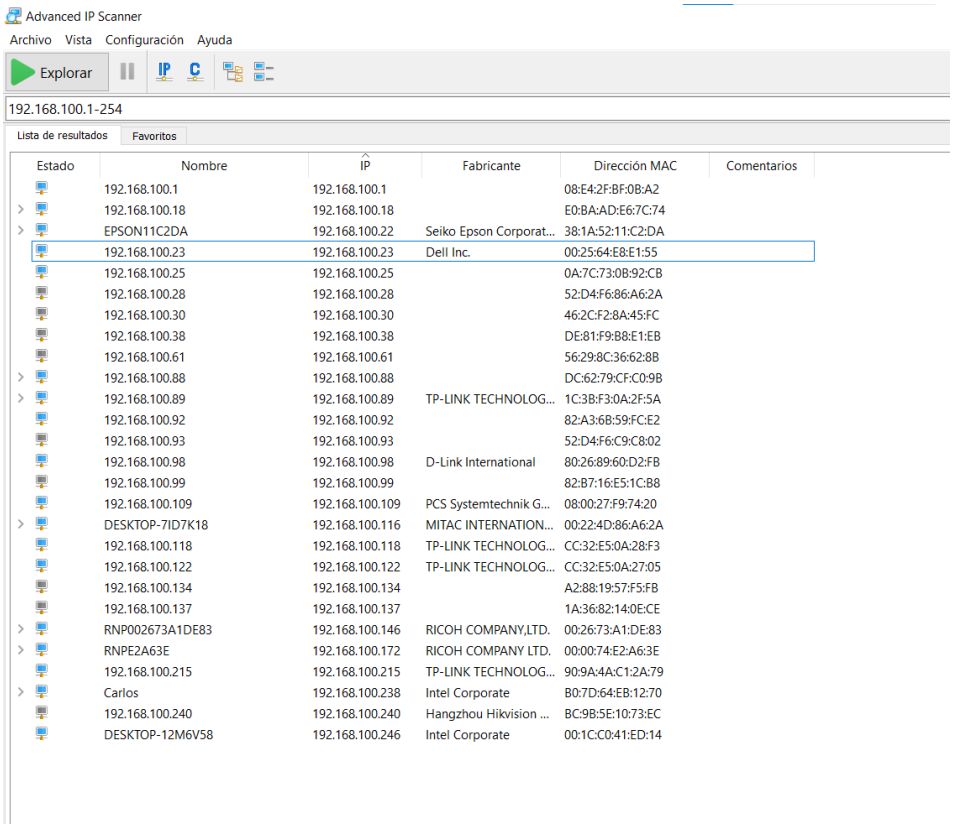


Figura 24. Descubrimiento de host’s en rectorado – red 3.

La herramienta resulta muy útil ya que por medio de esta se puede identificar los dispositivos de la institución y los dispositivos de usuarios finales, la Tabla muestra los activos de la institución con el potencial de almacenar o procesar datos.

Tabla 11. Inventario y control de activos empresariales.

Número	Dirección IP	Dirección MAC	Departamento
1	192.168.1.X	88:51:FB:4C:3B:14	Laboratorio
2	192.168.1.X	B4:B5:2F:C0:B8:19	Laboratorio
3	192.168.1.X	00:24:E8:01:69:64	Laboratorio
4	192.168.1.X	00:25:64:E8:DF:F3	Laboratorio
5	192.168.11.X	00:25:64:E8:E1:BF	Laboratorio
6	192.168.11.X	00:25:64:E9:1B:01	Laboratorio
7	192.168.11.X	00:25:64:E8:DF:0D	Laboratorio
8	192.168.11.X	00:25:64:E9:21:49	Laboratorio
9	192.168.11.X	74:D4:35:10:BF:43	Laboratorio
10	192.168.11.X	74:D4:35:16:A1:19	Laboratorio
11	192.168.11.X	00:25:64:E8:CD:73	Laboratorio
12	192.168.11.X	00:25:64:E8:E2:C4	Laboratorio

13	192.168.100.X	00:22:4D:86:A6:2A	Rectorado
14	192.168.100.X	00:1C:C0:41:ED:14	Rectorado
15	192.168.100.X	00:25:64:E8:E1:55	Rectorado

Inventario y control de activos de software (CIS Control 2)

Este control se enfoca en la gestión del software instalado dentro de la red, tiene como objetivo asegurarse que el únicamente el software autorizado se ejecute en los sistemas, identificando y permitiendo eliminar de manera proactiva cualquier software no permitido.

Salvaguarda: Elaborar y mantener actualizado el inventario de software.

Mediante la herramienta WinAudit se generó un inventario del software instalado en cada dispositivo de los activos de la empresa, los resultados se observan en la Tabla 12.

En el Anexo 3, se adjunta el reporte generado por la herramienta WinAudit.

Tabla 12. Inventario de software instalado.

Núm.	Nombre	Fabricante	Versión	Fecha de instalación	Autorizado
1	AnyDesk	AnyDesk Software GmbH	9.0.9	Desconocido	SI
2	Arduino IDE 2.3.6	Arduino SA	2.3.6	Desconocido	SI
3	Google Chrome	Google LLC	141.0.7390.123	20250630	SI
4	Microsoft Edge	Microsoft Corporation	142.0.3595.53	20251105	SI
5	Microsoft Office LTSC Professional Plus 2021 - es-es	Microsoft Corporation	16.0.14334.20344	Desconocido	SI

6	Microsoft OneDrive	Microsoft Corporation	25.199.1012.0002	Desconocido	SI
7	Microsoft Project Profesional 2021 - es-es	Microsoft Corporation	16.0.14334.20344	Desconocido	SI
8	Microsoft Visio LTSC Professional 2021 - es-es	Microsoft Corporation	16.0.14334.20344	Desconocido	SI
9	Office 16 Click-to-Run Extensibility Component	Microsoft Corporation	16.0.14334.20344	20251021	SI
10	Office 16 Click-to-Run Licensing Component	Microsoft Corporation	16.0.14334.20344	20251021	SI
11	Office 16 Click-to-Run Localization Component	Microsoft Corporation	16.0.14334.20344	20251021	SI
12	PSeInt versión 20250314	Pablo Novara	20250314	20250925	SI
13	Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	6.0.1.7548	Desconocido	SI
14	Roblox Player for USUARIO	Roblox Corporation	Desconocido	2025-11-11	NO
15	Scratch 3 Link and Desktop 1.0.17	EduSense and Dabida	1.0.17	20251027	SI
16	VLC media player	VideoLAN	3.0.21	Desconocido	SI
17	WebView2 Runtime de	Microsoft Corporation	142.0.3595.53	20251107	SI

	Microsoft Edge				
18	WinRAR 7.12 (64-bit)	win.rar GmbH	7.12.0	Desconocido	SI
19	Zoom Workplace (64-bit)	Zoom	6.5.7509	20250630	SI

Salvaguarda: Tratamiento de software no autorizado.

El software que no está autorizado se debe eliminar de los dispositivos de la institución ya que estas aplicaciones representan una expansión no gestionada de la superficie de ataque, a menudo estos programas carecen de soporte y/o parches de seguridad, introduciendo una vulnerabilidad a la red de la institución, además de que puede estar empaquetado con malware comprometiendo la integridad, confidencialidad y disponibilidad de los datos.

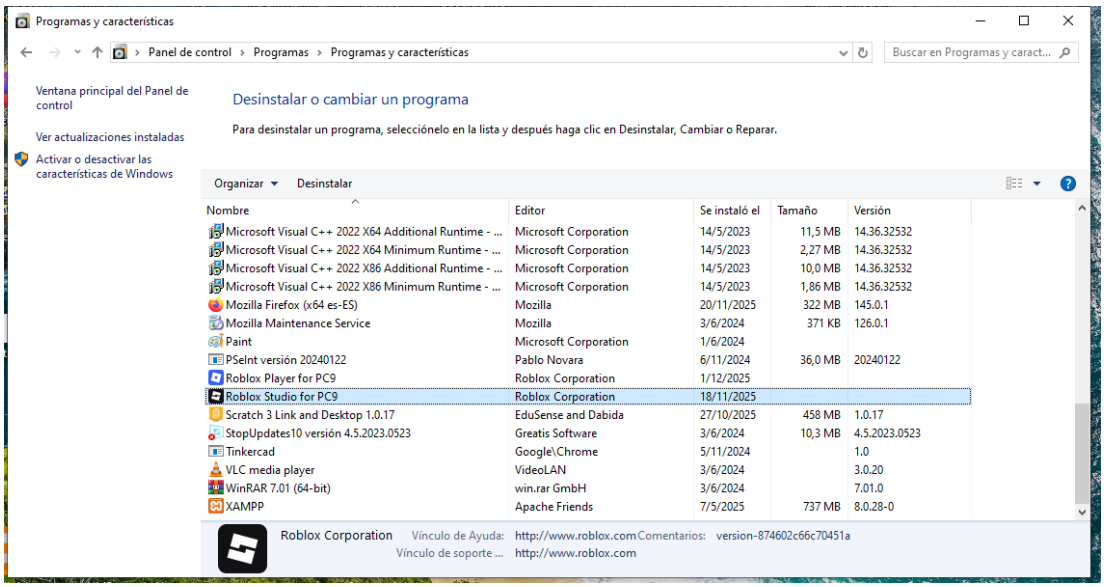


Figura 25. Desinstalación de software no autorizado.

c. Evaluación de vulnerabilidades

Mediante la herramienta Nessus se realizó el escaneo de los dispositivos de la institución para detectar las vulnerabilidades presentes, dando como resultado los siguientes resultados.

UEGEA_PC01

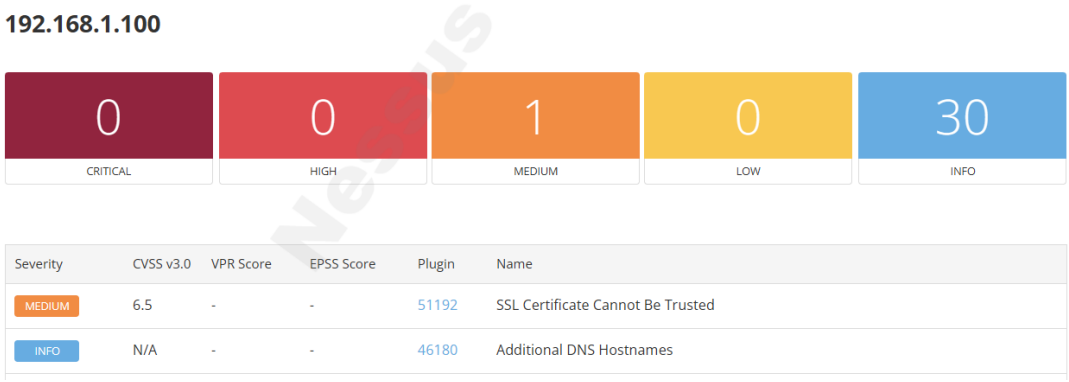


Figura 26. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC01.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 31 hallazgos (1 medio y 30 informativos). Tal como se muestra en la Figura 26.

Vulnerabilidad media

- Nombre: “SSL Certificate Cannot Be Trusted”.
- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSS v3.0 de 6.5.
- Esto indica un problema con la configuración del certificado de seguridad en el servicio que corre en esa IP, lo cual compromete la confianza en las comunicaciones cifradas.

UEGEA_PC02

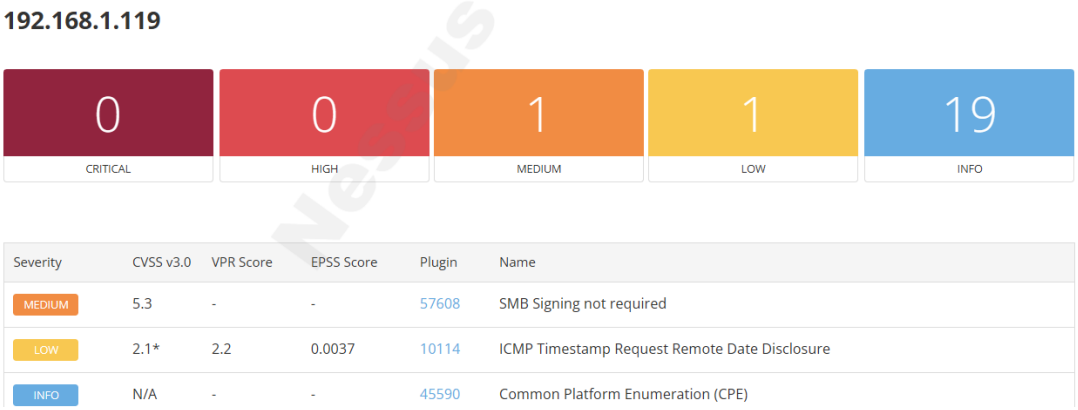


Figura 27. Resultados del escaneo de vulnerabilidades del pc UEGEA_PC02.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 27.

Vulnerabilidad Media

- Nombre: “SMB Signing not required”.
- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSSv3.0 de 5.3.
- La falta de firma de los paquetes SMB, expone el tráfico a ataques de Man-in-the Middle (MITM), permitiendo que un atacante intercepte y modifique datos o credenciales, Esto compromete la integridad y autenticidad de las comunicaciones internas.

Vulnerabilidad Baja

- Nombre: “ICMP Timestamp Request Remote Date Disclosure”.
- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSSv3.0 de 2.1.

- Esta vulnerabilidad divulga información de fecha y hora a través del protocolo ICMP. Aunque es de baja severidad, la información puede ser utilizada por atacantes como parte de la fase de reconocimiento para coordinar ataques o explotar vulnerabilidades basadas en el tiempo.

UEGEA_PC03

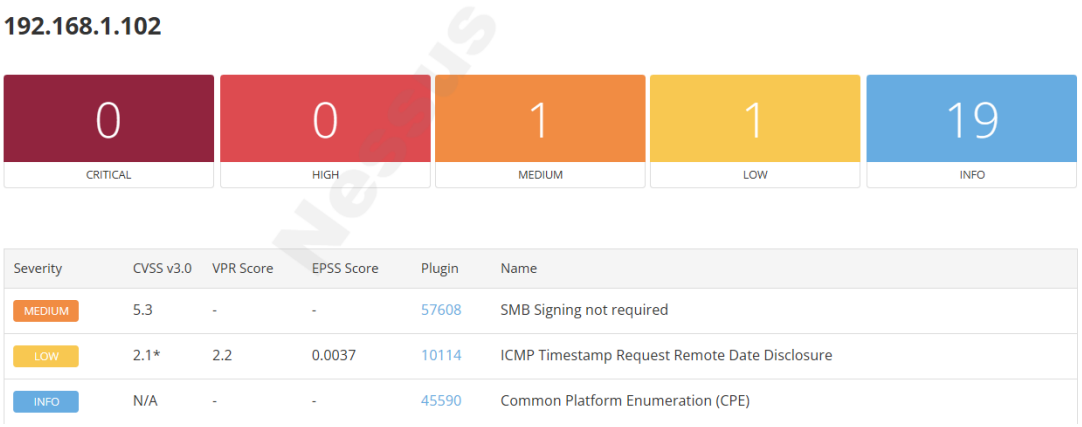


Figura 28. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC03.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 28.

UEGEA_PC04

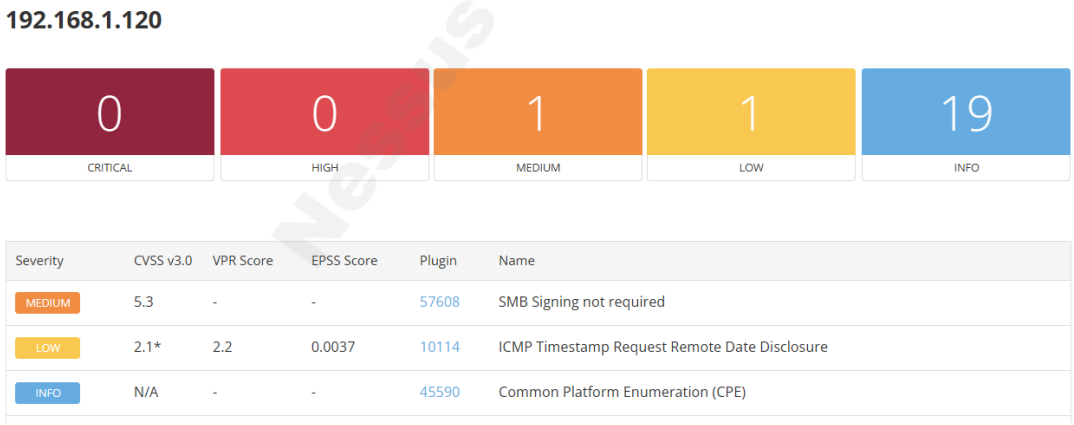


Figura 29. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC04.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 29.

UEGEA_PC05

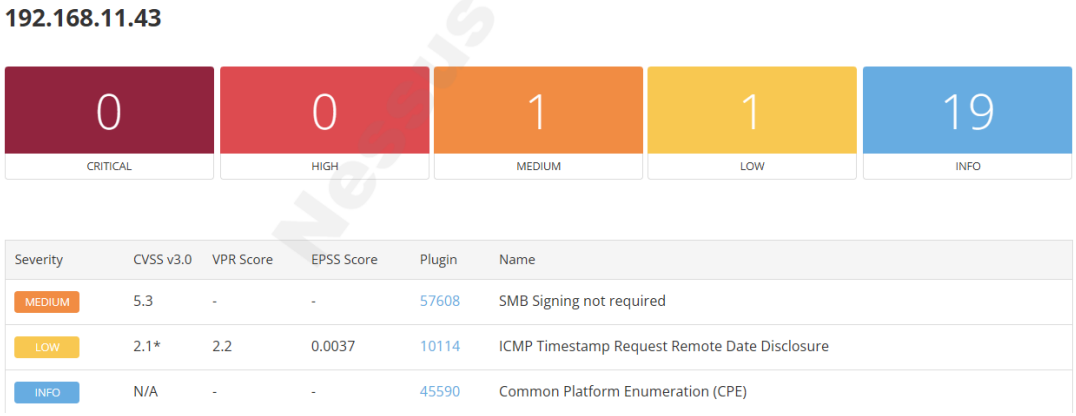


Figura 30. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC05.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 30.

UEGEA_PC06

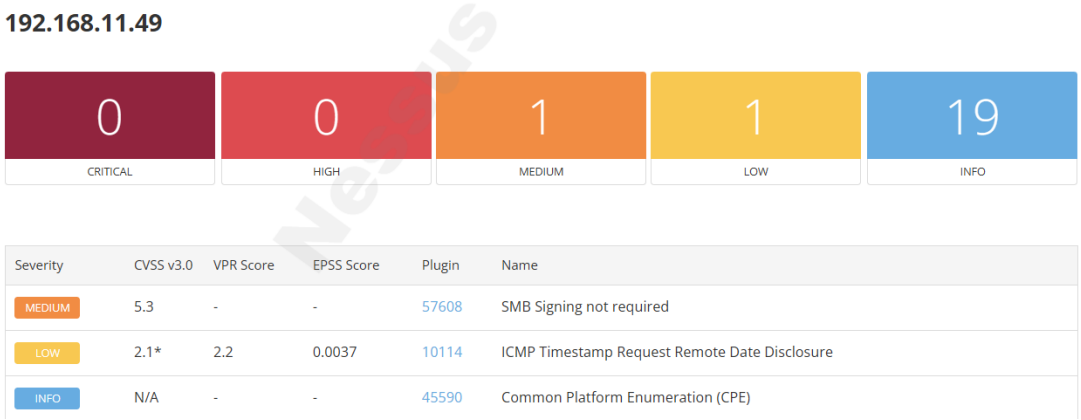


Figura 31. Resultados del escaneo de vulnerabilidades del pc UEGEA_PC06.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 31.

UEGEA_PC07

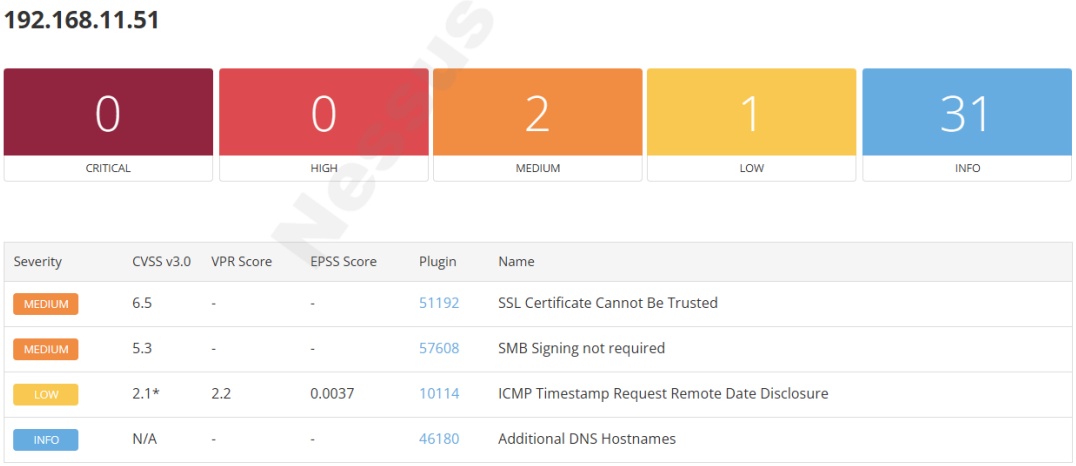


Figura 32. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC07.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 34 hallazgos (2 medios, 1 bajo y 31 informativos). Tal como se muestra en la Figura 32.

Vulnerabilidad media

- Nombre: “SSL Certificate Cannot Be Trusted”.
- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSS v3.0 de 6.5.
- Esto indica un problema con la configuración del certificado de seguridad en el servicio que corre en esa IP, lo cual compromete la confianza en las comunicaciones cifradas.

Vulnerabilidad media

- Nombre: “SMB Signing not required”.

- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSSv3.0 de 5.3.

- La falta de firma de los paquetes SMB, expone el tráfico a ataques de Man-in-the Middle (MITM), permitiendo que un atacante intercepte y modifique datos o credenciales, Esto compromete la integridad y autenticidad de las comunicaciones internas.

Vulnerabilidad Baja

- Nombre: “ICMP Timestamp Request Remote Date Disclosure”.

- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSSv3.0 de 2.1.

- Esta vulnerabilidad divulga información de fecha y hora a través del protocolo ICMP. Aunque es de baja severidad, la información puede ser utilizada por atacantes como parte de la fase de reconocimiento para coordinar ataques o explotar vulnerabilidades basadas en el tiempo.

UEGEA_PC08

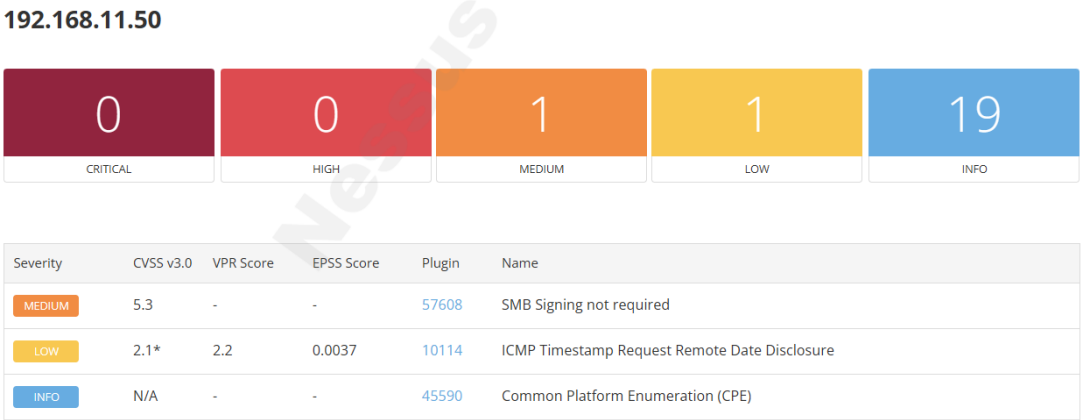


Figura 33. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC08.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 33.

UEGEA_PC09

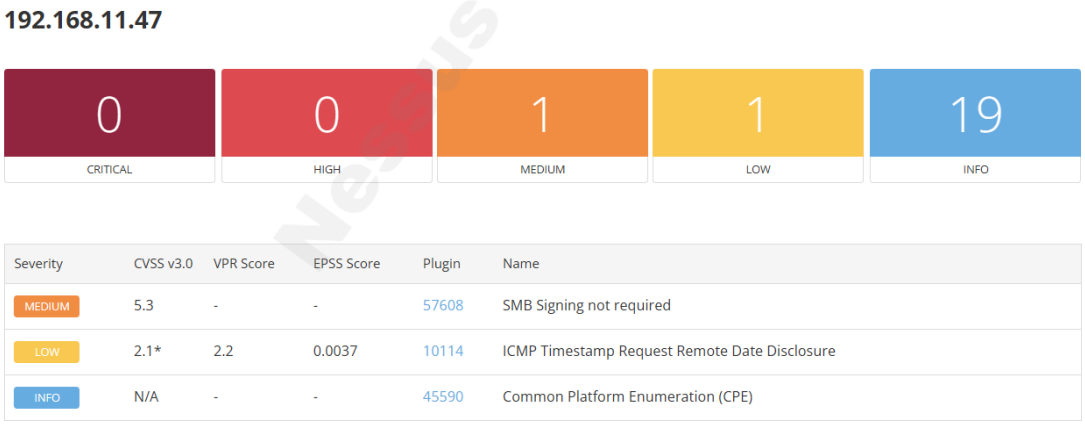


Figura 34. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC09.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 34.

UEGEA_PC10

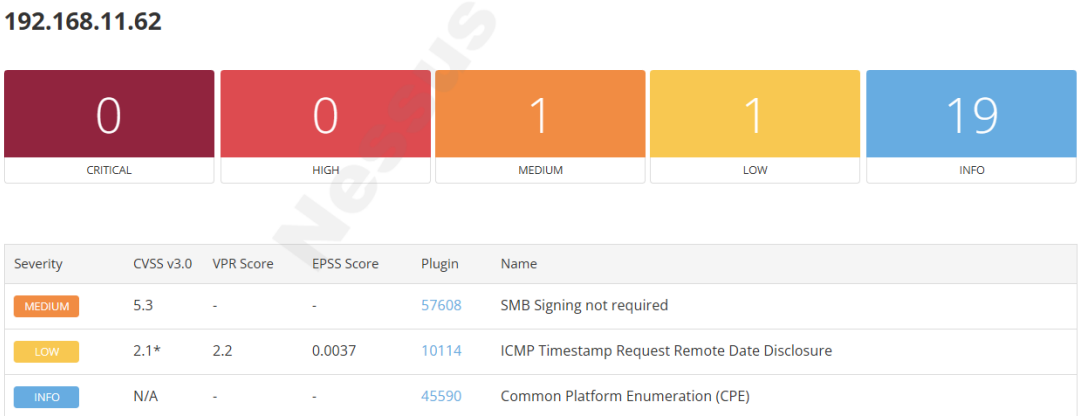


Figura 35. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC10.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 35.

UEGEA_PC11

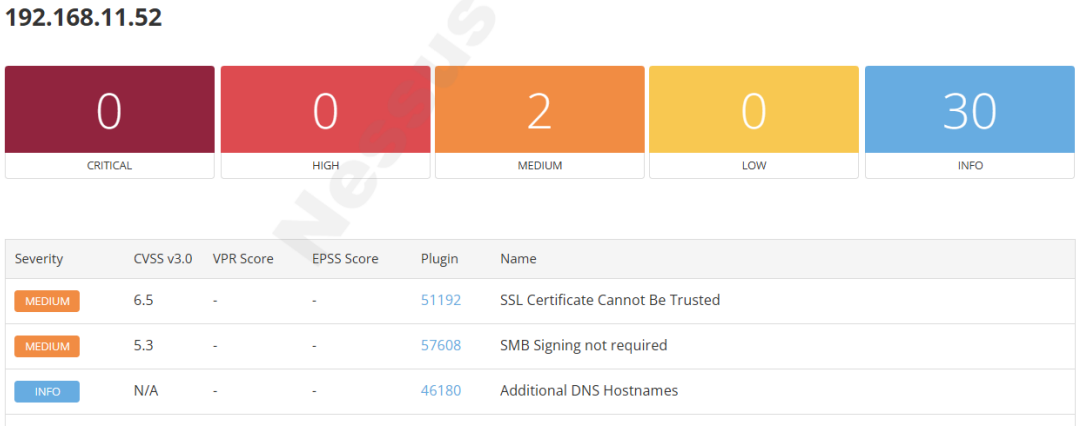


Figura 36. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC11.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 32 hallazgos (2 medios y 30 informativos). Tal como se muestra en la Figura 36.

Vulnerabilidad media

- Nombre: “SSL Certificate Cannot Be Trusted”.
- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSS v3.0 de 6.5.
- Esto indica un problema con la configuración del certificado de seguridad en el servicio que corre en esa IP, lo cual compromete la confianza en las comunicaciones cifradas.

Vulnerabilidad media

- Nombre: “SMB Signing not required”.
- Evaluación de riesgo: Esta vulnerabilidad tiene una puntuación CVSSv3.0 de 5.3.
- La falta de firma de los paquetes SMB, expone el tráfico a ataques de Man-in-the Middle (MITM), permitiendo que un atacante intercepte y modifique datos

o credenciales, Esto compromete la integridad y autenticidad de las comunicaciones internas.

UEGEA_PC12

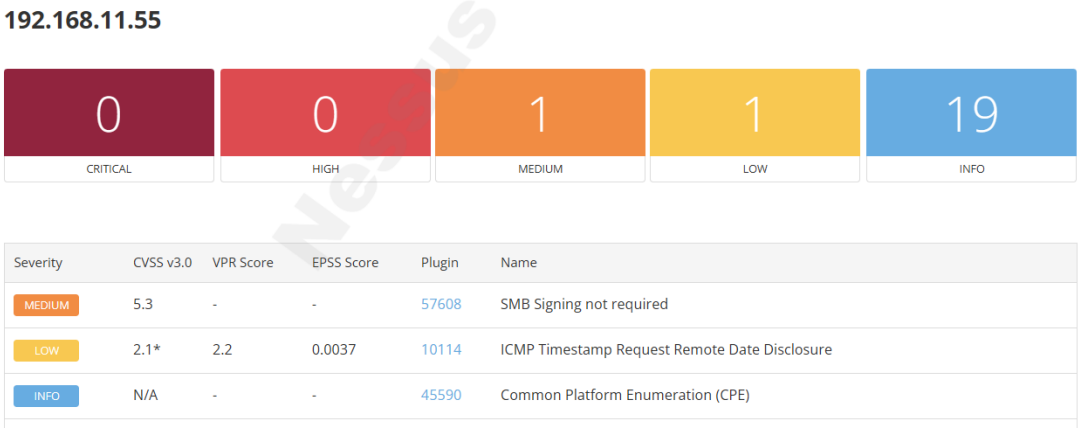


Figura 37. Resultado del escaneo de vulnerabilidades del pc UEGEA_PC12.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 37.

UEGEA_Rector

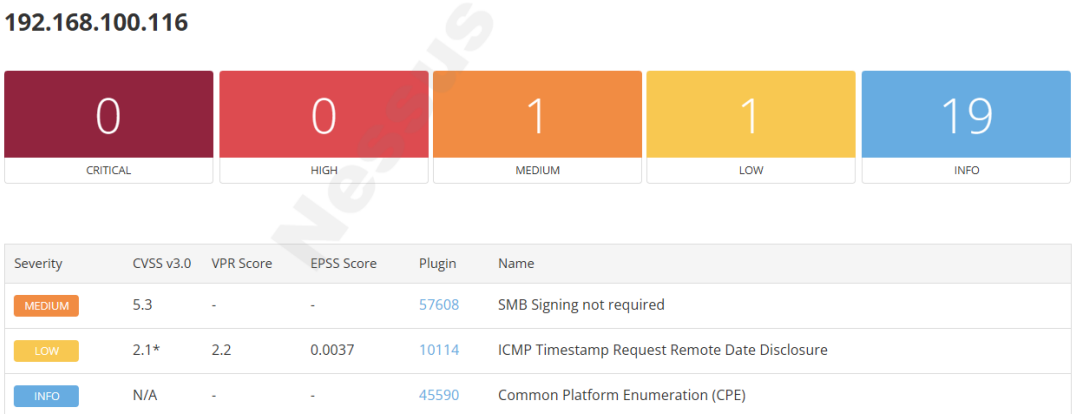


Figura 38. Resultado del escaneo de vulnerabilidades del pc UEGEA_Rector.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 38.

UEGEA_Vicerrector

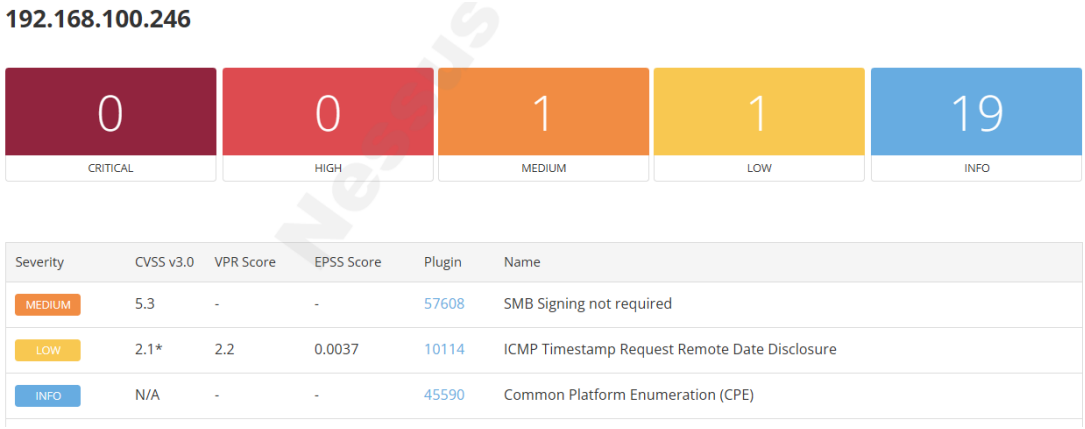


Figura 39. Resultado del escaneo de vulnerabilidades del pc UEGEA_Vicerrector.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 39.

UEGEA_Secretaria

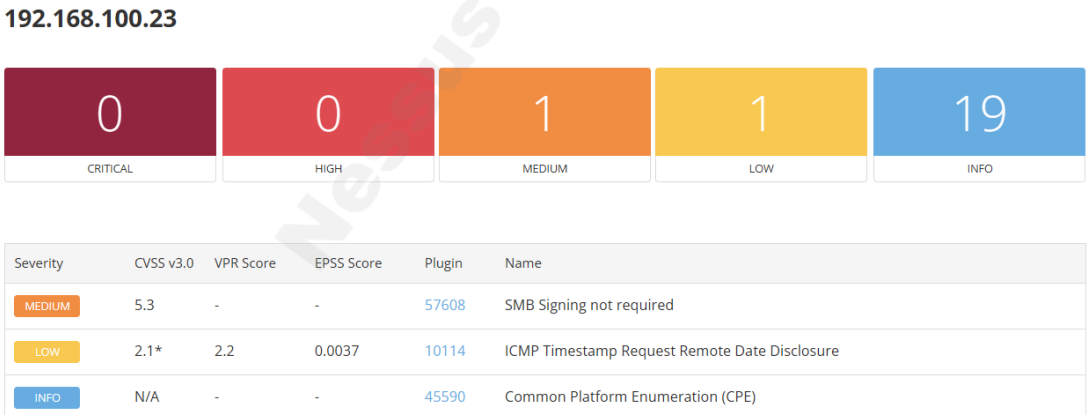


Figura 40. Resultado del escaneo de vulnerabilidades del pc UEGEA_Secretaria.

El escaneo de vulnerabilidades sobre la ip muestra como resultado 21 hallazgos (1 medio, 1 bajo y 19 informativos). Tal como se muestra en la Figura 40.

En la Tabla 13, se muestra un resumen de las vulnerabilidades encontradas.

Tabla 13. Resumen de vulnerabilidades encontradas.

Dispositivo	Crítica	Alta	Media	Baja	Total
UEGEA_PC01	0	0	1	0	1
UEGEA_PC02	0	0	1	1	2
UEGEA_PC03	0	0	1	1	2
UEGEA_PC04	0	0	1	1	2
UEGEA_PC05	0	0	1	1	2
UEGEA_PC06	0	0	1	1	2
UEGEA_PC07	0	0	2	1	3
UEGEA_PC08	0	0	1	1	2
UEGEA_PC09	0	0	1	1	2
UEGEA_PC10	0	0	1	1	2
UEGEA_PC11	0	0	2	0	2
UEGEA_PC12	0	0	1	1	2
UEGEA_RECTOR	0	0	1	1	2
UEGEA_VICERRECTOR	0	0	1	1	2
UEGEA_SECRETARIA	0	0	1	1	2

El diagnóstico de vulnerabilidades en 15 dispositivos de la unidad educativa General Eloy Alfaro, reveló que no se detectaron vulnerabilidades de nivel crítico ni Alto en la muestra analizada, lo que sugiere que las amenazas de mayor impacto están mitigadas o ausentes. Sin embargo, la mayoría de los equipos presentan 1 vulnerabilidad de nivel medio y 1 vulnerabilidad de nivel bajo, indicando la existencia de fallos de configuración o de higiene cibernética que deben ser atendidos. El número total de vulnerabilidades por dispositivo oscila entre dos y tres, destacando el equipo UEGEA_PC07 que consta con tres vulnerabilidades reportadas.

d. Análisis de riesgos

El Análisis de Riesgos constituye la piedra angular metodológica para la justificación de la propuesta de seguridad, conectando el diagnóstico técnico con los objetivos de mitigación. Este proceso permite identificar y catalogar las amenazas dirigidas a los activos críticos de la institución, evaluar las vulnerabilidades encontradas y determinar el nivel de riesgo inherente. La valoración se fundamenta en la combinación de dos factores clave: la probabilidad de ocurrencia de un evento adverso y la severidad del impacto que dicho evento tendría sobre los principios fundamentales de la información: confidencialidad, integridad y disponibilidad.

Para este estudio, se optó por una metodología de análisis cualitativo, estableciendo una escala tripartita (Baja, Media y Alta) tanto para la probabilidad como para el impacto.

El riesgo final se calculó como el producto de estas variables y se clasificó en tres niveles, que definen la urgencia de la remediación:

Riesgo Bajo (1-2): Nivel residual, considerado tolerable sin la necesidad de invertir en medidas de control inmediatas.

Riesgo Medio (3-4): Requiere la planificación de controles y el establecimiento de un monitoreo constante.

Riesgo Alto (6-9): Exige la implementación de medidas de mitigación y tratamiento inmediatas y prioritarias.

Tabla 14. Evaluación de riesgos.

Activo	**Amenaza**	**Vulnerabilidad**	**Impacto (1-3)**	**Probabilidad (1-3)**	**Nivel de riesgo**	**Clasificación**
Estaciones de laboratorio	Malware o exfiltración de información	Puertos usb libres, dispositivos sin contraseñas	3	3	9	Alto
Puntos de acceso / red Wi-Fi	Robo de contraseñas	Contraseñas débiles	3	2	6	Alto
Personal docente/estudiantil	Ataque de phishing	Ausencia de concinetización	3	3	9	Alto
Innfraestructura eléctrica	Perdida de información, fallo de hardware	Falta de conexiones adecuadas	3	1	3	Medio

La Tabla 13 muestra la evaluación de riesgos de la unidad educativa General Eloy Alfaro, basado en un modelo cualitativo simple, utilizado para la implantación práctica de la ISO/IEC 27001. el cálculo del nivel de riesgo se realiza multiplicando el impacto por la probabilidad.

3.2.2 Fase 2: Priorización de los controles según las necesidades

Una vez evaluada la condición actual de la institución en términos de seguridad informática, se procedió con la selección de los controles que permitan mitigar directamente los riesgos y mejoren la seguridad general de la institución. Los controles seleccionados se muestran en la Tabla 14.

Tabla 15. Controles seleccionados.

Control	**Título del Control**
CIS Control 1	Inventario y control de los activos empresariales.
CIS Control 2	Inventario y control de activos de software.
CIS Control 4	Configuración segura de activos y software empresarial.
CIS Control 5	Administración de cuentas.
CIS Control 6	Gestión de control de accesos.
CIS Control 7	Gestión continua de vulnerabilidades.
CIS Control 10	Defensas contra malware.
CIS Control 11	Recuperación de datos.
CIS Control 14	Concientización en seguridad y formación de habilidades.

3.2.3 Fase 3: Planificación y Preparación

Dada la naturaleza educativa de la institución y las restricciones presupuestarias y de personal de TI, la estrategia de mitigación se fundamenta en la implementación priorizada del Grupo de Implementación 1 (IG1) de los CIS Controls.

La fase de planificación y preparación se ha ejecutado mediante la definición de objetivos claros, enfocados en la reducción de los riesgos a un nivel tolerable, con un cronograma estructurado en fases de implementación manejables. En esta etapa se detalló la asignación de recursos, priorizando la utilización de soluciones de bajo costo y reasignando el tiempo del personal existente, siendo el encargado de TI de la institución la figura principal responsable de la ejecución técnica de las tareas.

La Tabla 16, muestra el plan de acción que permitió llevar a cabo la investigación, acompañada de las observaciones pertinentes para la gestión continua de seguridad cibernética.

Tabla 16. Cronograma o plan de acción

Num.	Control	Fecha inicio	Fecha fin	Responsable	Observación
CIS Control 1	Inventario y control de los activos empresariales.	13/10/2025	17/10/2025	Encargado de TI.	Se recomienda actualizar el inventario cada vez que un activo ingresa.
CIS Control 2	Inventario y control de activos de software.	20/11/2025	24/11/2025	Encargado de TI.	Se recomienda actualizar el inventario cada vez software es permitido.
CIS Control 4	Configuración segura de activos y software empresarial.	27/11/2025	31/11/2025	Encargado de TI.	Se recomienda actualizar la documentación anualmente.
CIS Control 5	Administración de cuentas.	03/11/2025	07/11/2025	Encargado de TI.	Se recomienda validar las cuentas de manera recurrente.
CIS Control 6	Gestión de control de accesos.	03/11/2025	07/11/2025	Encargado de TI.	Se recomida conceder permisos cada vez que una cuanta es creada.
CIS Control 7	Gestión continua de vulnerabilidades.	10/11/2025	21/11/2025	Encargado de TI.	Se recomienda realizar un escaneo de vulnerabilidades cada mes.
CIS Control 10	Defensas contra malware.	17/11/2025	21/11/2025	Encargado de TI.	
CIS Control 11	Recuperación de datos.	24/11/2025	28/11/2025	Encargado de TI.	Se recomienda realizar copias de seguridad semanalmente
CIS Control 14	Concientización en seguridad y formación de habilidades.	01/12/2025	05/12/2025	Encargado de TI.	Se recomienda realizar charlas de concientización cada año

3.2.4 Fase 4: Implementación

La fase de implementación se centró en la ejecución técnica de las salvaguardas de los controles seleccionados para el tratamiento de los riesgos detectados, de forma simultánea, se ejecutaron controles dirigidos al factor humano. Este enfoque garantiza una postura más robusta y gestionable en la institución.

a. Configuración segura de activos y software empresarial (CIS Control 4)

Salvaguarda: Configurar el bloqueo automático de sesiones en activos empresariales.

Se configuró el bloqueo automático de sesiones en los dispositivos de la institución después de un periodo de inactividad, para los dispositivos con propósito general, el periodo no debe exceder los 15 minutos, mientras que para los dispositivos móviles y de usuario final este periodo no debe exceder los 2 minutos.

Salvaguarda: Implementar y administrar un firewall en servidores.

La unidad educativa no cuanta con servidores, sin embargo, el uso de firewall conlleva a mejorar la postura de seguridad de los dispositivos, por tal motivo se revisó que el firewall de windows defender se encuentre activo en todos los activos de la institución.

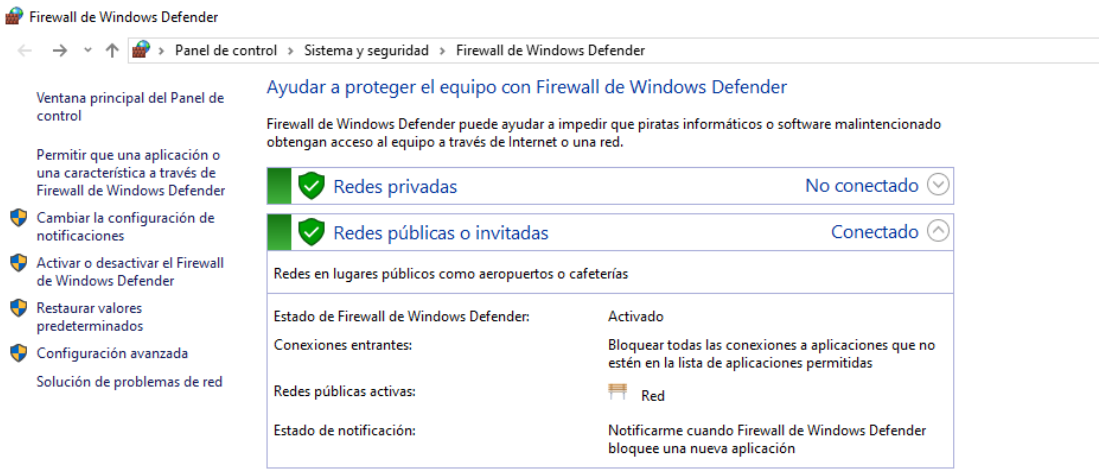


Figura 41. Activación de firewall de windows defender.

b. Administración de cuentas (CIS Control 5)

Salvaguarda: Utilice contraseñas únicas.

La implantación incluye la como mínimo una contraseña de 8 caracteres para cuentas que no utilicen autenticación multifactor (MFA) y 15 para cuentas que no lo utilicen.

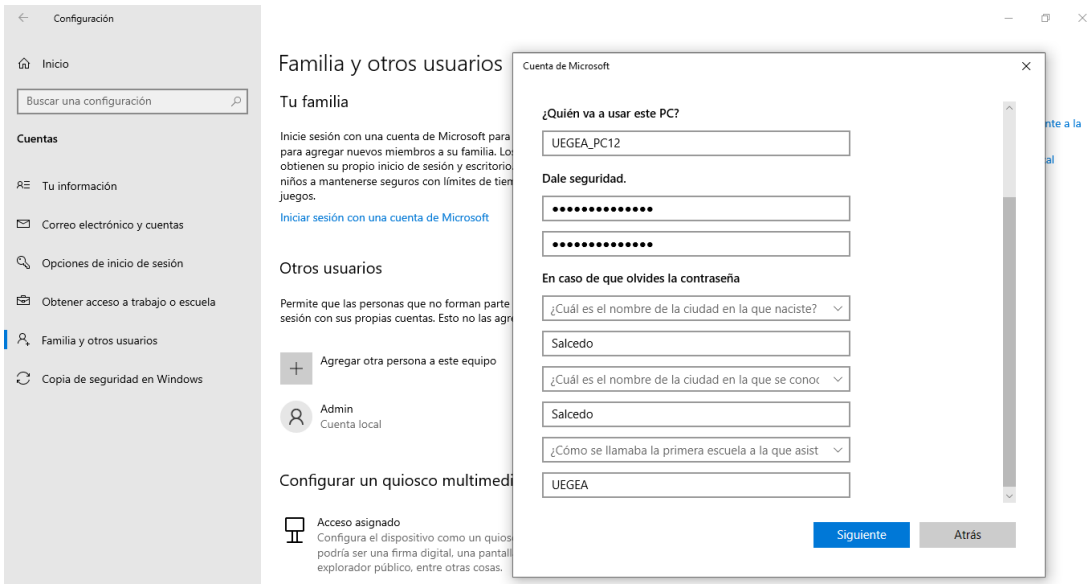


Figura 42. Configuración de contraseña en dispositivos de la institución.

c. Gestión de control de accesos (CIS Control 6)

Este control permite la otorgar y revocar privilegios de acceso para cuentas de usuario, administrador y servicio para activos empresariales.

Salvaguarda: Establecer y seguir un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de usuario

Se implementó un modelo de control de acceso basado en perfiles estándar, el cual automatiza la seguridad mediante la creación de dos cuentas locales fijas: una de Administrador, restringida al personal técnico para el mantenimiento del activo, y una de PC (Usuario Estándar) para el uso compartido de estudiantes y docentes. La implementación se asegura mediante una configuración maestra que garantiza el

principio de "menor privilegio", permitiendo que cualquier nueva contratación o cambio de rol se gestione otorgando únicamente las credenciales del perfil operativo, evitando así que usuarios no autorizados realicen cambios críticos en el sistema y asegurando una respuesta ágil y uniforme en todas las estaciones de trabajo.

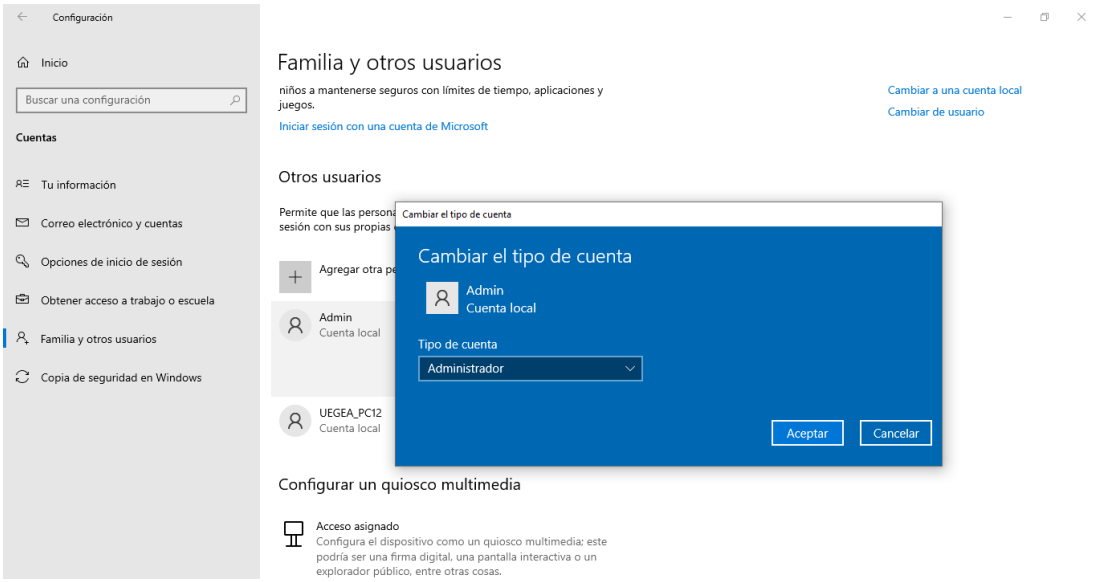


Figura 43. Otorgación de permisos de administrador y usuario a cuentas de los activos empresariales.

d. Gestión continua de vulnerabilidades (CIS Control 7)

Salvaguarda: Establecer y mantener un proceso de gestión de vulnerabilidades

Se estableció una periodicidad clara para la revisión técnica de los activos asegurando que los hallazgos críticos y medios (como los relacionados con la configuración) sean continuamente identificados y contrastados con la documentación del programa de seguridad. Revisar y actualizar esta documentación anualmente, o cuando ocurran cambios importantes en la infraestructura, es esencial para garantizar que el estado de la red se mantenga siempre dentro de un nivel de riesgo aceptable.

Salvaguarda: Establecer y mantener un proceso de remediación

La implementación de esta salvaguarda implica utilizar las herramientas instaladas para mantener una estrategia de remediación continua y basada en riesgos. La clave es

asegurar que las acciones correctivas, se lleven a cabo de manera efectiva, enfocándose siempre en los riesgos de mayor criticidad.

Salvaguarda: Remediar las vulnerabilidades detectadas

Después del análisis de vulnerabilidades se procedió a su respectiva remediación.

Vulnerabilidad: SSL Certificate Cannot Be Trusted

Para mitigar esta vulnerabilidad se deben seguir los siguientes pasos:

Identifica el sitio que da problemas, clic en detalles del certificado.

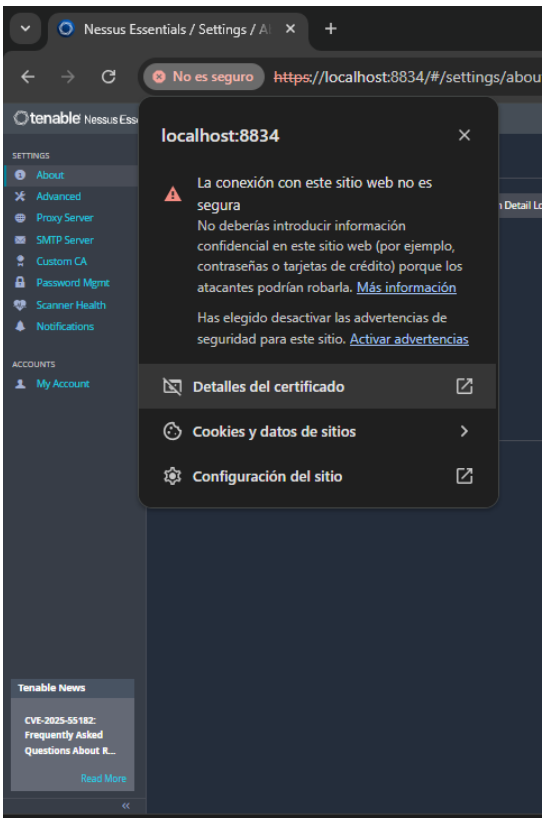


Figura 44. Identificación del servicio de la vulnerabilidad encontrada.

Selecciona la pestaña detalles y exporta el certificado.

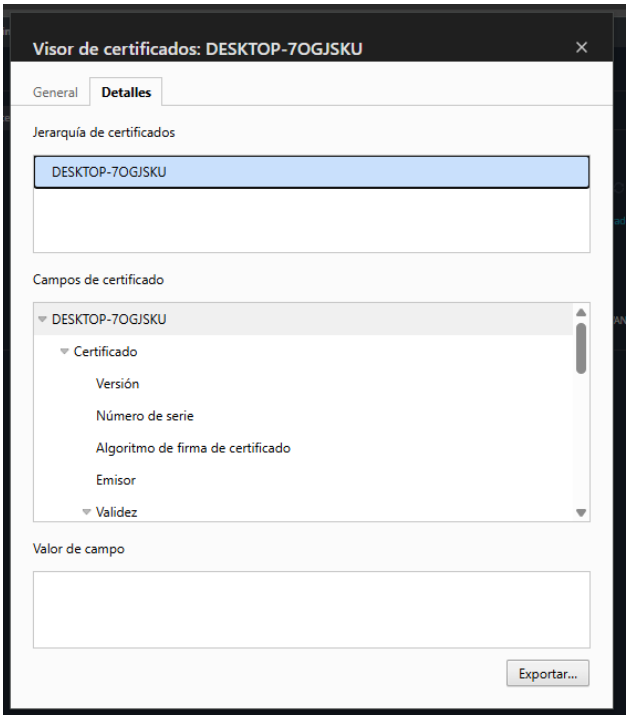


Figura 45. Exportación del certificado.

Selecciona la ruta de descarga y guarda el certificado.

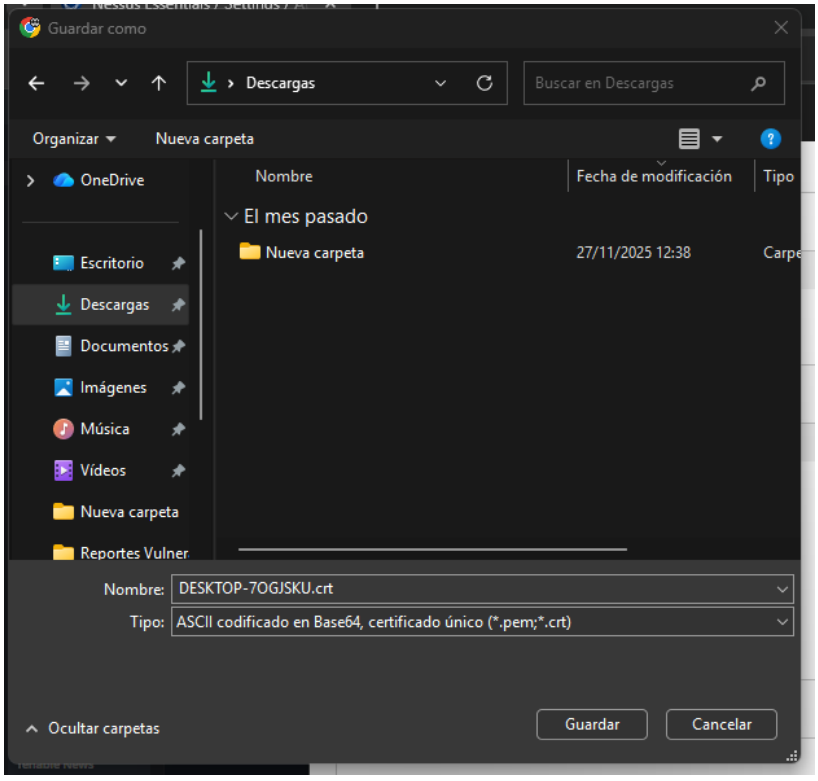


Figura 46. Selección de la ruta de descarga del certificado.

Con ayuda de un editor de texto y el bloc de notas abre el certificado y copia el contenido del mismo.

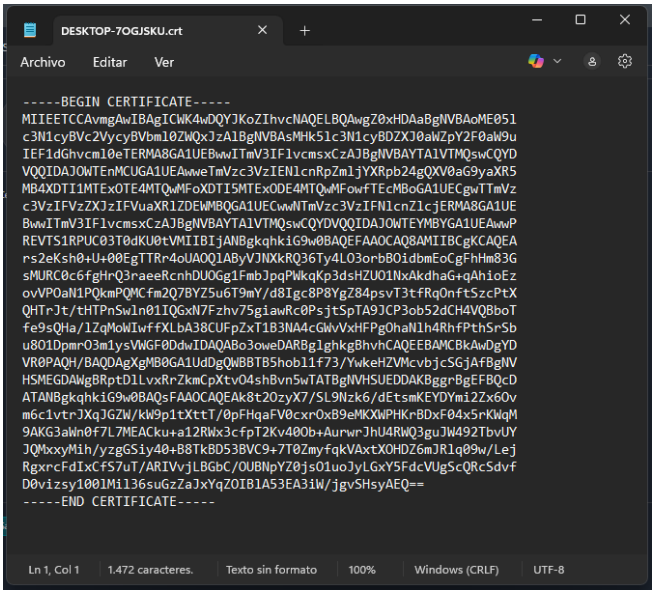


Figura 47. Contenido del certificado.

En la interfaz de nessus, en la parte de ajustes, selecciona la opción “Custom CA”, pega el contenido del certificado y guarda los cambios.

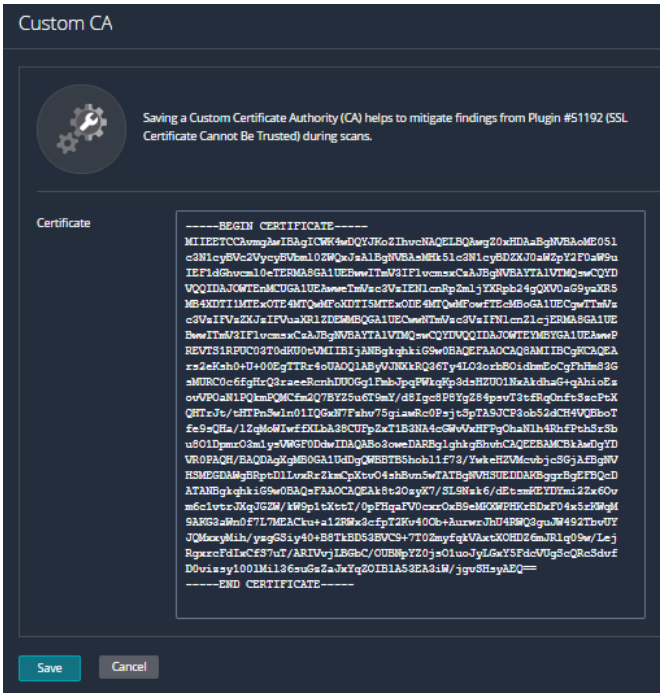


Figura 48. Certificado vinculado a nessus.

Para finalizar, reinicia el servicio de Nessus y ejecuta nuevamente el escáner

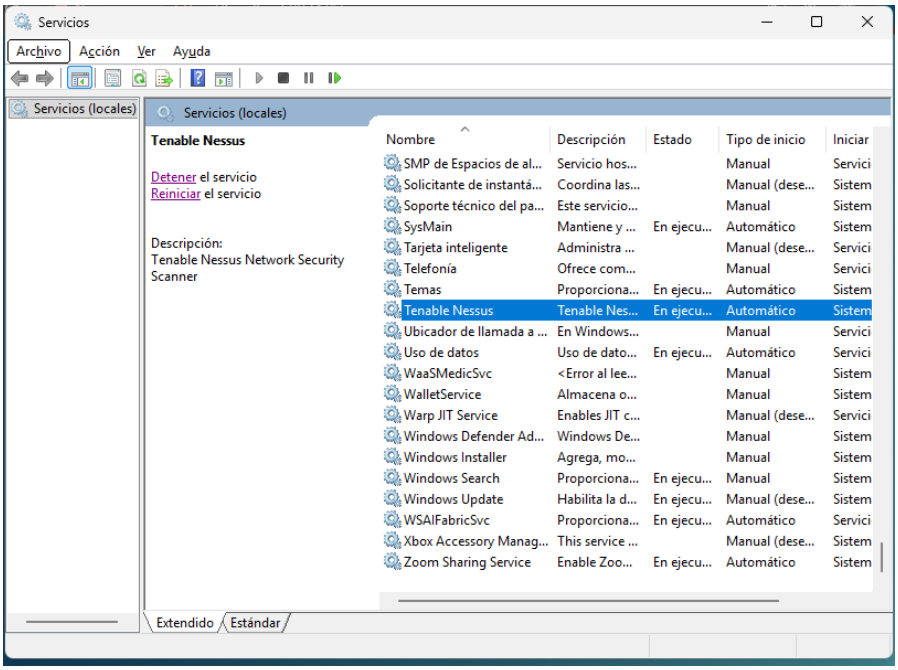


Figura 49. Reinicio del servicio de nessus.

Vulnerabilidad: SMB Signing not required

Ingresa a “Editor de directivas del grupo local” y da doble clic en la opción marcada.

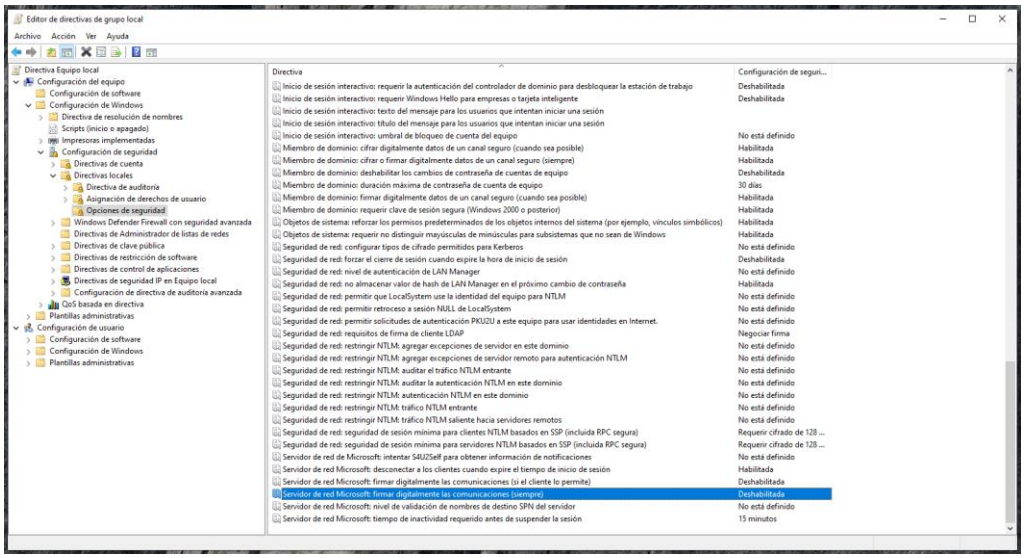


Figura 50. Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre).

Habilita el servicio y da clic en aplicar.



Figura 51. Habilitación del servicio: Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre).

Confirma los cambios a realizar.

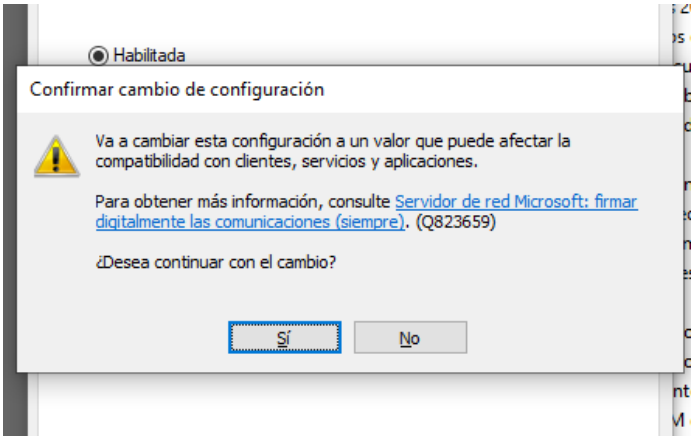


Figura 52. Confirmación de habilitación del servicio: Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre).

Vulnerabilidad: ICMP Timestamp Request Remote Date Disclosure

Abre powershell como administrador y crea una regla para permitir la comunicación de Nesuus, esto permite que el escáner muestre una falsa mitigación en el reporte.

Coloca la ip del servidor en donde se ejecuta nessus.

$NessusIP = "X.X.X.X"

Regla para permitir el escaneo completo desde la IP de Nessus.

New-NetFirewallRule -DisplayName "Permitir Trafico de Nessus" -Direction Inbound -RemoteAddress $NessusIP -Action Allow

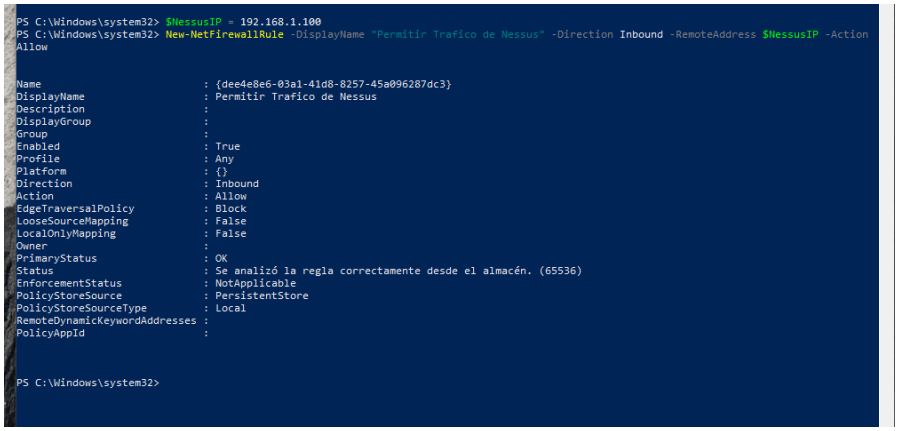


Figura 53. Regla que permite el escaneo desde la ip de nessus.

Creación de reglas para bloquear la vulnerabilidad.

Bloquea la vulnerabilidad ICMPv4 Timestamp

New-NetFirewallRule -DisplayName "Bloquear ICMPv4 Timestamp (10114)" -Direction Inbound -Protocol ICMPv4 -ICMPType 13 -Action Block -ErrorAction SilentlyContinue

Bloquea la vulnerabilidad ICMPv6 Tipo 13

New-NetFirewallRule -DisplayName "Bloquear ICMPv6 Tipo 13 (10114)" -Direction Inbound -Protocol ICMPv6 -ICMPType 13 -Action Block -ErrorAction SilentlyContinue

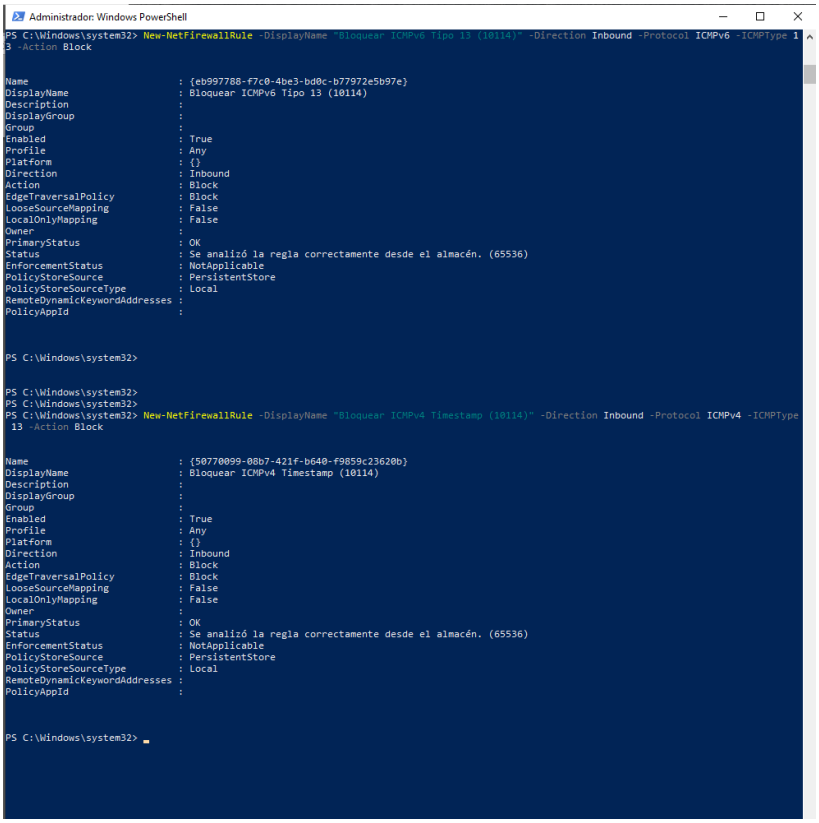


Figura 54. Ejecución de reglas para la mitigación de la vulnerabilidad.

Después de la mitigación realizada, se ejecutó por segunda vez el escaneo y dio como resultado los siguientes reportes

UEGEA_PC01

En este equipo se encontró la vulnerabilidad SSL Certificate Cannot Be Trusted, el resultado muestra que la vulnerabilidad ha sido remediada.

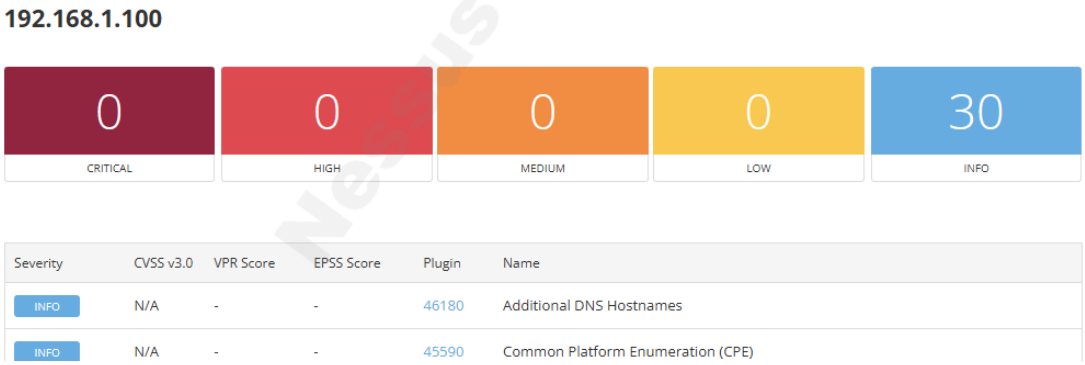


Figura 55. Resultado de la mitigación de vulnerabilidades.

UEGEA_PC0

En este equipo se encontraron las vulnerabilidades SMB Signing not required y ICMP Timestamp Request Remote Date Disclosure, el resultado muestra que las vulnerabilidades han sido mitigadas.

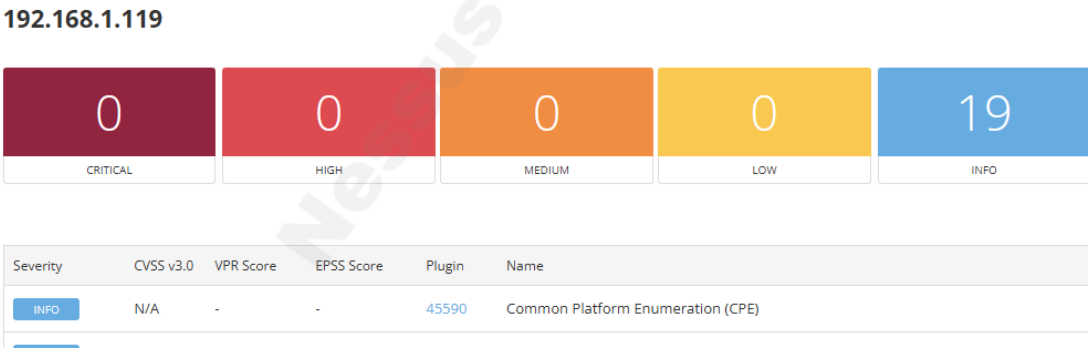


Figura 56. Resultado de la mitigación de vulnerabilidades.

e. Defensas contra malware (CIS Control 10)

Salvaguarda: Implementar y mantener software anti-malware.

Se realizó la descarga del software Avast Free Antivirus, este programa permitirá prevenir la propagación y ejecución de aplicaciones, códigos o scripts maliciosos en los activos empresariales.



Figura 57. Instalación de Avast Free Antivirus.

f. Recuperación de datos (CIS Control 11)

Salvaguarda: Establece y mantener un proceso de recuperación de datos

La implementación de esta salvaguarda se enfoca en el mantenimiento continuo de un proceso de recuperación de datos, lo cual es crucial para la resiliencia operativa de la Unidad Educativa General Eloy Alfaro. Este proceso debe abordar explícitamente el alcance de las actividades de backup, la priorización de la recuperación de los datos más sensibles y críticos, y la seguridad de los datos de respaldo. Considerando los riesgos de pérdida de información por fallas eléctricas (según la entrevista) o por ataques de malware (Riesgo Alto), esta salvaguarda garantiza la disponibilidad de los activos y la continuidad de las operaciones académicas y administrativas. Para asegurar su eficacia, la documentación de este proceso debe ser revisada y actualizada anualmente o ante cualquier cambio que afecte la infraestructura.

La ejecución de la salvaguarda implica un proceso de 3 etapas, liderado por el encargado del área de TI:

Definición

Se inicia identificando y priorizando los datos más críticos (registros académicos, prácticas de laboratorio, etc.) y el alcance de la recuperación. Se determinará la frecuencia de las copias de seguridad dependiendo de la sensibilidad de los datos (por ejemplo, cada mes) y el método de almacenamiento (Por ejemplo, discos duros externos o en la nube), asegurando la seguridad de los datos de respaldo para protegerlos de malware o acceso no autorizado.

Ejecución

El encargado de TI debe implementar un sistema automatizado de backup que garantice que los datos se copien según la frecuencia definida.

Prueba

La ejecución no termina con la copia de datos; la parte más crucial es la prueba periódica de recuperación, verificando que los datos puedan ser restaurados de forma exitosa y que la documentación del proceso se revise y actualice anualmente o cuando haya un cambio significativo

g. Concientización en seguridad y formación de habilidades (CIS Control 14)

La concientización en seguridad y formación de habilidades es indispensable para la estrategia de mitigación de la institución, ya que las acciones del factor humano desempeñan un papel crítico en el éxito o fracaso del programa de seguridad. Es frecuentemente más sencillo para un atacante manipular a un usuario para que revele información o instale malware a través de un enlace o archivo adjunto malicioso, que encontrar una vulnerabilidad técnica en la red.

Los propios usuarios, tanto intencional como involuntariamente, pueden desencadenar incidentes graves, como la pérdida de dispositivos, el uso de contraseñas débiles o el envío de datos confidenciales al destinatario equivocado. Por lo tanto, establecer y

mantener un programa formal de concientización es vital para influir en el comportamiento del personal y reducir los riesgos de ciberseguridad.

Salvaguarda: Establecer un programa de concientización sobre seguridad.

El programa de concientización y formación de habilidades en seguridad se plantea como una estrategia continua y formal dirigida a reducir el riesgo de incidentes derivados del factor humano en la institución. El propósito fundamental es educar a todos los miembros de la unidad educativa sobre cómo interactuar de manera segura con los activos y datos, contrarrestando la alta probabilidad de éxito de los ataques de ingeniería social (como el Phishing) que explotan la confianza de los usuarios.

Este programa, que incluye el uso de materiales educativos como trípticos y sesiones de capacitación, anualmente como mínimo, con el fin de asegurar que el personal esté debidamente capacitado para reducir los riesgos de ciberseguridad para la institución.

Salvaguarda: Capacitar a los miembros de la planta laboral para que reconozcan los ataques de ingeniería social.

La implementación de la salvaguarda requiere la capacitación específica del personal de la institución, para que de este modo sean capaces de reconocer y resistir los ataques de ingeniería social, incluyendo técnicas como la suplantación de identidad (phishing), pretextos y el seguimiento malicioso. Dado que el phishing es un vector de Riesgo Alto en la institución, este control es primordial para fortalecer la primera línea de defensa, el usuario.

El tríptico Anexo C. se diseñó como parte de esta propuesta servirá como una herramienta clave para esta capacitación, ya que proporciona información visual y concisa para educar a los usuarios sobre cómo identificar estas amenazas y reducir la probabilidad de que sean víctimas de manipulación psicológica por parte de los atacantes.

En la Tabla 15, se resume la lista de controles y salvaguardas implementadas en el desarrollo del presente proyecto.

Tabla 17. Resumen de Controles y salvaguardas implementadas.

Control	**Título del Control**	**Salvaguarda**
CIS Control 1	Inventario y control de los activos empresariales.	Establecer y mantener un inventario detallado de activos empresariales. Utilice una herramienta de descubrimiento activo.
CIS Control 2	Inventario y control de activos de software.	Elaborar y mantener actualizado el inventario de software. Tratamiento de software no autorizado.
CIS Control 4	Configuración segura de activos y software empresarial.	Configurar el bloque automático de sesiones en activos empresariales. Implementar y administrar un firewall en servidores.
CIS Control 5	Administración de cuentas.	Utilice contraseñas únicas.
CIS Control 6	Gestión de control de accesos.	Establecer y seguir un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de un usuario.
CIS Control 7	Gestión continua de vulnerabilidades.	Establecer y mantener un proceso de gestión de vulnerabilidades. Establecer y mantener un proceso de remediación. Remediar las vulnerabilidades detectadas.
CIS Control 10	Defensas contra malware.	Implementar y mantener software anti-malware.
CIS Control 11	Recuperación de datos.	Establecer y mantener un proceso de recuperación de datos.
CIS Control 14	Concientización en seguridad y formación de habilidades.	Establecer un programa de concientización sobre seguridad. Capacitar a los miembros de la planta laboral para que reconozcan los ataques de ingeniería social.

3.2.5 Fase 5: Monitorización, revisión y actualización

La implementación de los CIS Controls culmina en un ciclo de monitoreo continuo que garantiza la permanencia de la postura de seguridad lograda. Es esencial implementar sistemas de monitoreo para detectar y analizar eventos de seguridad que puedan indicar intentos de acceso no autorizado o incidentes en tiempo real. Más importante aún, la gestión de vulnerabilidades se convierte en un proceso recurrente, donde el encargado de TI supervisa de manera continua las nuevas vulnerabilidades que afecten tanto al software como al hardware, priorizando los esfuerzos de solución en función de la gravedad del riesgo (ejemplo, las reapariciones de vulnerabilidades SMB o de certificados SSL).

El componente de Revisión y Actualización de este paso es indispensable para mantener la resiliencia institucional. Esto implica la realización de Evaluaciones de seguridad periódicas para medir la eficacia de los controles implementados e identificar áreas de mejora. Asimismo, se deben realizar ejercicios de respuesta a incidentes y simulaciones de mesa con regularidad para probar la capacidad de la organización educativa para detectar, responder y recuperarse ante amenazas. Finalmente, la Actualización de políticas y procedimientos debe ser periódica, ajustando los documentos a las amenazas emergentes y a las lecciones aprendidas de los incidentes, garantizando que el programa de seguridad no se vuelva obsoleto.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- El análisis del estado actual de la infraestructura de red de la unidad educativa General Eloy Alfaro, realizado mediante la ficha de observación, la entrevista y la revisión de antecedentes, determinó la existencia de una brecha significativa en la higiene cibernética fundamental. Esta deficiencia se evidencia en la carencia de controles físicos y de gestión, tales como la ausencia de políticas para el control de acceso a puertos USB y la falta de un programa formal de concientización. Esta falta de formalización y la restricción presupuestaria incrementan la superficie de ataque y la dependencia del factor humano, confirmando la vulnerabilidad del entorno tecnológico.

- El escaneo de vulnerabilidades realizado sobre los equipos críticos de la infraestructura de red, utilizando la metodología de diagnóstico del marco de los CIS Controls, reveló la presencia de vulnerabilidades medias y un alto riesgo cibernético. Los resultados del escaneo confirmaron la existencia de configuraciones inseguras de red, incluyendo la falta de Firma SMB y el estado de Certificados SSL No Confiables en los dispositivos. Al mapear estos hallazgos a la matriz de evaluación de riesgos, se determinó que el Malware por USB y el phishing representan riesgos altos, con ponderaciones de 6 a 9, lo cual justificó la necesidad de implementar un marco de mitigación priorizado.

- Se implementaron las acciones de mitigación proporcionadas por los CIS Controls, logrando establecer un marco de ciberseguridad formal, sistemático y sostenible para la unidad educativa General Eloy Alfaro. Este proceso se centró en aplicar los controles esenciales para tratar los riesgos identificados. Al formalizar un plan de remediación basado en la criticidad del riesgo y definir procedimientos para el monitoreo continuo, se cumple con el objetivo de proveer a la institución de pautas claras para gestionar su ciberseguridad con

formalidad, optimizando su postura defensiva y reduciendo significativamente la probabilidad de incidentes.

4.2 Recomendaciones

- Se recomienda que el análisis de las vulnerabilidades identificadas sea complementado metodológicamente con un marco de referencia reconocido para la clasificación y contextualización de amenazas. Este uso adicional de un marco permitirá trascender la identificación de fallos técnicos, facilitando una mejora en la seguridad institucional.

- Se recomienda establecer formalmente la responsabilidad de la gestión de vulnerabilidades y la remediación continua al docente encargado de TI. Esta formalización debe incluir la realización periódica (mensual) de escaneos y la auditoría de los controles implementados. Es esencial documentar y revisar anualmente la efectividad de las correcciones aplicadas (como la Firma SMB) para asegurar que las vulnerabilidades Altas y Medias no reaparezcan y la madurez de seguridad se mantenga.

- Se recomienda implementar un programa obligatorio de capacitación anual y durante la contratación para todo el personal, centrado en el contenido de la Salvaguarda 14.2. El programa debe enfocarse en la enseñanza de cómo reconocer y resistir los ataques de ingeniería social (Phishing y Suplantación de Identidad). Al capacitar a la fuerza laboral, se reduce la probabilidad de incidentes causados por el error humano, creando una capa de defensa "humana" que complementa las soluciones técnicas del CIS.

- Se recomienda que, una vez que el Grupo de Implementación 1 (IG1) de los CIS Controls haya alcanzado una etapa de operación estable y sostenible, la unidad educativa General Eloy Alfaro planifique la expansión gradual de su marco de ciberseguridad migrando al Grupo de Implementación 2 (IG2). Esta transición debe ser considerada en los próximos presupuestos de mediano plazo (1 a 3 años). La migración al IG2 implica adoptar salvaguardas más avanzadas, como la gestión de la configuración de firewalls, la segmentación

de red (VLANs), o la autenticación multifactor (MFA) para las cuentas administrativas más críticas. Esta visión a futuro garantizará que la institución pueda mitigar amenazas más sofisticadas y aumentar su nivel de madurez, protegiendo la red a medida que crece su dependencia tecnológica.

REFERENCIAS BIBLIOGRÁFICAS

[1] C. Magazine, «2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics», Cybercrime Magazine. Accedido: 27 de noviembre de 2025. [En línea]. Disponible en: https://cybersecurityventures.com/cybersecurity-almanac-2024/

[2] «35 cybersecurity statistics to lose sleep over in 2025», WhatIs. Accedido: 27 de noviembre de 2025. [En línea]. Disponible en: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

[3] «Top Cybersecurity Statistics for 2025». Accedido: 1 de diciembre de 2025. [En línea]. Disponible en: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025

[4] «Global Cybercrime Report 2024: Which Countries Face the Highest Risk? | Blog | MixMode». Accedido: 1 de diciembre de 2025. [En línea]. Disponible en: https://www.mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk

[5] «Ecuador: Freedom on the Net 2024 Country Report», Freedom House. Accedido: 1 de diciembre de 2025. [En línea]. Disponible en: https://freedomhouse.org/country/ecuador/freedom-net/2024

[6] «Diseño e implementación de un sistema de seguridad mediante controles CIS para redes de acceso. Caso Instituto Nacional de Evaluación Educativa (INEVAL).» Accedido: 5 de diciembre de 2025. [En línea]. Disponible en: https://dspace.espoch.edu.ec/items/41ccdb3d-efb7-48c6-84c4-8e59151f315c

[7] J. C. Pardo Sarango, «Propuesta de implementación basada en controles CIS para una infraestructura de red: caso de estudio», 2025, Accedido: 11 de diciembre de 2025. [En línea]. Disponible en: https://repositorio.puce.edu.ec/handle/123456789/45983

[8] M. A. Ancajima Mendoza, «Propuesta de implementación de seguridad informática en las tic de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.», *Universidad Católica Los Ángeles de Chimbote*, mar. 2019, Accedido: 18 de mayo de 2025. [En línea]. Disponible en: https://repositorio.uladech.edu.pe/handle/20.500.13032/9386

[9] A. B. Santana Páez y R. A. Zurita Morales, «Análisis de la internetwork de la Institución Educativa Fiscal "Amazonas" y propuesta de rediseño siguiendo la metodología Top-Down Network Desing y los controles pertinentes del CIS Benchmark», bachelorThesis, 2021. Accedido: 5 de diciembre de 2025. [En línea]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/19702

[10] «How One School District Enhances Cyber Hygiene with the CIS Controls», CIS. Accedido: 9 de diciembre de 2025. [En línea]. Disponible en: https://www.cisecurity.org/case-study/school-district-enhances-cyber-hygiene-with-cis-controls/

[11] K. C. Laudon y J. P. Laudon, *Management Information Systems: Organization and Technology*, 4th ed. USA: Prentice-Hall, Inc., 1995.

[12] C. Pfleeger y S. Pfleeger, *Security in Computing.*, 5th ed. Pearson Education., 2015.

[13] P. Bowen, J. Hash, y M. Wilson, «SP 800-100. Information Security Handbook: A Guide for Managers», National Institute of Standards & Technology, Gaithersburg, MD, USA, Technical Report, sep. 2006.

[14] «CIS Controls», CIS. Accedido: 18 de mayo de 2025. [En línea]. Disponible en: https://www.cisecurity.org/controls/

[15] E. Turban, L. Volonino, y G. R. Wood, *Information Technology for Management: Digital Strategies for Insight, Action, and Sustainable Performance*, 10th ed. Wiley Publishing, 2015.

[16] W. Stallings, *Data and Computer Communications.* Pearson Education, 2016.

[17] C. C. Editor, «vulnerability - Glossary | CSRC». Accedido: 18 de mayo de 2025. [En línea]. Disponible en: https://csrc.nist.gov/glossary/term/vulnerability

ANEXOS

Anexo A. Encuesta a docentes de la Unidad Educativa General Eloy Alfaro.

ENCUESTA DIRIGIDA A DOCENTES

Instrucciones: Marque con una "X" la opción que mejor represente su respuesta.

1. ¿Sabe usted si la unidad educativa cuenta con un inventario de activos informáticos?
   ( ) Si
   ( ) No

2. ¿Con qué frecuencia utiliza los equipos y la red de la unidad educativa?
   (1) Diariamente
   (2) Ocasionalmente
   (3) Rara Vez
   (4) Nunca

3. ¿Qué tan segura considera que es la red de la unidad educativa para proteger su información personal e institucional?
   (1) Muy segura
   (2) Segura
   (3) Neutral
   (4) Insegura
   (5) Muy insegura

4. ¿Alguna vez ha notado problemas de rendimiento al momento de utilizar la red de la institución?
   (1) Siempre
   (2) Casi siempre
   (3) Varias veces
   (4) Rara vez
   (5) Nunca

5. ¿A recibido correos sospechosos (phishing) en sus cuentas de correros electrónicos?
   (1) Siempre
   (2) Casi siempre
   (3) A veces
   (4) Rara vez
   (5) Nunca

6. ¿Qué tan familiarizado se encuentra respecto a medidas de prevención y mitigación de vulnerabilidades de seguridad?

(1) Muy bien familiarizado
(2) Bien familiarizado
(3) Moderadamente familiarizado
(4) Poco familiarizado
(5) Muy poco familiarizado

7. ¿Estaría de acuerdo en recibir capacitación sobre ciberseguridad para ayudar a proteger su información y la de la unidad educativa?
   (1) Totalmente de acuerdo
   (2) De acuerdo
   (3) Neutral
   (4) En desacuerdo
   (5) Totalmente en desacuerdo

8. ¿Considera que la implementación de medidas adicionales de seguridad (por ejemplo, doble autenticación) mejorará la seguridad de acceso a las cuentas?
   (1) Totalmente de acuerdo
   (2) De acuerdo
   (3) Neutral
   (4) En desacuerdo
   (5) Totalmente en desacuerdo

9. ¿Cree que la red de la unidad educativa es vulnerable a ataques de seguridad?
   (1) Totalmente de acuerdo
   (2) De acuerdo
   (3) Neutral
   (4) En desacuerdo
   (5) Totalmente en desacuerdo

10. ¿Cree que la implementación de un conjunto priorizado de mejores prácticas de ciberseguridad como los CIS Critical Security Controls (CIS Controls) será beneficioso para la unidad educativa?
    (1) Totalmente de acuerdo
    (2) De acuerdo
    (3) Neutral
    (4) En desacuerdo
    (5) Totalmente en desacuerdo

Anexo B. Encuesta a estudiantes de la Unidad Educativa General Eloy Alfaro.

ENCUESTA DIRIGIDA A ESTUDIANTES

Instrucciones: Marque con una "X" la opción que mejor represente su respuesta.

1. ¿Con qué frecuencia utiliza los equipos y la red de la unidad educativa?
   (1) Diariamente
   (2) Ocasionalmente
   (3) Rara Vez
   (4) Nunca

2. ¿Ha notado mal funcionamiento es los equipos de la unidad educativa?
   (1) Siempre
   (2) Casi siempre
   (3) Rara vez
   (4) Nunca

3. ¿Qué tan seguro se siente al utilizar la red de la institución?
   (1) Muy seguro
   (2) Seguro
   (3) Neutral
   (4) Poco seguro
   (5) Muy poco seguro

4. ¿Qué tan informado esta sobre la importancia de utilizar una contraseña segura y por qué es importante?
   (1) Muy informado
   (2) Informado
   (3) Neutral
   (4) Poco informado
   (5) Muy poco informado

5. ¿Alguna vez ha tenido dificultad en descargar archivos o en acceder a sitios web desde los equipos de la unidad educativa?
   (1) Siempre
   (2) Casi siempre
   (3) Rara vez
   (4) Nunca

6. ¿Confía en que los trabajos y archivos que guarda en los equipos de la unidad educativa están seguros y no se perderán?
   (1) Totalmente confiado
   (2) Confiado
   (3) Neutral

(4) Poco confiado
(5) Muy poco confiado

7. ¿Cree que los equipos de la unidad educativa se encuentran protegidos contra programas maliciosos o virus?
   (1) Totalmente protegidos
   (2) Protegidos
   (3) Neutral
   (4) Poco protegidos
   (5) Muy poco protegidos

8. ¿Con que frecuencia ha accedido a cuentas personales desde equipos de la unidad educativa?
   (1) Siempre
   (2) Casi siempre
   (3) Varias veces
   (4) Rara vez
   (5) Nunca

9. ¿Estaría de acuerdo en seguir normas más estrictas en el uso de la red de la unidad educativa con el fin de tener una red más segura?
   (1) Totalmente de acuerdo
   (2) De acuerdo
   (3) Neutral
   (4) En desacuerdo
   (5) Totalmente en desacuerdo

10. ¿Estaría de acuerdo con tener una red más segura en la unidad educativa, aunque esto signifique tener una mayor restricción sobre la navegación y descarga de archivos o software?
    (1) Totalmente de acuerdo
    (2) De acuerdo
    (3) Neutral
    (4) En desacuerdo
    (5) Totalmente en desacuerdo

Anexo C. Tríptico sobre ingeniería social usado en la capacitación.

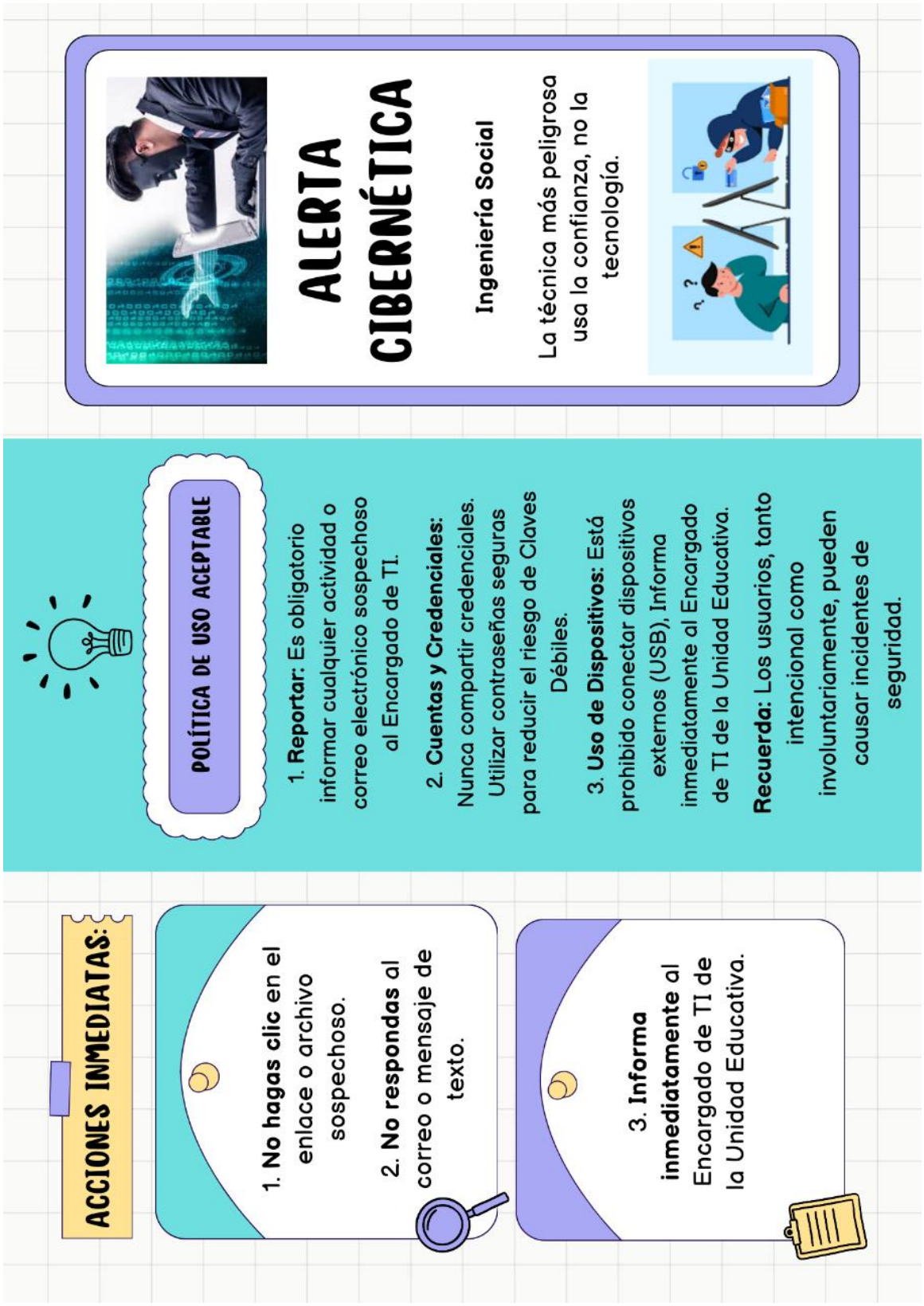


Figura 58. Tríptico usado en la capacitación.

Figura 59. Tríptico usado en la capacitación.