UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR

TECNOLOGÍAS DE LA INFORMACIÓN

AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LA “UNIDAD EDUCATIVA DR. JOSÉ MARÍA VELASCO IBARRA”

ALCIVAR MARCILLO JOSIAS DANIEL

AUTOR

MGS. POZO HERNÁNDEZ CLARA GUADALUPE

TUTOR

EL CARMEN, AGOSTO 2024

CERTIFICACIÓN DEL TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría del estudiante **ALCIVAR MARCILLO JOSIAS DANIEL**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2023(2)-2024(1), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es **AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LA "UNIDAD EDUCATIVA DR. JOSÉ MARÍA VELASCO IBARRA"**
La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 23 de julio del 2024

Lo certifico,

Ing. Clara Guadalupe Pozo Hernández, Mg.
Docente Tutor(a)
Área:

TRIBUNAL DE SUSTENTACIÓN

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EL CARMEN

APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con modalidad Proyecto Integrador, titulado "Auditoría Informática en la infraestructura tecnológica de la Unidad Educativa Dr. José María Velasco Ibarra", cuyo autor es ALCIVAR MARCILLO JOSIAS DANIEL de la Carrera de Ingeniería en Tecnologías de la Información y como Tutor de Trabajo de Titulación la Ing. Pozo Hernández Clara Guadalupe, Mg.

El Carmen, agosto de 2024

Ing. Wladimir Minaya, Mg.
Presidente del tribunal de titulación

Ing. Saed Reascos, Mg.
Miembro del tribunal de titulación

Ing. Jefferson Arca, Mg.
Miembro del tribunal de titulación

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LA "UNIDAD EDUCATIVA DR. JOSÉ MARÍA VELASCO IBARRA", corresponde exclusivamente a: Alcivar Marcillo Josias Daniel con CI.2300567175, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Alcivar Marcillo Josias Daniel

C.I. 2300567175

DEDICATORIA

Después de un largo año de arduo trabajo, gracias a Dios pude completar el objetivo el cual fue culminar mi trabajo de Titulación, le dedico este trabajo a mis padres quienes han sido piezas fundamentales que me han estado apoyando siempre continuamente, también agradezco profundamente a mis hermano/as ya que siempre estuvieron ahí conmigo apoyándome en todo momento.

JOSIAS ALCIVAR

AGRADECIMIENTO

En primer lugar, agradecido con Dios ya que sin él yo no hubiera podido llegar hasta aquí, también agradezco profundamente a la Ing. Clarita ya que, sin su ayuda, orientación y su paciencia no hubiera sido posible completar este proyecto, también le agradezco profundamente a mis padres ya que siempre han estado ahí conmigo apoyándome, también agradezco al apoyo de mis hermano/as que siempre estuvieron alentándome para que yo pudiera seguir adelante y cumplir este objetivo el cual nos llena de felicidad a todos.

JOSIAS ALCIVAR

ÍNDICE GENERAL

PORTADA I

CERTIFICACIÓN DEL TUTOR II

TRIBUNAL DE SUSTENTACIÓN III

DEDICATORIA V

JOSIAS ALCIVAR V

AGRADECIMIENTO VI

ÍNDICE GENERAL VII

ÍNDICE DE TABLAS XIII

ÍNDICE DE ILUSTRACIONES XV

ÍNDICE DE ANEXOS XVI

RESUMEN XVII

ABSTRACT XVIII

CAPÍTULO I 1

1.1 Introducción 1

1.2 Presentación del tema 2

1.3 Ubicación y contextualización de la problemática 2

1.4 Planteamiento del problema 3

1.4.1 Problematización 3

1.4.2 Génesis del problema 3

1.4.3 Estado actual del problema 3

1.5 Diagrama causa – efecto del problema 4

1.6 Objetivos 5

1.6.1 Objetivo general 5

1.6.2 Objetivos específicos 5

1.7 Justificación 5

1.8 Impactos esperados 6

1.8.1 Impacto tecnológico 6

1.8.2 Impacto social 6

1.8.3 Impacto ecológico 7

CAPÍTULO II 8

2 MARCO TEÓRICO 8

2.1 ANTECEDENTES HISTÓRICOS 8

2.1.1 Auditoría Informática 8

2.1.2 Infraestructura Tecnológica 9

2.2 Antecedentes de investigaciones relacionadas al tema presentado 9

2.2.1 Incidencia del uso de infraestructura tecnológica en los procesos de inter-aprendizaje, en la escuela Julio Matovelle en el séptimo grado, sección vespertina. 9

2.2.2 Auditoría informática a la infraestructura tecnológica y sistemas de información bajo el estándar cobit en la institución educativa escuela normal Superior de Quibdó ... 10

2.2.3 Auditoría informática en la empresa distribuidora los paisas 10

2.2.4 Auditoría informática, para la evaluación de riesgos en la seguridad de la información en la cooperativa de ahorro y crédito Prodvisión, de la provincia de Tungurahua, cantón Pelileo. 11

2.2.5 Auditoría informática para optimizar el rendimiento de los sistemas y equipos informáticos aplicando la metodología computer resource management review (crmr), en la cooperativa de ahorro y crédito maquita Ltda. Del cantón Ambato parroquia Quisapinch. 11

2.3 Definiciones conceptuales 12

2.3.1 Variable Independiente 12

2.3.1.1 Concepto de la auditoría y concepto de la informática 12

2.3.1.2 Definición de Auditoría en Informática 13

2.3.1.3 Introducción a la seguridad informática 14

2.3.1.4 Fundamentos de la ciberseguridad 14

2.3.1.5 Análisis de riesgo de los sistemas de información 15

2.3.1.6 Las Vulnerabilidades 16

2.3.2 Variable dependiente 16

2.3.2.1 Sistemas informáticos 16

2.3.2.2 Funcionamiento de un Sistema Informático 16

2.3.2.3 Sistemas operativos 17

2.3.2.4 Funciones del SO 17

2.3.2.5 Componentes físicos Hardware 17

2.3.2.6 Componentes lógicos Software 18

2.3.3 Metodología de desarrollo 19

1. MAGERIT 19

2.4 Conclusiones del marco teórico 20

CAPÍTULO III 21

3 MARCO INVESTIGATIVO 21
3.1 Introducción 21
3.2 Tipos de investigación 22
3.2.1 Investigación Cuantitativa 22
3.3 Métodos de investigación 22
3.3.1 Exploratorio 23
3.3.2 Descriptivo 23
3.4 Fuentes de información de datos 24
3.5 Fuentes primarias 24
3.6 Fuentes secundarias 24
3.6.1 Encuestas 25
3.6.2 Entrevista 25
3.7 Estrategia operacional para la recolección de datos 26
3.7.1 Población 26
3.7.2 Muestra 26
3.7.3 Análisis de las herramientas de recolección de datos a utilizar 26
3.7.3.1 Encuesta 26
3.7.3.2 Entrevista 27
3.7.3.3 Estructura de los instrumentos de recolección de datos aplicados 29
3.7.4 Plan de recolección de datos 29
3.8 Análisis y presentación de resultados 30

3.8.1 Presentación y descripción de los resultados obtenidos 30
3.8.1.1 Análisis de datos obtenidos a través de la encuesta.....30
3.8.1.2 Análisis de datos obtenidos a través de la entrevista.....35
3.8.1.3 Presentación y descripción de los resultados obtenidos 40
3.8.2 Informe final del análisis de los datos.....40
CAPÍTULO IV.....42
4 MARCO PROPOSITIVO.....42
4.1 Introducción 42
4.2 Descripción de la propuesta 43
4.2.1 Propósito 43
4.2.2 Ámbito del análisis de riesgo.....43
4.2.3 Perspectiva análisis de riesgo.....43
4.3 Determinación de recursos.....44
4.3.1 Humanos 44
4.3.2 Tecnológicos.....45
4.3.3 Económicos.....45
4.3.4 Planificación 46
4.3.5 Programa de auditoria.....46
4.4 Desarrollo (Análisis de riesgo).....47
4.4.1 Identificación de activos 48
4.4.2 Valoración de activos.....59

4.4.3 Identificación de Amenazas 60
4.4.3.1 Cuestionario para analizar los riesgos 63
4.4.4 Valoración de amenazas 68
4.4.5 Fase 03 Impacto residual 68
4.5 APLICACIÓN DE LA AUDITORÍA 69
4.5.1.1 FOTOGRAFIAS DE LA APLICACIÓN DE LA ENTREVISTA Y LOS CONTROLES EVALUADOS, EXPLICACIÓN. 69
4.5.1.2 TABULACIÓN DE DATOS 72
4.5.1.3 ANALIZAR RIESGOS 73
CAPÍTULO V 76
5 EVALUACIÓN DE RESULTADOS 76
5.1 Informe de Auditoría 76
5.1.1.1 Dirigido a: 76
5.1.1.2 Motivo: 76
5.1.1.3 Objetivos: 76
5.1.1.4 Alcance: 76
5.1.1.5 Personal relacionado: 77
5.1.1.6 Hallazgos: 77
5.2 NIVEL DE SEGURIDAD GENERAL 77
5.2.1 OPINIÓN 83
5.3 CONCLUSIONES DE LA AUDITORÍA 84
5.4 RECOMENDACIÓNES DE LA AUDITORÍA 84

CAPÍTULO VI.....93

6 CONCLUSIONES Y RECOMENDACIONES 93

6.1 Conclusiones 93

6.2 Recomendaciones.....94

6.3 BIBLIOGRAFÍA.....95

6.4 ANEXOS.....100

6.5 Anexo E: Fotografías 103

6.6 Glosario 114

ÍNDICE DE TABLAS

Tabla 1 Plan de recolección de datos.....29

Tabla 2 Análisis de datos a través de encuesta 34

Tabla 3.Análisis de datos a través de la entrevista.....39

Tabla 4. Determinación de recursos. Humanos 45

Tabla 5. Determinación de recursos. Tecnológicos.....45

Tabla 6. Determinación de recursos. Económicos.....46

Tabla 7. Programa de Auditoría.....47

Tabla 8. Identificación activos Hardware 51

Tabla 9. Identificación activos Software 58

Tabla 10. Tabla de Valoración de activos.....59

Tabla 11. Valoración de activos Hardware y Software 60

Tabla 12. Identificación de Amenazas de los activos (Hardware uy software).....62

Tabla 13 Valoración de amenazas 68

Tabla 14. Fotografía de controles aplicados 72

Tabla 15. Leyenda (Probabilidad e Impacto).....74

Tabla 16. Matriz de Riesgos 74

Tabla 17. Riesgos encontrados 83

ÍNDICE DE ILUSTRACIONES

Ilustración 1Ubicación la Institución Educativa 2

Ilustración 2Vista de la entrada principal de la Institución 2

Ilustración 3. Árbol del problema 4

Ilustración 4. Valoración de riesgo 73

Ilustración 5. Tabla de Análisis de riesgo. (Gravedad) 73

Ilustración 6. Tabla para analizar el nivel de aparición. (Probabilidad) 73

Ilustración 7. Guía de buenas prácticas 85

Ilustración 8. Índice de guía de buenas practicas 86

Ilustración 9. Objetivo de la Guía 87

Ilustración 10. Introducción de la Guía 88

Ilustración 11. Recomendaciones sobre los controles de seguridad 89

Ilustración 12. Recomendaciones sobre Mantenimiento Físico y Uso de equipos 90

Ilustración 13. Recomendaciones sobre el Uso de programas 91

Ilustración 14. Recomendaciones sobre el Uso de contraseñas, Indicadores para crear contraseñas y control de red de wifi 92

ÍNDICE DE ANEXOS

Anexo A: Asignación de tutor 100

Anexo B: Certificado de la empresa 101

Anexo C: Reporte del sistema antiplagio 102

Anexo D: Evidencia de aplicación de encuestas y entrevista 109

RESUMEN

En el ámbito de la informática, las auditorías se han vuelto esenciales debido a la dificultad que enfrentan muchas organizaciones para mantener el control y asegurar que grandes volúmenes de datos y activos estén en perfecto orden y sin vulnerabilidades. Por esta razón, se consideró necesario realizar una auditoría informática en la Unidad Educativa "Dr. José María Velasco Ibarra".

Como método de investigación, se empleó un enfoque cuantitativo y se llevó a cabo una auditoría utilizando la metodología Magerit. Para determinar la muestra, se seleccionaron 24 personas de la institución, incluyendo al Rector/a, Vicerrector/a, Inspector/a, secretaria y otros docentes.

Como parte del desarrollo de la auditoría informática, tanto lógica como física, se utilizó la metodología Magerit para facilitar el análisis e identificar los riesgos y vulnerabilidades presentes en los sistemas de información y en la infraestructura del laboratorio.

Se implementó una tabla de estimación de riesgo para identificar los peligros tras la evaluación de vulnerabilidades en el laboratorio de cómputo, obteniendo los siguientes resultados: el riesgo de robo tiene un 40% de probabilidad y se considera apreciable; los daños al equipo tienen un 68% de probabilidad y se consideran muy graves; el riesgo de incendio tiene un 57% de probabilidad y se considera importante; el riesgo de malware tiene un 72% de probabilidad y se considera muy grave; y el phishing tiene un 88% de probabilidad y también se considera muy grave.

De antemano se recomienda seguir la guía de buenas prácticas que fue implementada para mejorar el uso del laboratorio.

ABSTRACT

In the IT field, audits have become essential due to the difficulty that many organizations face in maintaining control and ensuring that large volumes of data and assets are in perfect order and without vulnerabilities. For this reason, it was considered necessary to carry out a computer audit in the “Dr. José María Velasco Ibarra”.

As a research method, a quantitative approach was used and an audit was carried out using the Magerit methodology. To determine the sample, 24 people from the institution were selected, including the Rector, Vice Rector, Inspector, secretary and other teachers.

As part of the development of the computer audit, both logical and physical, the Magerit methodology was used to facilitate the analysis and identify the risks and vulnerabilities present in the information systems and laboratory infrastructure.

A risk estimation table was implemented to identify dangers after evaluating vulnerabilities in the computer laboratory, obtaining the following results: the risk of theft has a 40% probability and is considered appreciable; damage to equipment has a 68% probability and is considered very serious; the risk of fire has a 57% probability and is considered important; the risk of malware has a 72% probability and is considered very serious; and phishing has an 88% probability and is also considered very serious.

Beforehand, it is recommended to follow the good practices guide that was implemented to improve the use of the laboratory.

CAPÍTULO I

1.1 Introducción

La “Unidad Educativa Dr. José María Velasco Ibarra”, ubicada en el recinto de San Ramón de Tigrillo, se distingue por su riguroso enfoque educativo y la dedicación de sus 24 docentes para enseñar a una población estudiantil de 560 alumnos. Esta institución ofrece una única titulación, el Bachillerato en Ciencias, y sus clases se imparten exclusivamente en la mañana.

En sus instalaciones, cuenta con un laboratorio de cómputo equipado con 24 computadoras. No obstante, con el paso de los años, este laboratorio ha experimentado un considerable deterioro debido a la falta de mantenimiento adecuado. Muchas computadoras han dejado de funcionar, limitando la capacidad de los estudiantes para realizar actividades tecnológicas y expandir sus conocimientos en esta área crucial.

El objetivo principal de este trabajo es realizar una auditoría informática en la Unidad Educativa “Dr. José María Velasco Ibarra” para asegurar que los sistemas de información y la infraestructura tecnológica estén en orden y libres de vulnerabilidades.

Se empleó un enfoque cuantitativo como metodología de investigación para garantizar la objetividad y precisión en la recopilación y análisis de datos. La auditoría se llevó a cabo utilizando la metodología Magerit, un marco reconocido para la gestión de riesgos en tecnologías de la información. Para determinar la muestra, se seleccionaron 24 personas que forman parte de la institución, incluyendo al Rector/a, Vicerrector/a, Inspector/a, secretaria y otros docentes. Esta fue realizada para obtener una visión representativa y comprensiva del estado selección de los sistemas de información y la infraestructura tecnológica.

Se propuso realizar una auditoría informática en la Unidad Educativa “Dr. José María Velasco Ibarra” utilizando un enfoque cuantitativo y la metodología Magerit. Esta metodología permite un análisis exhaustivo tanto de los aspectos lógicos como físicos de los sistemas de información y la infraestructura del laboratorio.

Como resultado, se encontraron riesgos el cual representan peligro para el laboratorio entre los riesgos encontrados tenemos: robo, daño de equipos, incendio, malware y phishing, se

analizaron estos riesgos y se implementó una guía para el intervenir ante cualquier situación de riesgo que se presente.

1.2 Presentación del tema

AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LA "UNIDAD EDUCATIVA DR. JOSÉ MARÍA VELASCO IBARRA"

1.3 Ubicación y contextualización de la problemática

La "Unidad Educativa Dr. José María Velasco Ibarra" se encuentra ubicada en el recinto de San Ramón de Tigrillo, es un colegio que cuenta con 24 docente y 560 estudiantes, se caracteriza por su estricta enseñanza, también por la disposición de cada uno de los docentes para enseñar a los estudiantes.

Esta institución cuenta con una sola rama de Titulación que es Bachiller en Ciencias, las clases son totalmente matutinas. El colegio cuenta con un laboratorio de computación, en el cual hay 24 computadoras

Ilustración 1Ubicación la Institución Educativa

1.4 Planteamiento del problema

1.4.1 Problematización

Hace varios años atrás la Unidad Educativa "Dr. José María Velasco Ibarra" tuvo la oportunidad de contar con un laboratorio de computación, en la actualidad dicho laboratorio le hace falta un mantenimiento, y las computadoras han empezado a deteriorarse. Muchas computadoras han dejado de funcionar, por lo cual los estudiantes no pueden realizar sus actividades en el área tecnológica y aumentar sus conocimientos.

Para crear una auditoría debemos conocer los motivos por el cual el laboratorio se encuentra en dicho estado. ¿Cuál es la situación actual del laboratorio de computación?

1.4.2 Génesis del problema

La Unidad Educativa "Dr. José María Velasco Ibarra" fue fundada en el año 2001, el motivo por el cual se creó fue para darle una educación a todos los jóvenes y niños que vivían alrededor del sector, con el pasar del tiempo la institución fue creciendo, en el año 2015 se obtuvo de parte del gobierno un laboratorio de computación con una cantidad de 24 computadoras, estas con el fin de promover una mejor educación a los estudiantes de dicha institución, a lo largo del tiempo, los equipos han empezado a deteriorarse por motivo de que no ha tenido un respectivo mantenimiento, el cual les ayude a tener un mejor rendimiento. No ha tenido ningún docente que se encargue de cada cierto tiempo llevar control a cada uno de los equipos

1.4.3 Estado actual del problema

El problema empezó cuando nadie se hizo cargo del llevar un manejo del laboratorio hubo falta de control en los equipos esto ocasionaba que cualquier estudiante utilice las

máquinas sin ningún tipo de restricción, también la falta de limpieza era un problema ya que el polvo dañaba las computadoras y esto provocaba una corta duración a las máquinas, la falta de mantenimiento se podía ver de diferentes formas ya que no solamente se dañaban las computadoras sino también los inmuebles, se empezaron a dañar las mesas, las sillas y esto generaba problema entre los estudiantes y profesores que querían utilizar el laboratorio, por otro lado el laboratorio cuenta con un mal estado en la infraestructura electrónica dado que los cables se encuentran regados en el suelo y esto puede ocasionar que lleguen a quemarse los equipos por una descarga eléctrica por falta de mantenimiento, el laboratorio está totalmente en un descontrol y esto ha generado hasta pérdida de componentes, como cables, de adaptadores, mouse, teclados, etc.

1.5 Diagrama causa – efecto del problema

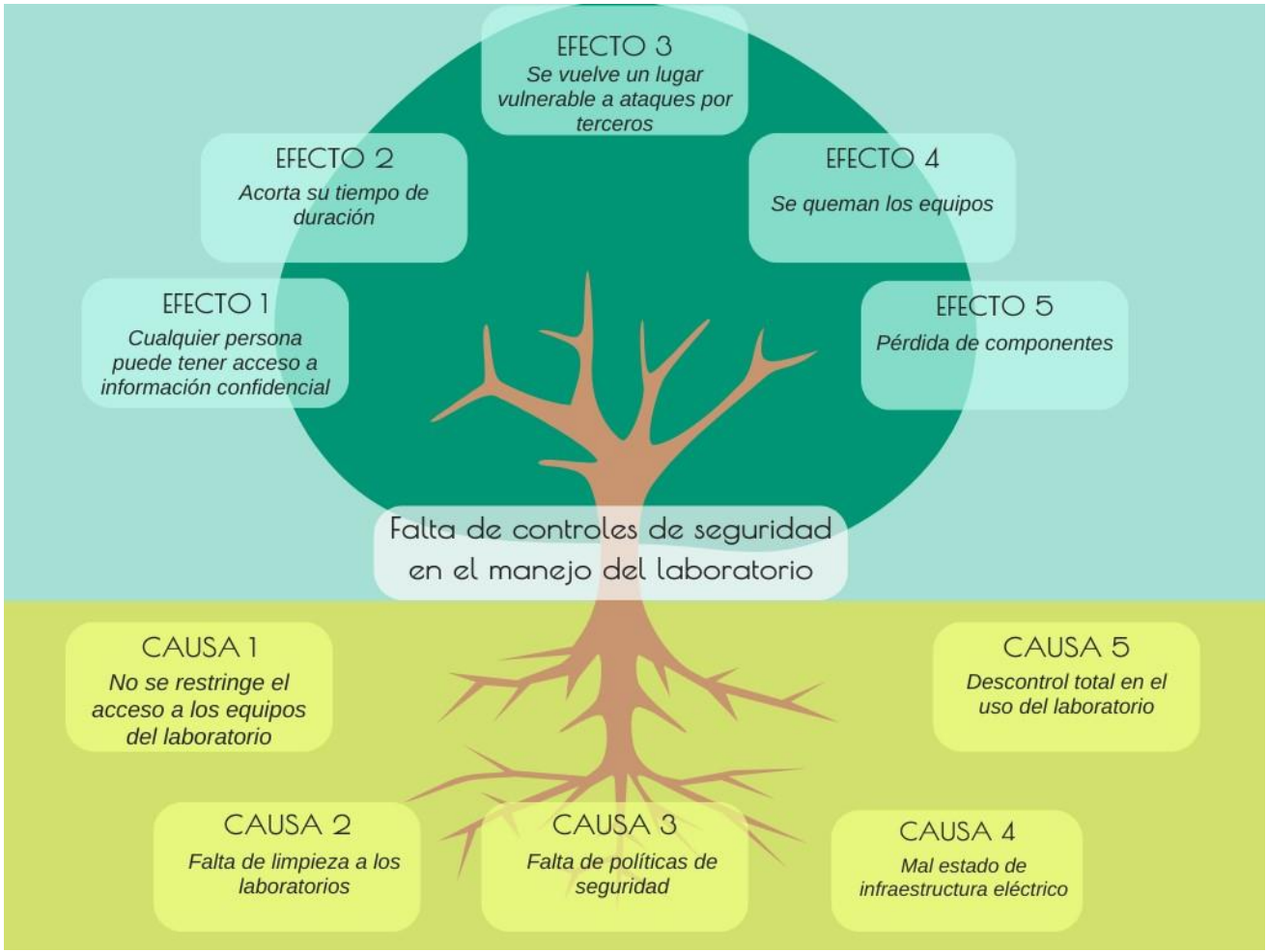


Ilustración 3. Árbol del problema

1.6 Objetivos

1.6.1 Objetivo general

Realizar una auditoría de seguridad informática en el área del laboratorio de computación de la Unidad Educativa “Dr. José María Velasco Ibarra”.

1.6.2 Objetivos específicos

- Identificar la problemática mediante una revisión general de la infraestructura de laboratorio de cómputo.
- Investigar en diferentes libros para fundamentar la auditoría informática y también lo que es la infraestructura tecnológica.
- Aplicar métodos, técnicas de investigación, para que se pueda justificar que existe el problema a solucionar mediante el presente proyecto.
- Evaluar la seguridad del laboratorio y analizar de los riesgos de seguridad informática de la institución.
- Elaborar un informe con los hallazgos y con resultados más relevantes de la Auditoría, para ayudar a la institución con una lista de recomendaciones para evitar que sean vulnerables.

1.7 Justificación

La auditoría informática se ha convertido en un pilar muy fundamental a nivel mundial para muchas empresas, a través del desarrollo de auditorías muchas empresas cumplen con los reglamentos establecidos por la ley o/y por la empresa, esta ayuda a recoger, agrupar información y avaluar si la empresa cumple con todos los reglamentos.

La auditoría se encarga de realizar una investigación a fondo en una empresa y con los resultados obtenido se genera un análisis del estado en que se encuentra la empresa. Con la auditoría que se va a generar los puntos más vulnerables y que tenga la institución en el ámbito tecnológico y a través de los resultados tomar medidas correctivas que aseguren a la empresa, y brindar confiabilidad, confidencialidad y disponibilidad.

En esta Institución aún no se ha realizado ninguna auditoría por lo tanto se vio en la necesidad de desarrollar una para determinar el estado se encuentra el laboratorio de esta institución. Gracias a que la institución me concedió el permiso para evaluar sus instalaciones.

A través de esta auditoría que se va a desarrollar, la institución obtendrá los resultados sobre el estado en el que se encuentra el laboratorio, y se les brindará algunas alternativas para proteger el laboratorio de computación y así la institución tomará las debidas medidas de precaución.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

En lo tecnológico el impacto que se obtendrá a través de la auditoría será que por medio de la investigación y con los resultados obtenidos, se evitará ataques a la infraestructura y a los equipos para que estos no sean vulnerables y estar preparados para cualquier situación de peligro ya sea por medio de hackers o alguien que intente sobrepasas la seguridad de la infraestructura de la institución.

1.8.2 Impacto social

En la sociedad estudiantil les beneficia mucho tanto a los estudiantes como a los docentes, porque con los resultados de la auditoría se deberá tomar las medidas necesarias para darle un buen uso y mantenimiento para que este pueda ser utilizado por los estudiantes y sacar el mayor provecho y aumentar sus conocimientos.

1.8.3 Impacto ecológico

La institución o empresa tomará medidas de seguridad las cuáles ayuden que los equipos tecnológicos alargarán su tiempo y éstos no sean desechados ya que esto produce que se infecte el medio ambiente, pero si se cuida también se estará cuidando el medio ambiente.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 ANTECEDENTES HISTÓRICOS

2.1.1 Auditoría Informática

En la década de 1960, los sistemas de información comenzaron a ser cada vez más comunes en las empresas, especialmente en los bancos y en los departamentos administrativos de las grandes corporaciones. La información, que antes era completamente documental, empezó a almacenarse en archivos magnéticos, iniciando así el proceso de automatización de las actividades manuales. Sin embargo, este avance se produjo a un ritmo lento debido a los elevados costos de las computadoras. (Uribe, 2000)

Es la evaluación y el examen de los controles, sistemas y procedimientos informáticos, así como de los equipos de cómputo, su uso, eficiencia y seguridad dentro de la organización que maneja el procesamiento de la información. El objetivo es, mediante la identificación de alternativas, alcanzar un uso más eficiente y seguro de la información, los equipos y el recurso humano, mejorando los procesos y logrando una organización ágil, dinámica, controlada y segura de manera integral. (León, 2017)

Los objetivos de la auditoría de sistemas son los siguientes: realizar una evaluación exhaustiva con un equipo multidisciplinario y especializado en el ámbito de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del departamento de informática. Además, se pretende analizar el uso de los recursos financieros en las áreas del centro de información, así como la eficiencia del sistema computacional, sus equipos periféricos e instalaciones. Asimismo, se evalúa el aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y el mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información. (Chulde, 2017)

A finales de la década de 1960, se comienza a reconocer la necesidad de auditar los sistemas de información, marcando prácticamente el nacimiento de la Auditoría Informática (AI) propiamente dicha. En 1968, en Estados Unidos, varias asociaciones de profesionales identifican la necesidad de desarrollar y proporcionar documentación a los auditores para guiarlos y orientarlos en la auditoría y control de sistemas computarizados. En la década de

1970, el intercambio de experiencias da lugar a la aparición de las primeras obras sobre auditoría informática, que posteriormente son traducidas al español. (Jorge, 2015)

2.1.2 Infraestructura Tecnológica

En 1959 comenzó la era de las mainframes y minicomputadoras. La introducción de las máquinas IBM 1401 y 7090 en ese año marcó el inicio del uso comercial generalizado de las computadoras mainframe. (Fortes, 2016)

La infraestructura de TI está compuesta por una serie de dispositivos físicos y aplicaciones de software esenciales para el funcionamiento de toda la empresa. Además, la infraestructura de TI se define como un conjunto de servicios integrales que atraviesan la organización, financiados por la administración y que incorporan tanto capacidades humanas como técnicas. Estos servicios incluyen, plataformas de cómputo utilizadas para ofrecer servicios informáticos que conectan a empleados, clientes y proveedores dentro de un entorno digital coherente. Esto abarca desde grandes mainframes hasta computadoras de escritorio y portátiles, además de asistentes digitales personales y dispositivos para Internet. (Laudon, 2019)

Estas computadoras poseían la capacidad necesaria para soportar miles de terminales remotas en línea, conectadas a la mainframe central mediante protocolos de comunicación y líneas de datos propietarias. Las minicomputadoras, producidas por Digital Equipment Corporation (DEC), ofrecían potentes máquinas a precios más asequibles que las mainframes de IBM. Esto permitió la computación descentralizada, adaptada a las necesidades específicas de departamentos individuales o unidades de negocio, en lugar de compartir el tiempo de uso en una sola y enorme mainframe. (Cabuto, 2018)

2.2 Antecedentes de investigaciones relacionadas al tema presentado

2.2.1 Incidencia del uso de infraestructura tecnológica en los procesos de inter-aprendizaje, en la escuela Julio Matovelle en el séptimo grado, sección vespertina.

El proyecto sobre la influencia del uso de infraestructura tecnológica tiene como objetivo mejorar la calidad educativa mediante la integración de tecnologías en los procesos de inter-aprendizaje. Esta investigación busca identificar las principales ventajas del uso adecuado de los laboratorios de computación en el proceso de inter-aprendizaje en los estudiantes de séptimo año de Educación General Básica en la institución educativa Julio

Matovelle. La metodología empleada para el análisis de caso incluye métodos y técnicas cualitativas, utilizando fichas de observación y encuestas. Los resultados obtenidos de las encuestas aplicadas a los docentes son descritos y analizados. Los estudiantes representan el 50% de la población, lo que hace que la muestra sea adecuada y significativa. (León Amendaño, 2018)

2.2.2 Auditoría informática a la infraestructura tecnológica y sistemas de información bajo el estándar cobit en la institución educativa escuela normal Superior de Quibdó

Este proyecto tiene como objetivo asistir a una institución en la mejora de su seguridad interna mediante la recopilación de información sobre su infraestructura tecnológica. Para ello, se realizaron entrevistas al personal del Departamento de Sistemas con el fin de identificar sus necesidades y requerimientos técnicos. La metodología utilizada combina enfoques cuantitativos y cualitativos. Los resultados revelan que la institución no posee un cronograma periódico para el mantenimiento preventivo y correctivo de los equipos, y que, en ocasiones, estas tareas son llevadas a cabo por estudiantes. Es esencial que la institución implemente un cronograma regular de mantenimiento de equipos. (Machado Lloreda, 2018)

2.2.3 Auditoría informática en la empresa distribuidora los paisas

El presente proyecto de auditoría está dirigido a una empresa que se dedica a la elaboración, comercialización y venta de productos en los sectores de panadería, pastelería, pizzería, heladería y maquinaria. Su objetivo es realizar una auditoría informática a la empresa Distribuidora Los Paisas, evaluando la administración, control, monitoreo y uso de las tecnologías de información y comunicación. La metodología del proyecto se basó en un enfoque cualitativo, permitiendo evaluar de manera detallada los diversos controles y políticas aplicados, o en algunos casos, la ausencia de estos, para valorar el manejo adecuado o inadecuado de los recursos informáticos de la empresa. Los resultados incluyen el análisis de la información estratégica de la empresa, la documentación preliminar, el análisis de la información y la evaluación del control interno. (Chávez Tisalema, Repositorio en Digital Universidad Técnica de Ambato, 2022)

2.2.4 Auditoría informática, para la evaluación de riesgos en la seguridad de la información en la cooperativa de ahorro y crédito Prodvisión, de la provincia de Tungurahua, cantón Pelileo.

El presente proyecto de investigación se llevó a cabo con el objetivo de realizar una Auditoría Informática en la Cooperativa de Ahorro y Crédito Provisión. El propósito de esta auditoría es analizar las posibles deficiencias y proporcionar orientación al personal responsable del área informática. La meta es evaluar la situación actual y la infraestructura tecnológica de la cooperativa. Se empleó la metodología OCTAVE, una herramienta de análisis de riesgos que estudia los riesgos basándose en los principios de Confidencialidad, Integridad y Disponibilidad. Entre los resultados obtenidos, se identificó que no existen políticas ni procedimientos escritos para la gestión de la seguridad física de la red. Actualmente, la gestión de estas tareas recae en los encargados de cada sala, quienes las realizan de manera individual y sin uniformidad. (Paul, Repositorio Digital Universidad Tecnica de Ambato, 2021)

2.2.5 Auditoría informática para optimizar el rendimiento de los sistemas y equipos informáticos aplicando la metodología computer resource management review (crmr), en la cooperativa de ahorro y crédito maquita Ltda. Del cantón Ambato parroquia Quisapinch.

El presente proyecto surge de la necesidad de evaluar el funcionamiento de los sistemas y equipos informáticos de la institución financiera. Para ello, se lleva a cabo una Auditoría Informática utilizando la metodología CRMR (Computer Resource Management Review). El objetivo es optimizar el rendimiento de los sistemas y equipos informáticos mediante esta metodología. En el proyecto, se utilizaron entrevistas y encuestas detalladas, las cuales se describen a continuación. Como resultado, se obtuvo una evaluación de la condición actual y la infraestructura de las áreas auditables, contribuyendo al control interno informático de la Cooperativa de Ahorro y Crédito Maquita LTDA. (Mayorga Mayorga, 2023)

2.3 Definiciones conceptuales

2.3.1 Variable Independiente

2.3.1.1 Concepto de la auditoría y concepto de la informática

El concepto de revisión a menudo se malinterpreta, considerándose únicamente como una evaluación destinada a encontrar y señalar errores. Así, el término "implementación de la revisión" se ha utilizado como sinónimo de la identificación de defectos que deben detectarse antes de una auditoría, justificando la realización de una revisión. Sin embargo, el término auditoría tiene un alcance más amplio; no solo identifica errores, sino que es un estudio riguroso diseñado para evaluar la eficacia y eficiencia de la unidad u organización, y determinar acciones alternativas para mejorar la organización y alcanzar los objetivos recomendados. (Antonio, 2019)

La auditoría de seguridad informática evalúa exhaustivamente todos los procesos relacionados con la seguridad, tanto físicos como lógicos. La seguridad física se enfoca en la protección de componentes de hardware, dispositivos, instalaciones y entornos de los sistemas informáticos. Los auditores deben verificar que estos elementos estén adecuadamente protegidos contra posibles desastres, incendios, robos, entre otros riesgos. Por otro lado, la seguridad lógica se centra en la protección del software, los procesos y programas del sistema. La auditoría de seguridad lógica incluye el análisis de la correcta protección y actualización de estos componentes, así como la salvaguarda de los datos del sistema. (Tejada, 2015)

El auditor tiene el derecho de revisar y evaluar las cuentas con el propósito de medir la eficacia y utilidad de sus acciones, permitiéndole así tomar decisiones que faciliten la corrección o mejora de errores, sugiriendo cursos de acción alternativos. Al igual que existen normas y procedimientos específicos para las auditorías contables, también deben establecerse normas y procedimientos para las auditorías informáticas dentro de la profesión. Estas pueden inspirarse en la experiencia de otras industrias, pero presentan características particulares y se fundamentan en la filosofía de que la auditoría no debe limitarse a la detección de errores, sino que también debe enfocarse en la evaluación y mejora de lo existente, corrigiendo fallos y proponiendo soluciones alternativas. (Loor, 2021)

2.3.1.2 Definición de Auditoría en Informática

Según Tejada (2015) El procedimiento para obtener y analizar evidencias que relacionen ambas pruebas se divide en varias etapas:

- Inspección de los sistemas de la organización para identificar los controles existentes.
- Realización de pruebas de cumplimiento para verificar el adecuado funcionamiento de los controles identificados.
- Análisis de las evidencias obtenidas durante las pruebas de cumplimiento para evaluar el alcance y la precisión de las pruebas sustantivas.
- Verificación de la validez de los datos mediante las evidencias obtenidas en las pruebas sustantivas.

Una auditoría de TI implica la revisión y evaluación de los controles, sistemas y procedimientos de información, así como la eficiencia, uso y seguridad de los equipos informáticos utilizados en el procesamiento de datos en una organización. El propósito de esta auditoría es promover un uso más eficiente, confiable y seguro de la información, implementando alternativas que faciliten la toma de decisiones adecuadas. La información recolectada es fundamental para disminuir la incertidumbre en el proceso de toma de decisiones, y el valor de esta disminución está vinculado a los beneficios derivados de las decisiones tomadas. (Verduga, 2020)

Según Solorzano (2020) los factores que pueden afectar a una organización a través de controles y auditorías de TI incluyen:

- Es necesario controlar el desarrollo del uso de la computadora.
- Controlar el uso de la computadora es cada vez más importante y costoso.
- Los altos costos del fracaso para las organizaciones
- Abuso informático
- Posible pérdida de potencia de procesamiento de datos.
- La posibilidad de una decisión equivocada.
- Necesidad de mantener la privacidad

2.3.1.3 Introducción a la seguridad informática

La sección inicial explora los aspectos fundamentales de la seguridad informática, abarcando sus conceptos clave, componentes, terminología, definiciones de virus y una variedad de estrategias para la prevención y corrección en este campo. (Castro, 2018)

- **La seguridad en términos generales:**

La seguridad está estrechamente ligada a la gestión de riesgos, lo cual implica que siempre hay estrategias disponibles para evitar o prevenir riesgos. Existen medidas específicas que pueden implementarse para reducir al mínimo estas situaciones. La seguridad se define como la eliminación de riesgos, concepto que abarca cuatro acciones esenciales aplicables en cualquier entorno de seguridad: prevención, transferencia, mitigación y aceptación de riesgos. (Morán, 2018)

- **Concepto de seguridad informática:**

La ciberseguridad se dedica a salvaguardar los sistemas informáticos. Según varios especialistas, la informática se centra en los procedimientos, técnicas y sistemas para el manejo, almacenamiento y transmisión de datos. Además, la protección de la información abarca no solo los activos informáticos, sino también cualquier medio que contenga datos, lo que amplía su aplicación a prácticamente todos los sectores, siendo crucial en el ámbito de la informática al abordar cualquier concepto relacionado. (Mero, 2018)

2.3.1.4 Fundamentos de la ciberseguridad

En esta sección se explorarán los conceptos, amenazas, riesgos y vulnerabilidades asociados con la ciberseguridad en las organizaciones. Además, se abordarán las diferentes áreas de vulnerabilidad que pueden ser aprovechadas por ciberdelincuentes para llevar a cabo ataques, tales como la ingeniería social y el principio de privilegio mínimo. (Merino, 2020)

- **Los tres pilares de seguridad**

Los datos comprenden diversos elementos como valores, números, medidas, palabras y documentos originales. La información, por su parte, añade valor al dato al proporcionar conocimiento. En entornos empresariales, los datos pueden manifestarse en manuales de procedimientos, registros de empleados, proveedores y clientes, así como bases de datos de facturación. Estos conjuntos de datos se transforman en informes que contribuyen al crecimiento y eficiencia de la empresa. La seguridad de la información se fundamenta en garantizar que todos los usuarios puedan acceder a la información relevante con integridad y

disponibilidad, minimizando riesgos y maximizando la eficiencia operativa. (Navarrete, 2018)

La confidencialidad implica asegurar que solo el personal autorizado pueda acceder a la información pertinente, permitiendo que cada sistema automatizado o independiente utilice únicamente los recursos necesarios para sus funciones. Este principio no solo protege los mensajes, sino también todos los datos e información bajo su responsabilidad. La integridad, por otro lado, constituye el segundo pilar de la seguridad, asegurando que la información no se pierda ni se vea comprometida de manera deliberada o accidental. La utilización de información incorrecta puede ser tan perjudicial como su pérdida, ya que incluso manipulaciones sutiles pueden desencadenar errores acumulativos y decisiones adversas. (Quimiz, 2018)

La accesibilidad es crucial para asegurar que la información tenga un nivel mínimo de seguridad. Es fundamental que la información sea accesible más allá de los usuarios específicos para ser verdaderamente útil. Además, su integridad depende de que el acceso no sea complicado o imposible, asegurando que la información valiosa esté disponible para todos aquellos que la requieran. (Merino, 2020)

2.3.1.5 Análisis de riesgo de los sistemas de información

El análisis de riesgos de nuestros activos es fundamental para evaluar el posible impacto de cualquier incidente de seguridad. Este impacto generalmente se refleja en términos económicos, pero también puede afectar la credibilidad y la reputación de nuestra marca, lo cual tiene implicaciones financieras significativas. Además, el incumplimiento de leyes, normativas y procedimientos durante un incidente puede agravar aún más las consecuencias. Los conceptos clave en la gestión de riesgos incluyen activos, amenazas, vulnerabilidades, impacto y probabilidad. (Arantes, 2022)

Un riesgo se refiere a un evento o serie de eventos que tienen el potencial de amenazar la viabilidad de un proyecto organizacional o de obstaculizar su éxito. La definición de riesgo ha sido objeto de extensos debates, aunque existe consenso en las características fundamentales que todo riesgo informático debe poseer. Primero, implica incertidumbre: el evento en cuestión puede o no materializarse, no se puede asegurar su ocurrencia. Segundo, conlleva la posibilidad de pérdida: en caso de que el riesgo se materialice, se anticipan diversas consecuencias adversas para la organización. (Tejada, 2015)

2.3.1.6 Las Vulnerabilidades

2.3.1.6.1 Vulnerabilidades físicas

Las vulnerabilidades físicas pueden tener un impacto directo en la infraestructura organizacional. Por ejemplo, los desastres naturales, como los terremotos en áreas de alto riesgo, representan una alta vulnerabilidad, pudiendo interrumpir servicios y afectar la disponibilidad, generando problemas adicionales. Del mismo modo, las inundaciones son otro ejemplo de riesgo físico. Además, las deficiencias en los controles de acceso a infraestructuras críticas pueden permitir accesos no autorizados, lo que representa un riesgo significativo. La introducción no autorizada de dispositivos USB también plantea amenazas a la seguridad al permitir la copia de información y afectar la infraestructura. (Cruzatti, 2018)

2.3.2 Variable dependiente

2.3.2.1 Sistemas informáticos

Un sistema informático es una configuración de dispositivos que incluyen al menos una unidad central de procesamiento (CPU), conectados física y lógicamente entre sí a través de redes locales o comunicaciones remotas. Estos dispositivos se integran mediante componentes de software que permiten la interacción con diversos agentes externos, incluidos los usuarios humanos. (Pérez J. S., 2015)

El propósito fundamental de un sistema informático es facilitar el procesamiento, almacenamiento, entrada y salida de datos, los cuales son parte integral de sistemas de información, tanto generales como específicos. Para cumplir con este objetivo, el sistema informático se dota de diversos recursos adaptados a su aplicación específica. Conocido en el ámbito tecnológico como SI, un sistema informático es un conjunto organizado de elementos interrelacionados que permiten almacenar y procesar información de manera automática. Estas herramientas informáticas se destacan por su velocidad y eficiencia, facilitando así la toma de decisiones y la resolución de problemas en las organizaciones. Además de analizar problemas, los sistemas informáticos permiten la creación de nuevos productos basados en la información recopilada. Estos sistemas están compuestos por tres partes interrelacionadas: componentes físicos, lógicos y humanos. (Lopez, 2019)

2.3.2.2 Funcionamiento de un Sistema Informático

Un sistema informático gestiona diversos tipos de información, como números, texto, imágenes, sonidos y vídeo, procesándolos mediante entradas y salidas. Utiliza mecanismos

específicos de representación, almacenamiento y presentación, como se detalla a continuación. Desde la perspectiva humana, es sencillo distinguir entre números, texto, imágenes, sonidos y vídeo gracias a nuestros sentidos y el cerebro. A diferencia del funcionamiento humano, los ordenadores, como máquinas digitales basadas en la electrónica, operan mediante la representación exclusiva de información binaria. Por lo tanto, necesitan codificar la información del mundo real en formatos binarios y utilizar métodos para su presentación adecuada. (Pérez J. C., 2015)

2.3.2.3 Sistemas operativos

Un sistema operativo se define como un conjunto de programas diseñados para actuar como intermediarios entre el hardware de una computadora y el usuario, facilitando así la utilización del equipo. Estos sistemas proporcionan interfaces atractivas y de fácil uso. El sistema operativo tiene la responsabilidad de crear y eliminar procesos, planificar su ejecución y proveer mecanismos de sincronización. En la era moderna, los sistemas operativos son multitarea, por lo que es crucial gestionar los procesos de manera efectiva para optimizar el rendimiento del sistema. Es esencial monitorear constantemente la carga de la CPU por proceso y el estado de los demás procesos. El componente clave encargado de asignar la CPU y gestionar el tiempo de ejecución es el planificador. Un sistema operativo típicamente incorpora varios tipos de planificadores: el planificador a largo plazo, encargado de decidir qué procesos se admiten en el sistema, y el planificador a corto plazo, que selecciona entre los procesos listos para ejecutarse en la CPU. (Monge, 2023)

2.3.2.4 Funciones del SO

La principal función de un sistema operativo consiste en proporcionar al usuario una interfaz intuitiva para interactuar con el ordenador de manera efectiva. Uno de sus objetivos primordiales es asegurar la comodidad del usuario al hacer que el uso del ordenador sea más fácil y accesible mediante el sistema operativo. Además, promueve la eficiencia al optimizar el uso de los recursos del equipo. Las funciones de un sistema operativo varían según el enfoque. Desde la perspectiva de los programadores, debe ofrecer una interfaz sencilla que oculte la complejidad del hardware, mientras que para el usuario final debe proporcionar una experiencia cómoda, como ya se mencionó anteriormente. (Campos, 2023)

2.3.2.5 Componentes físicos Hardware

La palabra 'hardware' tiene su origen en el inglés y se traduce literalmente como 'ferretería'. Se refiere al conjunto físico de elementos que componen un sistema informático,

incluyendo equipos eléctricos, cables, periféricos y otros componentes físicos conectados a la máquina. Para comprender el funcionamiento de una computadora, es útil categorizar el hardware según las funciones desempeñadas por las diferentes unidades del sistema. De acuerdo con esta clasificación, encontramos dispositivos de entrada, como teclados o ratones; unidades de procesamiento, como microprocesadores o memoria; y dispositivos de salida, como monitores o impresoras. (Caccuri, 2018)

Compuesto por los componentes físicos del Sistema de Información (SI), el hardware incluye los dispositivos terminales, los canales y los medios de almacenamiento de información. Estos dispositivos son tanto electrónicos como electromecánicos, diseñados para captar información, realizar cálculos y presentar datos mediante sensores, unidades de procesamiento, almacenamiento y monitores, entre otros (Pérez Tejada, 2015)

2.3.2.6 Componentes lógicos Software

El término "software" fue introducido por primera vez en 1957 por J.W. Tukey, quien lo presentó en un artículo publicado en 1958 en "American Mathematical Monthly", denominándolo "computer software". En este artículo, Tukey enfatizó la importancia de aprovechar las capacidades de cálculo de las computadoras, permitiendo a los programadores crear y organizar conjuntos complejos de instrucciones que serían traducidas a un lenguaje comprensible para las máquinas. El software se refiere a los componentes del sistema que no tienen una representación física y se utilizan para el procesamiento de información, incluyendo programas de ordenador que gestionan estructuras de datos, como las bases de datos, que son colecciones organizadas de información que sustentan el sistema. (Carlos, 2015)

El software abarca el conjunto de componentes lógicos requeridos para el funcionamiento de un sistema informático, consistiendo en elementos intangibles y no físicos. Su rol es crucial en cualquier sistema informático, ya que facilita la interacción y gestiona el hardware para llevar a cabo las tareas solicitadas por el usuario. En términos amplios, el software incluye programas informáticos, procedimientos, normas, documentación y datos esenciales para el funcionamiento de un sistema de cómputo. (Lopez, 2019)

2.3.3 Metodología de desarrollo

1. MAGERIT

Alcanzar una seguridad absoluta es una meta poco realista. Sin embargo, mediante la implementación continua de sistemas de seguridad que se basen en estándares, normativas y metodologías, es posible lograr un nivel de seguridad adecuado que reduzca los riesgos. Este estudio tiene como objetivo resaltar las características clave de una metodología que ayuda en el análisis y la identificación de riesgos y vulnerabilidades en los sistemas de información. En el artículo, se presenta a MAGERIT como una herramienta y un marco de referencia que facilita este proceso. (Zabala, 2018)

La metodología MAGERIT se distingue por su enfoque en el análisis y gestión de riesgos en Tecnologías de la Información (TI). Dentro del ámbito del gobierno de las TI, resulta impracticable implementar todas las metodologías existentes simultáneamente. Por esta razón, es esencial evaluar y seleccionar la metodología que mejor se adapte a cada organización. Es importante mencionar que, aunque hay numerosas metodologías diseñadas para enfrentar diferentes problemas, cada una está específicamente elaborada para resolver contextos particulares, con enfoques y niveles de detalle variados. En última instancia, es crucial optar por la metodología más adecuada en cada caso, teniendo en cuenta la disponibilidad de información y el nivel de detalle necesario. (Guzmán J. P., 2018)
La metodología MAGERIT se destaca en el análisis y gestión de riesgos en Tecnologías de la Información. Esta metodología clasifica los activos organizacionales en diferentes grupos, lo que facilita la identificación de riesgos y la implementación de medidas adecuadas para su control y prevención. Desarrollada por el Consejo Superior de Administración Electrónica de las administraciones públicas de España, MAGERIT subraya la importancia de la gestión de riesgos dentro de las directrices de buen gobierno. Desde su lanzamiento en 1997, MAGERIT ha evaluado los riesgos desde una perspectiva económica, con el fin de adherirse a los principios fundamentales y cumplir con los requisitos mínimos necesarios para garantizar una protección adecuada de la información, asegurando una aplicación proporcional. (Alchundia, EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT, 2018)

El análisis y la gestión de riesgos en MAGERIT se llevan a cabo a través de tres volúmenes: métodos, catálogo de elementos y guía técnica.

- El primer libro de MAGERIT: método, ofrece una guía exhaustiva para el análisis de la gestión de riesgos y la estructura del proyecto de implementación de esta metodología. Este documento detalla la organización requerida para el modelo de gestión de riesgos, abarcando aspectos como los métodos de análisis de riesgos. Entre ellos, se incluyen tres tipologías: métodos cualitativos, cuantitativos y semicuantitativos, los cuales se utilizan para evaluar el nivel de riesgo en contextos empresariales. (Guzmán J. P., 2018)
- El segundo libro de MAGERIT, titulado 'Catálogo de Elementos', se presenta como una herramienta esencial para facilitar el análisis de riesgos en las empresas. Este libro ofrece un catálogo detallado que abarca varios aspectos clave: tipos de activos, dimensiones para evaluar estos activos (como disponibilidad, integridad de los datos, confidencialidad, autenticidad y trazabilidad), criterios de valoración (permitiendo el uso de diversas escalas de valoración, generalmente cualitativas y a discreción del usuario), así como amenazas comunes a los sistemas de información y las salvaguardias recomendadas para su protección. (Alchundia, El análisis y gestión, enfoque de la metodología magerit, 2018)
- El tercer libro de MAGERIT proporciona a los usuarios guías técnicas tanto específicas como generales para llevar a cabo proyectos de análisis y gestión de riesgos. Entre las guías técnicas específicas se incluyen el análisis mediante tablas, que tiene como objetivo estandarizar y especificar valoraciones y estimaciones dentro de un rango preestablecido. Además, se presenta el análisis algorítmico, que se subdivide en dos enfoques: el modelo cualitativo, destinado a ofrecer una valoración relativa del riesgo para los activos, y el modelo cuantitativo, que se centra en cuantificar las variaciones del riesgo. (Ordoñes, 2019)

2.4 Conclusiones del marco teórico

En el marco teórico se pudo fundamentar a través de investigación cada uno de los subtemas que están relacionado con las variables las cuales eran auditoría informática e infraestructura tecnológica, también se pudo resaltar temas más importantes que están relacionados con el tema de proyecto.

También en el marco teórico se pudo realizar lo que fue la investigación de los antecedentes históricos en la cual se pudo conocer la historia de cada una de las variables, también se agregó la metodología que se utilizó en este proyecto de investigación.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

El diseño de investigación cuantitativa representa el enfoque predominante, buscando obtener conocimientos fundamentales de manera imparcial a través de conceptos y variables medibles. Este método estructurado implica la recopilación y análisis de datos provenientes de diversas fuentes, haciendo uso de herramientas informáticas, estadísticas y matemáticas para generar resultados concluyentes y proyectables a una población mayor

En el contexto específico de la auditoría realizada en la Unidad Educativa "Dr. José María Velasco Ibarra", se aplicó el método cuantitativo mediante entrevistas y encuestas a los docentes. Este enfoque proporcionó información actualizada sobre el estado del laboratorio de computación, identificando problemas y evaluando la necesidad de medidas preventivas. Los datos recopilados fueron tabulados y analizados estadísticamente para proporcionar una visión clara del estado actual del laboratorio.

El método descriptivo empleado expuso los aspectos clave del laboratorio, como la configuración de hardware, eficacia de los procedimientos y seguridad de la red. La observación y recopilación de datos facilitaron la selección de características críticas para la evaluación y éxito del laboratorio de computación.

Dos métodos de investigación cuantitativa destacados fueron utilizados para recopilar datos: la encuesta y la entrevista. La encuesta, dirigida a los docentes de la institución, proporcionó información directa sobre el manejo y problemas del laboratorio, mientras que las entrevistas con autoridades como el rector y la vicerrectora confirmaron la existencia de los problemas identificados

3.2 Tipos de investigación

3.2.1 Investigación Cuantitativa

El diseño de investigación cuantitativa es el enfoque experimental predominante en muchas disciplinas científicas. Su objetivo principal es obtener conocimientos fundamentales y seleccionar el modelo más adecuado para una comprensión objetiva de la realidad, utilizando datos recolectados y analizados a través de conceptos y variables medibles. Este tipo de investigación ofrece una forma estructurada de recopilar y analizar datos de diversas fuentes, empleando herramientas informáticas, estadísticas y matemáticas para obtener resultados. Es concluyente en su propósito, ya que busca cuantificar el problema y determinar su grado de generalización mediante resultados aplicables a una población más amplia. (Neill, 2018)

Este enfoque se implementó durante la auditoría mediante entrevistas y encuestas realizadas al cuerpo docente de la institución. El objetivo era recabar información actualizada sobre el laboratorio de computación con el fin de verificar la presencia de problemas existentes y tomar medidas preventivas. Además, los resultados de las encuestas y entrevistas fueron tabulados para obtener estadísticas que reflejaran el estado actual del laboratorio. (Victor, 2018)

La investigación cuantitativa se aplicó para comprender relaciones de causas y efectos mediante las encuestas con preguntas cerradas y mediante esto realizar un análisis estadístico y matemático.

Se aplicó el método cuantitativo en la entrevista a las autoridades de la institución, para determinar en número el porcentaje de las preguntas aplicadas y además determinar el porcentaje de niveles de riesgos encontrados en el laboratorio de la Unidad Educativa “Dr. José María Velasco Ibarra”, con el objetivo de recolectar información sobre el estado actual del laboratorio para verificar la presencia de los problemas existentes y tomar medidas preventivas. Además, los resultados de las encuestas y entrevistas fueron tabulados para obtener estadísticas que reflejaran el estado actual del laboratorio.

3.3 Métodos de investigación

Existen algunos métodos como el exploratorio, descriptivo y el estudio de casos, entre otros.

3.3.1 Exploratorio

Son útiles durante las fases iniciales del proceso de toma de decisiones gerenciales. Estos instrumentos están diseñados para facilitar una investigación preliminar de la situación específica en cuestión. Además, son adecuados en contextos donde la dirección está en la búsqueda de identificar problemas existentes o potenciales oportunidades para nuevos enfoques, ideas o hipótesis relacionadas con el estudio en curso.**Fuente especificada no válida.**

Se delimitó con precisión el alcance del método exploratorio para identificar las áreas específicas del laboratorio de computación sujetas a investigación preliminar. Los objetivos de la auditoría exploratoria se definieron de manera clara e incluyeron la identificación de posibles problemas en la seguridad de la información, la eficiencia en el uso de recursos, así como la evaluación de oportunidades para la implementación de nuevas tecnologías (Mite, 2019)

El método exploratorio en esta investigación se utilizó para la identificación del problema también para la recopilación de información sobre las causas existentes dentro del laboratorio de la Unidad Educativa "Dr. José María Velasco Ibarra" las cuales son: que no se restringe el acceso a los equipos, también la falta de limpieza en el laboratorio, la falta de políticas de seguridad, el mal estructurado eléctrico y el descontrol total en el uso del laboratorio, en la recolección de problemas también existe un problema el cual es: falta de controles de seguridad en el manejo de laboratorio, entre los efectos encontramos: cualquier persona puede tener acceso a información confidencial, acortan su tiempo de duración, se vuelve un lugar vulnerable a ataques por terceros, se queman los equipos, pérdida de componentes, estos son los efectos encontrados dentro de la investigación y se realizó una guía para el buen uso del laboratorio.

3.3.2 Descriptivo

El método descriptivo en esta investigación se utilizó como un método preciso para recolectar información, a través de las preguntas de encuestas realizadas a los docentes de la Unidad Educativa "Dr. José María Velasco Ibarra" y entrevistas realizadas a las autoridades de la institución que está conformada por: Rectora, Vise-rectora, Inspectora, Secretaria, se describió mediante variedades categóricas, entre ellas numéricas y gráficas, en las cuales

numéricas se utilizaban para calificar el porcentaje de riesgos según las preguntas y mediante gráficas mostrar información apreciable mediante los cálculos y porcentaje.

La descripción surge como resultado directo de la observación y representa el primer paso necesario hacia la formulación de explicaciones. La función principal de la descripción es integrar los hallazgos observados, presentando los rasgos fundamentales del fenómeno estudiado de manera detallada. El método descriptivo facilita la selección de características clave o propiedades del objeto de estudio, describiéndolas exhaustivamente dentro de un marco conceptual específico. Este enfoque metodológico es aplicable en cualquier paradigma de investigación.**Fuente especificada no válida.**

Se empleó un enfoque descriptivo para identificar los elementos esenciales del fenómeno investigado, en este caso, el laboratorio de computación. Se detallan aspectos como la configuración del hardware, la efectividad de los procedimientos y la seguridad de la red, entre otros. A partir de la observación y recopilación de datos, se seleccionaron las características críticas que influyen decisivamente en la evaluación y el rendimiento exitoso del laboratorio de computación. (Maria, 2019)

3.4 Fuentes de información de datos

3.5 Fuentes primarias

En las fuentes primarias, el investigador obtiene las mejores pruebas disponibles: testimonios de testigos oculares de los hechos pasados y objetos reales que se usaron en el pasado y que se pueden examinar ahora. Estas fuentes constituyen elementos básicos de la investigación. La fuente primaria es el objeto del estudio y, a falta de éste, el primer registro sobre el mismo, por oposición a cualquier registro derivado de éstos, que se califican como fuentes secundarias. La investigación primaria se basa fundamentalmente en fuente de este tipo, pero recurre también a las fuentes secundarias. (Moguel, 2005)

Entre las fuentes primarias tenemos:

- Las autoridades
- Los equipos dentro del laboratorio

3.6 Fuentes secundarias

El investigador recurre también a las fuentes secundarias, es decir información que proporcionan las personas que no observaron directamente la situación. Las fuentes

primarias y secundarias pueden hacer que el investigador modifique el esquema del problema cuando la información indique que ello es necesario. (Moguel, 2005)

Entre las fuentes secundarias tenemos:

- Los docentes de la institución

3.6.1 Encuestas

Se utilizan dos métodos de investigación cuantitativa muy populares para recopilar datos cuantitativos:

Encuesta: Tradicionalmente, las encuestas se realizaban en formato físico; sin embargo, hoy en día han evolucionado hacia plataformas en línea. Las preguntas cerradas son fundamentales en este proceso, ya que permiten recopilar datos cuantitativos de manera eficiente. Estas preguntas ofrecen opciones de respuesta específicas adaptadas a cada consulta particular. Actualmente, las encuestas son un componente esencial para obtener información de una audiencia más amplia en comparación con los métodos tradicionales. **Fuente especificada no válida.**

La encuesta fue realizada a los docentes de la Unidad Educativa "Dr. José María Velasco Ibarra" con el objetivo de recolectar información sobre el manejo del laboratorio, ya que por medio de la encuesta podemos obtener una información más directa.

3.6.2 Entrevista

La entrevista constituye una técnica de investigación cuantitativa diseñada para obtener información confiable y válida con el fin de probar hipótesis de trabajo. Es esencialmente estructurada y planificada, siguiendo un conjunto de directrices tanto en su preparación como en su aplicación, análisis e interpretación de los datos recogidos. (Mejía, 2014)

La entrevista fue realizada a las autoridades de la institución entre ellos el/la rector/a, la vicerrectora, con la finalidad de obtener información sobre el manejo del laboratorio para confirmar el problema que existe dentro de este.

3.7 Estrategia operacional para la recolección de datos

3.7.1 Población

La población fueron los 24 docentes de la institución, en la cual se recopiló información mediante encuesta y entrevista que sirvieron para confirmar cada una de las causas que se identificaron en el árbol del problema.

3.7.2 Muestra

Esta estrategia no se utilizó porque no existía a cantidad necesaria de docentes para sacar una muestra

3.7.3 Análisis de las herramientas de recolección de datos a utilizar

Esta encuesta está dirigida a los docentes de la institución.

Objetivo: El objetivo de la encuesta es recopilar datos y obtener información específica sobre el estado en que se encuentra el laboratorio de computación, para así obtener un análisis de cada respuesta de los encuestados, esto con la finalidad de confirmar la hipótesis del problema que había dentro del laboratorio de computación.

3.7.3.1 Encuesta

1. ¿Existen políticas de acceso y restricciones para garantizar la seguridad de los laboratorios de computación?

   SI ( ) NO ( )

2. ¿Usted conoce un reglamento para el uso del laboratorio?

   SI ( ) NO ( )

3. ¿Le han socializado el reglamento para el uso del laboratorio?

   SI ( ) NO ( )

4. ¿Existe en el laboratorio instrucciones visibles de cómo manejar los equipos del laboratorio?

   SI ( ) NO ( )

5. ¿Usted conoce el proceso para reportar algún daño dentro del laboratorio?

   SI ( ) NO ( )

6. ¿Considera que el nivel de limpieza en el laboratorio es el adecuado?
   SI ( ) NO ( )

7. ¿Usted considera que los equipos se encuentran en buen estado?
   SI ( ) NO ( )

8. ¿Usted ha observado que se les dé mantenimiento a los equipos del laboratorio?
   SI ( ) NO ( )

9. ¿Cree que la falta de limpieza en el laboratorio podría afectar la calidad de los resultados de las pruebas?
   SI ( ) NO ( )

10. ¿Cree que el mal estado de la infraestructura eléctrica podría representar un riesgo para la seguridad?
    SI ( ) NO ( )

11. ¿Se lleva a cabo un mantenimiento regular de la infraestructura eléctrica?
    SI ( ) NO ( )

12. ¿Considera que los cables del laboratorio están debidamente organizados?
    SI ( ) NO ( )

13. ¿Usted conoce si la institución cuenta con políticas de acceso al laboratorio?
    SI ( ) NO ( )

14. ¿Usted ha observado si en el laboratorio existen equipos que están fuera de servicio y siguen dentro del laboratorio?
    SI ( ) NO ( )

3.7.3.2 Entrevista

Esta entrevista está dirigida a: Los docentes que conforman la máxima autoridad de la institución

Objetivo: El objetivo de la entrevista para extraer información de forma directa y detallada sobre el manejo y control del laboratorio de computación, mediante la entrevista también se verificará los procedimientos y controles, para así confirmar la existencia del problema que existía dentro del laboratorio de computación.

1. ¿Cómo describiría las condiciones actuales del laboratorio de computación?

2. ¿Han reportado los docentes los problemas técnicos que han encontrado en el laboratorio?

3. ¿Cuáles son los problemas técnicos más comunes que han enfrentado dentro del laboratorio?

4. ¿Qué medidas de seguridad se implementan para proteger la información y datos almacenados en las computadoras del laboratorio?

5. ¿Cómo se gestionan las actualizaciones de software en las computadoras del laboratorio?

6. ¿Cómo se gestiona y controla el acceso a Internet en el laboratorio de computación?

7. ¿Existen restricciones de uso de Internet para los estudiantes?

8. ¿Existen políticas claras sobre el uso de los equipos en el laboratorio de computación?

9. ¿Se realiza algún tipo de mantenimiento preventivo en las computadoras del laboratorio?

10. ¿Con qué frecuencia se lleva a cabo este mantenimiento dentro del laboratorio?

    _____

    _____

11. ¿Existe un plan de contingencia en caso de fallas significativas en el laboratorio de computación?

    _____

    _____

3.7.3.3 Estructura de los instrumentos de recolección de datos aplicados

3.7.4 Plan de recolección de datos

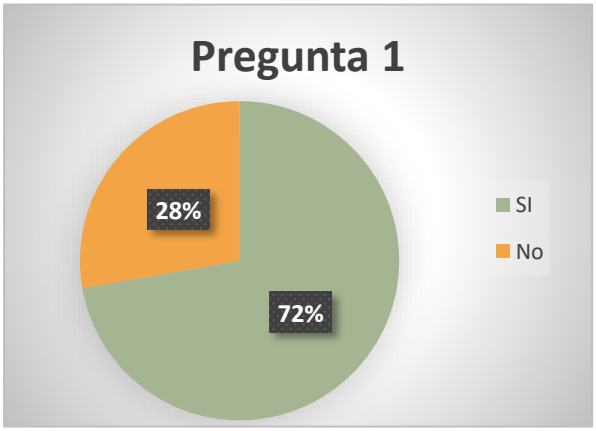
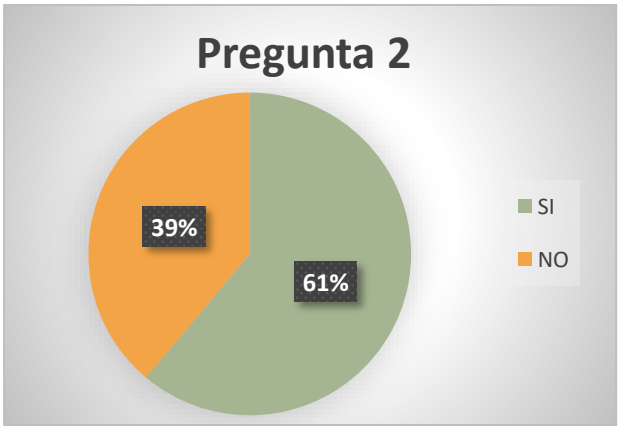
FECHA	ACTIVIDAD	OBSERVACIÓN
05/01/2024	Se realizó una visita a la institución para coordinar que día se iba a realizar la encuesta y entrevista	Reunión con la rectora de la institución
08/01/2024	Se realizó la encuesta a los docentes.	Todos los docentes aceptaron la encuesta
24 /01/2024	Se realizo la entrevista a las autoridades de la institución.	Las autoridades aceptaron dar la entrevista

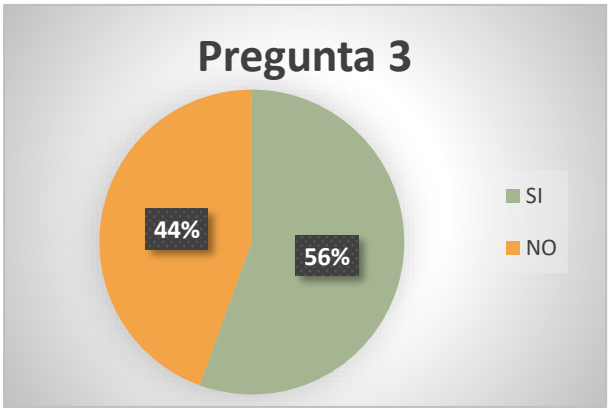
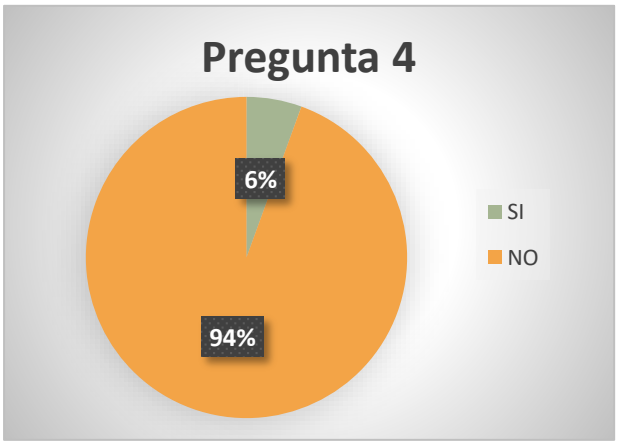
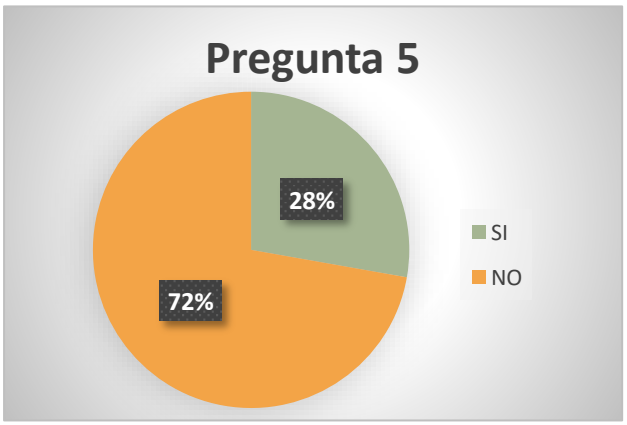
Tabla 1 Plan de recolección de datos

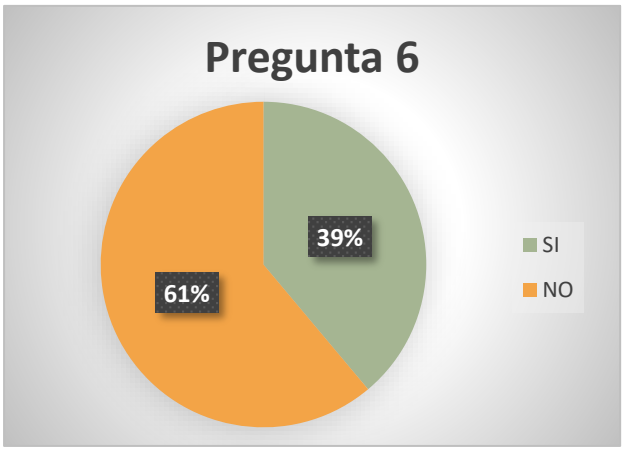
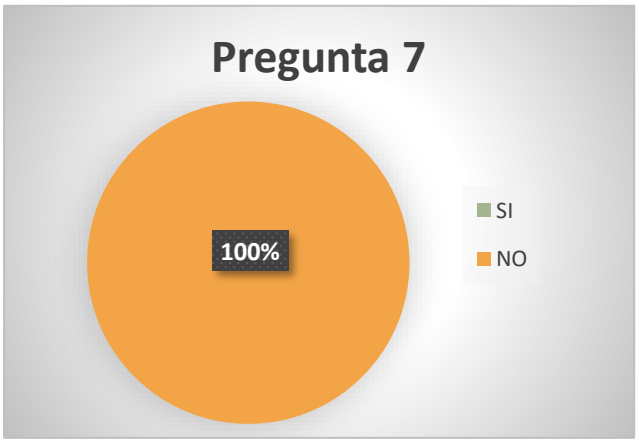
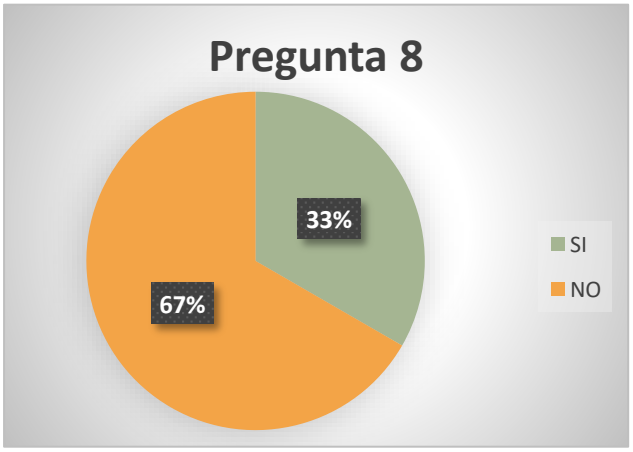
3.8 Análisis y presentación de resultados

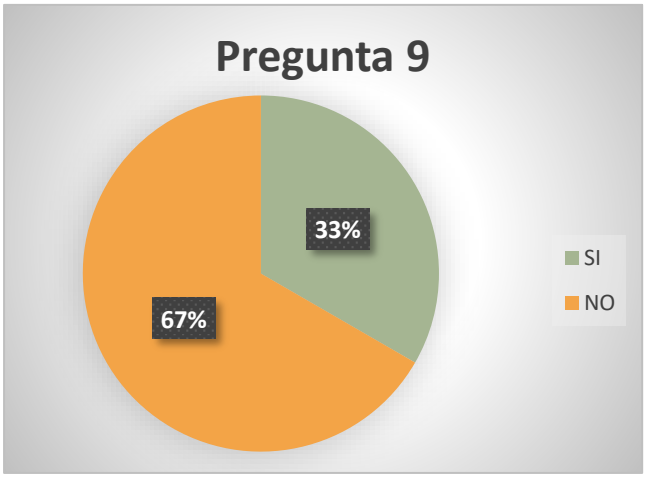
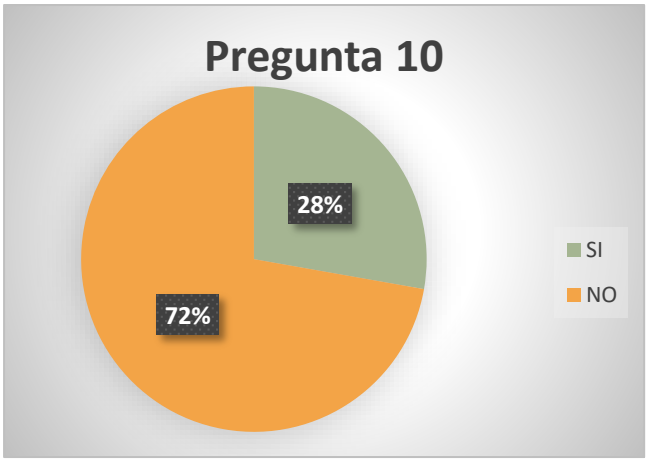
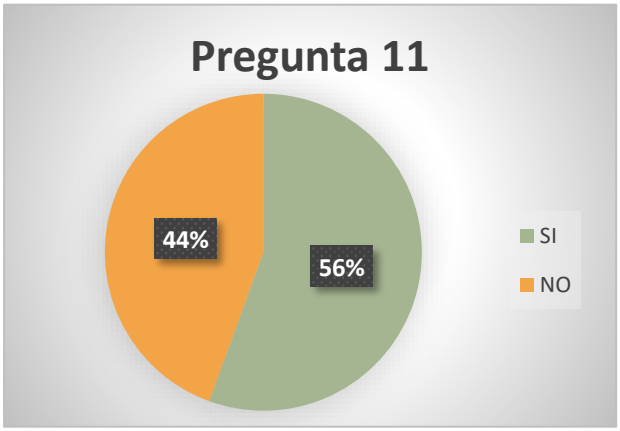
3.8.1 Presentación y descripción de los resultados obtenidos

3.8.1.1 Análisis de datos obtenidos a través de la encuesta

Pregunta	Respuesta	Interpretación
1). ¿Existen políticas de acceso y restricciones para garantizar la seguridad de los laboratorios de computación?		Según la encuesta que se realizó a los docentes, casi tres cuartas partes de los docentes encuestados manifiestan que la institución si cuentan con políticas de seguridad.
2). ¿Usted conoce un reglamento para el uso del laboratorio?		A través de la encuesta que se realizó a los docentes, un poco más de la mitad si conocen el reglamento para el uso del laboratorio.

Pregunta	Respuesta	Interpretación
3). ¿Le han socializado el reglamento para el uso del laboratorio?		Por medio de la encuesta que se realizó a los docentes, casi la mitad de ellos si les han socializado el reglamento del uso del laboratorio.
4). ¿Existe en el laboratorio instrucciones visibles de cómo manejar los equipos del laboratorio?		Según las respuestas de los docentes, casi la totalidad considera que no existen instrucciones visibles sobre el manejo de los equipos.
5). ¿Usted conoce el proceso para reportar algún daño dentro del laboratorio?		Como resultado de las encuestas tenemos que la mayor parte de los docenes no conocen el proceso para reportar los daños en el laboratorio.

Pregunta	Respuesta	Interpretación
6). ¿Considera que el nivel de limpieza en el laboratorio es el adecuado?		A través de la encuesta que se realizó a los docentes, más de la mitad considera el nivel de limpieza en el laboratorio no es adecuado.
7). ¿Usted considera que los equipos se encuentran en buen estado?		Como resultado tenemos que todos los docentes consideran que los equipos no se encuentran en buen estado.
8). ¿Usted ha observado que se les dé mantenimiento a los equipos del laboratorio?		Según la encuesta que se realizó a los docentes tenemos que, más de la mitad de los docentes no han observado el que el laboratorio haya recibido mantenimiento.

Pregunta	Respuesta	Interpretación
9). ¿Se lleva a cabo un mantenimiento regular de la infraestructura eléctrica?		Como resultado de las encuestas tenemos que, el mayor porcentaje de los docentes no han observado que el laboratorio tenga un mantenimiento de la infraestructura eléctrica.
10). ¿Considera que los cables del laboratorio están debidamente organizados?		Según los resultados de la encuesta tenemos que casi la tercera parte de los docentes consideran que los cables no están debidamente organizados
¿Usted conoce si la institución cuenta con políticas de acceso al laboratorio?		A través de la encuesta que se realizó tenemos que un poco más de la mitad de los docentes si conocen que en la institución hay políticas de acceso al laboratorio.

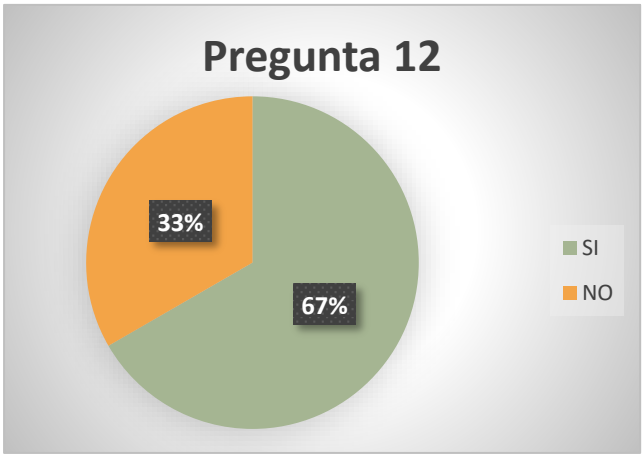
Pregunta	Respuesta	Interpretación
¿Usted ha observado si en el laboratorio existen equipos que están fuera de servicio y siguen dentro del laboratorio?		Como resultado de la encuesta que se realizó tenemos que más de un cuarto de los docentes no han observado que en el laboratorio siguen estando los equipos que están fuera de servicio

Tabla 2 Análisis de datos a través de encuesta

3.8.1.2 Análisis de datos obtenidos a través de la entrevista

Pregunta	Respuesta	Respuesta	Respuesta	Interpretación
1. ¿Cómo describiría las condiciones actuales del laboratorio de computación?	No funcionan casi ninguna de las computadoras y el proyecto también está en funcionamiento	La estructura física en buen estado, pero las computadoras están en pésimo estado, casi todas están dañadas.	Las condiciones en las que se encuentran las computadoras del laboratorio no son buenas, están ahí las computadoras, pero no están en funcionamiento.	Según la entrevista realizada se puede verificar que el laboratorio no está en buenas condiciones y que las computadoras están en pésimo estado y pocas son las que funcionan.
2. ¿Han reportado los docentes los problemas técnicos que han encontrado en el laboratorio?	Desde el año anterior habían realizado reportes de forma verbal, pero empezaron estos reportes cuando había los apagones	Si, a través de reportes verbales nos han comunicado que las computadoras no funcionan	Si lo hacen, pero no podemos hacer nada ya que la institución no cuenta con ingresos, ni tampoco con ayuda del distrito.	Se puede observar mediante la entrevista realizada, que los docentes si reportan los problemas técnicos dentro del laboratorio, pero no pueden hacer nada ya que no cuentan con ingresos ni ayuda del distrito.

Pregunta	Respuesta	Respuesta	Respuesta	Interpretación
3. ¿Cuáles son los problemas técnicos más comunes que han enfrentado dentro del laboratorio?	Fallos en cada una de las computadoras, esto se daba ya que a algunas se les habían dañado los cables, este problema se da ya que no recibe mantenimiento de continuo.	Las computadoras no funcionan, ese el problema más común que han enfrentado por eso últimamente no se le está dando uso a los equipos.	Desprogramación de las computadoras, viene a veces y les ponen programas y luego esos programas vuelven a fallar, pero esto pasa porque no se lleva un mantenimiento preventivo, por ese caso existen varias computadoras que han dejado de funcionar	A través de la entrevista a las autoridades, se puede notar que entre los problemas más comunes en el laboratorio es que las computadoras no se da mantenimiento y se desprograman y mediante esto varios equipos han dejado de funcionar
4. ¿Qué medidas de seguridad se implementan para proteger la información y datos almacenados en las computadoras del laboratorio?	Todas las computadoras tienen bloqueos a paginas prohibidas, y además se tenía acceso a las demás computadoras desde una maquina principal que controlaba las demás.	No se han implementado ninguna medida de seguridad porque los docentes no utilizan las computadoras para guardar su información, los equipos solamente lo utilizan los estudiantes para hacer consultas o	No se utiliza las computadoras del laboratorio para guardar información de los docentes, las computadoras se utilizan para enseñarles cosas básicas a los estudiantes, como utilizar Word y PowerPoint que los estudiantes realicen alguna	Según la entrevista realizada a las autoridades, las maquinas no tienen bloqueo a páginas prohibidas y los docentes tampoco utilizan las computadoras del laboratorio para guardar información,

		realizar algún trabajo de PowerPoint	investigación y ellos mismo traen sus memorias USB para guardar su información.	solamente utilizan los equipos para que los estudiantes realicen investigaciones.
Pregunta	**Respuesta**	**Respuesta**	**Respuesta**	**Interpretación**
5. ¿Cómo se gestionan las actualizaciones de software en las computadoras del laboratorio?	La última actualización fue realizada hace dos años, desde ese tiempo no ha recibido ningún mantenimiento.	No se realizan actualizaciones porque no hay un docente encargado que lleve a cabo este procedimiento	Se les ha realizado las observaciones al ing. de las Tics del distrito para que realicen un mantenimiento, esto con respecto a que a veces las computadoras dejan de funcionar por falta de actualizaciones, pero ellos no prestan atención a nuestros pedidos, ya que les dan prioridad a otras instituciones más cercanas.	Según la entrevista realizada a los docentes, se puede observar que, si han reportado al distrito para que realicen mantenimiento incluido las actualizaciones, pero en el distrito no les brindan ayuda.
6. ¿Cómo se gestiona y controla el acceso a Internet en el laboratorio de computación?	El internet se gestiona por medio conexión inalámbrica ya que los cables de internet que se conectaban a	Se lleva a cabo a través de conexión inalámbrica ya que no cuentan con cables para la conexión por	Por general casi ninguna computadora tiene internet por cable, solamente se hacen las conexiones vía	Como podemos observar a través de la entrevista que ninguna de las computadoras no tiene internet

	cada computadora se dañaron y otros se extraviaron.	cable.	inalámbrica, pero se les desactiva después que terminan de utilizarlas.	por cable solamente utilizan conexiones vía inalámbrica.
7. ¿Existen restricciones de uso de Internet para los estudiantes?	Si hay restricciones, no les permitimos que ellos tengan conexiones en sus dispositivos, pero varias ocasiones la contraseña se filtra y ellos vuelven a tener internet en sus dispositivos.	Si existen restricciones, pero ellos de cualquier manera buscan la forma de obtener la clave.	Si hay restricciones para los estudiantes, pero ellos buscan la forma de conseguir la clave y volver a tenerlas, pero ahora se está utilizando el método de quitar los teléfonos celulares para tratar de controlar un poco la situación.	Por medio de la entrevista realizada, podemos observar que los docentes si restringen el uso de internet a los estudiantes, pero los estudiantes buscan la forma de volver a tener la clave.
8. ¿Existen políticas claras sobre el uso de los equipos en el laboratorio de computación?	Si hay un manual, y algunas veces se les ha socializado a los estudiantes, pero ellos no se rigen a las políticas	Si hay políticas y se ha socializado a los estudiantes que utilizan las computadoras, pero ellos no rigen a las políticas y apagan las computadoras desconectándolas desde el tomacorriente y	Hay un manual de procedimientos de como prender y apagar las computadoras, siempre se les enseña esto a los estudiantes antes de utilizar el laboratorio, pero en el estado que se encuentra ahora es	Según la entrevista vemos que en la institución si hay políticas sobre el uso de los equipos, que incluso les enseñan a los estudiantes a cómo utilizar los equipos en el

		eso ocasiona que de dañen	difícil enseñar cada una de estas políticas.	laboratorio.
9. ¿Se realiza algún tipo de mantenimiento preventivo en las computadoras del laboratorio?	No tenemos personal que se encargue de gestionar el mantenimiento de los equipos.	No ya que no contamos con un laboratorista que lleve a cabo estos procesos.	No hay personal encargado que este al frente del laboratorio para que maneje la parte de darle mantenimiento, y como dije enante, ya ha reportado varias veces sobre esto al distrito, pero no tenemos respuestas.	A través de la entrevista realizada tenemos que en la institución no hay un docente encargado del laboratorio, y no se puede llevar a cabo un mantenimiento ya que nadie se hace responsable de los equipos.
10. ¿Con qué frecuencia se lleva a cabo este mantenimiento dentro del laboratorio?	No se ha realizado mantenimiento a las computadoras desde hace casi 5 años.	Estos equipos llevan varios años sin recibir mantenimiento la última vez que le hicieron el mantenimiento fue antes de la pandemia y hasta el momento no han vuelvo a ser revisado.	El ultimo mantenimiento que se realizó fue antes de la pandemia, fue entre el 2018 o 2019, y desde ese entonces estas máquinas ya no han recibido ningún mantenimiento y esto ha hecho que las computadoras empiecen a deteriorarse.	Según la entrevista realizada podemos observar que el laboratorio de computación tiene varios años sin recibir mantenimiento y por este motivo las computadoras se han deteriorado.

Tabla 3.Análisis de datos a través de la entrevista

3.8.1.3 Presentación y descripción de los resultados obtenidos

Una vez realizado los cuestionarios se preguntó a los docentes mediante una encuesta referida a las causas entre las ellas tenemos que no se restringe el acceso a los equipos del laboratorio y mediante la encuesta en la pregunta cuatro se preguntó que si se restringía el acceso a los equipos del laboratorio el 72% de los docentes supieron manifestar que, si había políticas, pero no las ponen en prácticas

Otra de las causas que se pudo evidenciar fue sobre la falta de limpieza en el laboratorio, a través de la encuesta en la pregunta seis donde se preguntó sobre el nivel de limpieza en el laboratorio el 61% los docentes supieron manifestar que el nivel de limpieza no es el adecuado

También otras que las causas que se pudo evidenciar fueron cuando se preguntó sobre la falta de políticas de seguridad en la pregunta once de la encuesta se preguntó si la institución contaba con políticas de seguridad el 56% de los docentes supieron decir que, si existen políticas, pero desconocen de ellas ya que no ha sido socializadas

También otra de las causas que se pudo evidenciar fue sobre el mal estructurado eléctrico en la pregunta diez de la encuesta se preguntó si los cables estaban debidamente organizados y el 72% de los docentes supieron manifestar que los cables no están correctamente organizados y esto puede ocasionar daños

Otra de las causas que se pudieron identificar eran sobre el descontrol total en el uso del laboratorio para justificar esta causa tenemos la pregunta doce donde se pregunta si dentro del laboratorio aún existen equipos que están fuera de servicio y siguen en el laboratorio, y el 67% de los docentes supieron manifestar que si hay equipos que siguen dentro del laboratorio que están fuera de servicio.

3.8.2 Informe final del análisis de los datos

A través de la investigación que se realizó por medio de entrevista y encuesta y pudo evidenciar del problema que existe dentro del laboratorio, por este motivo es necesario realizar brindar una ayuda a la institución por medio de la auditoría, ya que por medio de esta

se podrá verificar que existe un problema dentro del laboratorio y se podrá establecer sugerencias del manejo de los equipos para llevar una buena administración y que los equipos no se sigan deteriorando, ya que el buen funcionamiento del laboratorio beneficia tanto a los docentes como a los estudiantes en el aprendizaje por este motivo es importante investigar para conocer los problemas que afronta y como se pueden solucionar.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

En el entorno actual de rápido evolución tecnológica, la seguridad y la gestión eficiente de la infraestructura tecnológica son cruciales para la continuidad y el éxito de cualquier organización. Esta investigación se enfoca en el análisis de riesgos de la infraestructura del laboratorio de la Unidad Educativa “Dr. José María Velasco Ibarra”, con el propósito de identificar los activos críticos, identificar las amenazas y evaluar los activos, amenazas, estimar el impacto y el nivel de riesgo.

El análisis de riesgos es un proceso fundamental que permite identificar los peligros que comprometen la seguridad del laboratorio de computación y determinar su magnitud y destacar las áreas que requieren intervención rápida. A través del estudio realizado ser han identificado los activos importantes, los cuales serán evaluadas para medir que tan expuestos están y medir el impacto y riesgo.

Para abordar la problemática identificada, se ha planteado una solución integral en el cual se incluye la recopilación de información de entrevista y encuesta, herramientas que son imprescindible para obtener datos útiles y precisos sobre las vulnerabilidades del laboratorio.

4.2 Descripción de la propuesta

4.2.1 Propósito

El análisis de riesgo de la infraestructura tecnológica se llevó a cabo con la finalidad de identificar los activos relevantes para la organización, determinar las amenazas a las que están expuestos los equipos y la infraestructura del laboratorio de computación y estimar el nivel de impacto de las amenazas y el nivel de riesgo de los activos.

4.2.2 Ámbito del análisis de riesgo

El análisis de riesgos consiste en identificar los peligros que pueden comprometer la seguridad de la información, evaluar su magnitud y determinar las áreas que requieren medidas de protección. Este estudio ha permitido identificar los activos relevantes o críticos para la organización, reconocer las amenazas a las que están expuestos estos activos, evaluar su magnitud (impacto y riesgo) y, con base en ello, determinar las salvaguardas necesarias para mitigar el impacto de dichas amenazas. El resultado obtenido no solo incluye el análisis y valoración de riesgos, sino también la elaboración de un Plan de Mantenimiento Preventivo de Equipos Informáticos, cuyo objetivo es detectar y solucionar problemas técnicos antes de que provoquen la indisponibilidad del equipo.

4.2.3 Perspectiva análisis de riesgo

Con base en la problemática identificada en la investigación, se propuso la solución más adecuada para alcanzar los objetivos establecidos y prevenir ataques informáticos en la institución. Para ello, se recopiló información esencial mediante encuestas y entrevistas, que proporcionaron datos útiles y precisos sobre el problema a resolver.

Tras analizar las vulnerabilidades y aplicar los controles de la norma correspondiente, el siguiente paso será elaborar un manual de usuario. Este manual detallará las

vulnerabilidades detectadas, los peligros a los que está expuesta la infraestructura, y los pasos a seguir para implementar buenas prácticas de seguridad dentro de la institución.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recursos	Función	Actividad
1	Ing. Clara Guadalupe Pozo Hernández	Tutora del proyecto de Titulación	Colaboradora que brindará orientación al estudiante encargado del proyecto
1	Ing. Karina Toala	Rectora de la Institución donde se realizará el proyecto.	Informante clave
1	Lic. Genita Bravo	Vise rectora de la Institución	Informante clave
1	Lic. Nery Mendoza	Inspector	Informante clave
1	Lic. Andrea Loor	Secretaria	Informante clave
18	Docentes de la institución	Impartir clases	Participaron en las encuestas para identificación de problemática
1	Josias Daniel Alcivar Marcillo	Llevar a cabo el cumplimiento del proyecto de	Investigación

		titulación.	

Tabla 4. Determinación de recursos. Humanos

4.3.2 Tecnológicos

Cantidad	Recurso	Actividad
1	Portátil lenovo core i7 12 GB de RAM	Equipo informático utilizado para el desarrollo de la investigación.
1	Teléfono	Recopilar información
1	Impresora EpsonL380	Realizar impresión
1	Cámara	Tomar fotografías
1	Office	Word para realizar el proyecto
1	Conexión de internet	Para realizar las investigaciones

Tabla 5. Determinación de recursos. Tecnológicos

4.3.3 Económicos

Cantidad	Descripción	Precio Unitario	Subtotal
10	Transporte	1	10
1	Portátil lenovo core i5 12 GB de RAM	600	600
1	Teléfono	300	300

Cantidad	Descripción	Precio Unitario	Subtotal
1	Impresora EpsonL380	300	300
1	Paquete de 500 hoja para impresión	5	5
1	Office		
1	Conexión de internet	25	25
		Total	1240$

Tabla 6. Determinación de recursos. Económicos

4.3.4 Planificación

4.3.5 Programa de auditoria

Programa de auditoría física para la identificación de riesgos en el laboratorio de computación de la Unidad Educativa "Dr. José María Velasco Ibarra"			
Objetivos: 1. Identificar los riesgos de seguridad física del Laboratorio de la Unidad Educativa "Dr. José María Velasco Ibarra" 2. Evaluar el nivel de seguridad informática física del Laboratorio de la Unidad Educativa "Dr. José María Velasco Ibarra"			
TÉCNICAS Y PROCEDIMIENTOS	REF. A PAPEL DE TRABAJO	FECHA	RESPONSABLE
1.1 Identificación de activos	C1	07/05/0224	Josias Alcivar

1.2 Valoración de activos	C1	16/05/2024	Josias Alcivar
1.3 Cuestionario para analizar riesgos	C1	20/05/2024	Josias Alcivar
1.4 Realizar entrevista a la Rectora de la institución	C1	10/06/2024	Josias Alcivar
1.5 Inspección del laboratorio	C1	10/06/2024	Josias Alcivar
2.1 Analizar cuestionario e identificar riesgos	A1	18/06/2024	Josias Alcivar
2.2 Analizar riesgos y calcular impacto	A2	19/06/2024	Josias Alcivar
2.3 Valoración de riesgo	A3	19/06/2024	Josias Alcivar
2.4 Elaborar plan de medida	A4	09/07/2024	Josias Alcivar
2.6 Elaborar informe	I1		Josias Alcivar
Realizado por:		Revisado por:	
Conclusiones: Observaciones:			

Tabla 7. Programa de Auditoría

4.4 Desarrollo (Análisis de riesgo)

Para el presente trabajo se utilizó la metodología MAGERIT, que es una metodología que está enfocada al análisis y gestión de riesgos informáticos, esta metodología se ofrece como marco y guía y para determinar los riesgos informáticos. (Ppito, 2017)

La metodología MAGERIT establece 6 fases para el desarrollo del análisis de riesgo, en cual no se utilizarán salvaguardas y riesgo residual por motivo que solo se realizará una guía y después la institución debería implementar esas medidas y en un futuro volver a evaluar riesgos para verificar si fueron efectivas o no, en las cuales solo se aplicarán las siguientes:

- Identificación y Valoración Activos.
- Identificación de Amenazas.
- Valoración de Riesgos

- Impacto residual.

4.4.1 Identificación de activos

Cada organización tiene activos y recursos que representan los valores y necesidades de la organización. Estos activos y recursos se pueden dividir en capas: código, nombre, descripción, características, modelo, cantidad, encargado.

Nº	Código	Nombre	Descripción	Característica	Modelo	Cantidad	Encargado/a
1	932F2H	PC DESKTOP	Equipo que se utiliza para realizar tareas, y otros trabajos de oficio.	Intel(R) Celeron(R) CPU N2820 @2.13GHz 2.13 GHz	LG	20	Lic. Karina Toala
2	PI122	Mouse	Dispositivo de entrada diseñado para manipular objetos en la pantalla	Rating 5V, 100mA 3D Optical Mouse	Speedmind	15	Lic. Karina Toala
3	7260HMW BN	Intel NUC	Intel NUC es un barebone dentro de una caja de muy pequeñas dimensiones.	Salida de gráficos Mini-DP 1.2; Mini-HDMI 1.4a. Cantidad de pantallas admitidas 3.	DN2820FYK	20	Lic. Karina Toala

Nº	**Código**	**Nombre**	**Descripción**	**Característica**	**Modelo**	**Cantidad**	**Encargado/a**
4	TP-Link_D8BA	Router tp-link	Equipos que permiten la conexión a internet entre los usuarios	Velocidad de transmisión Inalámbrica de 300Mbps ideal tanto para las tareas sensibles a banda ancha y trabajo básico	TL-WR844N	1	Lic. Karina Toala
5	1110630	Sistema de Alarma	Alarma de incendio y antirrobo	Es capaz de controlar hasta 28 zonas inalámbricas vía radio	Visonic	1	Lic. Karina Toala
6	AX1800 Wi-Fi 6 GPON VoiP	Router tp-link	Conectividad: 1 SC/APC PON Port 4 puertos Gigabit LAN Ethernet.	Wi-Fi: Wi-Fi 6 AX1800 1201 Mbps (5 GHz) + 574 Mbps (2,4 GHz).	XX230v	1	Lic. Karina Toala

No	Código	Nombre	Descripción	Característica	Modelo	Cantidad	Encargado/a
7	291Q-32N	Regulador de voltaje Forza	Evita que los equipos se dañen a causa de una descarga eléctrica	- Proteje la energía de sus equipos periféricos y ahorra espacio en su oficina.	Capacidad: 100VA/500W Voltaje nominal: 110V	14	Lic. Karina Toala
8	S34F54	Aire acondicionado LG	Mantener fresco el área del laboratorio	Ventana de 1 t y 220 v.	Midea	1	Lic. Karina Toala
9	100-240V	Proyector EPSON	Proyectar o mostrar imágenes fijas o en movimiento	Excelente calidad. Lámpara con una duración hasta de 10.000 horas3 Conectividad avanzada	H854A	1	Lic. Karina Toala

Tabla 8. Identificación activos Hardware

Nº	**Código**	**Nombre**	**Tipo**	**Características**	**Descripción**	**Licencia**	**Versión**	**PC que cuentan con el programa**	**Encargado/a**
1	00425-0000-00002-AA567	Windows	Sistema Operativo Windows10 64 bits	*Intel(R) Celeron(R) CPU N2820 @2.13GHz 2.13 GHz*	Permite manejar recursos físicos y programas	Gratuita	1809	10	Lic. Karina Toala
2	1002912CV2	Canva	Educativa	Gratuita Pagada	Es una aplicación de edición gratuita que se puede usar computadora y te permite crear diferentes tipos de arte.	Software comercial	2.5	4	Lic. Karina Toala

Nº	**Código**	**Nombre**	**Tipo**	**Licencia**	**Descripción**	**Modelo de desarrollo**	**Versión**	**PC que cuentan con el programa**	**Encargado/a**
3	9392111	Chat GTP	prototipo	privativa	Es una App AI que está diseñada para resolver preguntas por los usuarios.	OpenAI		7	Lic. Karina Toala
4	45034	Adobe Acrobat	Autoedición	Acrobat Pro: Comercial Acrobat reader: freeware	Es el único visor de PDF gratuito que permite abrir e interactuar con todos los tipos de contenido PDF	Adobe	24.002.20759	10	Lic. Karina Toala

Nº	**Código**	**Nombre**	**Tipo**	**Licencia**	**Descripción**	**Modelo de desarrollo**	**Versión**	**PC que cuentan con el programa**	**Encargado/a**
5	00425	Chrome	Navegador Web	Gratuita	Es un navegador multiplataforma que utilizan los usuarios para realizar sus tareas.	Google	124.0.6367.60	10	Lic. Karina Toala
6	02360	Firefox	Navegador Web	Gratuita	Es multiplataforma ya que permite al usuario realizar varias tareas.	Mozilla Foundation	123.0	3	Lic. Karina Toala

Nº	**Código**	**Nombre**	**Tipo**	**Licencia**	**Descripción**	**Modelo de desarrollo**	**Versión**	**PC que cuentan con el programa**	**Encargado/a**
7	00425	Opera Internet Browser	Navegador Web	Gratuita	Navegador que se utiliza para realizar investigaciones.	Opera Software ASA	109.0.5097.59	2	Lic. Karina Toala
8	00425	Zoom Meetings Installer	Software VolP	Freemium, software propietario	App que se utiliza para realizar llamadas, presentar trabajos de forma que el usuario pueda verla.	Zoom Video Communications	5.17.10	1	Lic. Karina Toala

Nº	**Código**	**Nombre**	**Tipo**	**Licencia**	**Descripción**	**Modelo de desarrollo**	**Versión**	**PC que cuentan con el programa**	**Encargado/a**
9	00425	Glary Utilities	Herramienta para mantenimiento de archivos	Gratis	Ayuda al equipo a optimizar su uso	GlarySoft	5.206.0.235	1	Lic. Karina Toala
10	091103	PC Manager	Mantenimiento	Gratis	es un programa creado por Microsoft para limpiar internamente Windows en el ordenador.	Microsoft	3.1.1.0	4	Lic. Karina Toala

Nº	**Código**	**Nombre**	**Tipo**	**Licencia**	**Descripción**	**Versión**	**PC que cuentan con el programa**	**Encargado/a**
11	A32V4DS	AVG	Antivirus	Gratuita	Es un programa antivirus detección de amenazas, protección contra virus	21.6.3189	6	Lic. Karina Toala

Nº	Código	Nombre	Tipo	Licencia	Descripción	Versión	PC que cuentan con el programa	Encargado/a
12	00414-50000-00000-AA688	Microsoft Office (Word, Power Point, Excel)	Herramientas de ofimática	Office 19	Es un conjunto de herramientas destinadas a la creación, edición, almacenamiento y transmisión de información.	Office 16	10	Lic. Karina Toala

Tabla 9. Identificación activos Software

1

4.4.2 Valoración de activos

Una vez identificados los activos de la organización, procedemos a evaluarlos en las tres dimensiones de la seguridad de la información: confidencialidad, integridad y disponibilidad. Esto implica determinar su valor asignando una puntuación en un rango del 1 al 5, según su nivel de importancia.

Valor		Criterio
5	Extremo	Muy valioso
4	Muy Alto	Valioso
3	Alto	Medianamente valioso
2	Medio	Poco valioso
1	Bajo	Insignificante

Tabla 10. Tabla de Valoración de activos

ACTIVOS DEL HARDWARE					
ACTIVO		**VALORACIÓN DE ACTIVO**			
CÓDIGO	**NOMBRE**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**
932F2H	PC DESKTOP	2	5	5	4.00
7260HMW BN	Intel NUC	4	5	5	4.66
TP-Link_D8BA	Router tp-link	4	5	4	4.33
1110630	Sistema de Alarma	2	5	5	4.00
AX1800 Wi-Fi 6 GPON VoiP	Router tp-link	5	5	4	4.66
54545-777	Regulador de voltaje Forza	1	2	5	2.66
SSTL-88	Aire acondicionado LG	1	1	1	1.00
100-240V	Proyector EPSON	1	1	1	1.00

ACTIVOS DEL SOFTWARE					
ACTIVO		**VALORACIÓN DE ACTIVO**			
CÓDIGO	**NOMBRE**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**
00425-0000-00002-AA567	Windows	4	4	5	4.33
00414-50000-00000-AA688	Microsoft Office (Word, Power Point, Excel)	5	4	5	4.33
	Canva	2	1	2	1.66
	AVG	5	1	3	4.00
	ChatGTP	1	1	2	1.66
	Adobe Acrobat	1	1	5	2.33
	Chrome	4	4	5	4.33
	Firefox	4	3	3	3.33
	Opera Internet Browser	3	3	1	2.33
	Zoom Meetings	1	1	1	1.00
	Glary Utilities	3	2	2	3.00
	PC Manager	1	1	3	3.66

Tabla 11. Valoración de activos Hardware y Software

4.4.3 Identificación de Amenazas

Después de identificar los activos o recursos que requieren protección, es necesario evaluar las amenazas a las que estos están expuestos. A continuación, se debe determinar contra qué amenazas se debe proteger a los activos, considerando la probabilidad de que ocurran. Las amenazas se pueden categorizar en cuatro tipos principales: naturales, de origen industrial, errores y fallos no intencionados, y ataques deliberados.

ACTIVOS (HARDWARE)	AMENAZAS
PC DESKTOP	- Daños del equipo - Robos - Incendio
Intel NUC	- Daños del equipo - Robo - Incendio
Router tp-link	- Daños del equipo - Robo - Incendio
Sistema de Alarma	- Daños del equipo - Incendio - Incendio
Router tp-link	- Daños del equipo - Robo - Incendio
Regulador de voltaje Forza	- Daños del equipo - Robo - Incendio
Aire acondicionado LG	- Daños del equipo - Robo - Incendio
ACTIVOS (SOFTWARE)	**AMENAZAS**
Windows	- Malware - Phishing
Microsoft Office (Word, Power Point, Excel)	- Phishing - Malware
Canva	- Phishing - Malware
AVG	- Phishing
ChatGTP	- Phishing
Adobe Acrobat	- Phishing
Chrome	- Malware - Phishing -

Firefox	- Malware - Phishing
Opera Internet Browser	- Malware - Phishing
Zoom Meetings	- Phishing
Glary Utilities	- Phishing - Malware
PC Manager	- Phishing - Malware

Tabla 12. Identificación de Amenazas de los activos (Hardware uy software)

4.4.3.1 Cuestionario para analizar los riesgos

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 1- 5

- **Robo**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿El laboratorio de computación cuenta con cerraduras en las puertas?			
2. ¿Hay cámaras de seguridad instaladas en el laboratorio y sus alrededores?			
3. ¿Existen detectores de movimiento en el laboratorio?			
4. ¿Las ventanas del laboratorio tienen rejas o algún tipo de protección?			
5. ¿El acceso al laboratorio está restringido al personal no autorizado?			
6. ¿Se realiza un registro de las personas que entran y salen del laboratorio?			
7. ¿Hay personal de seguridad que supervise el laboratorio?			
8. ¿Se cuenta con un sistema de alarma en caso de intrusión?			
9. ¿Los equipos están anclados o asegurados físicamente para evitar su fácil sustracción?			
10. ¿Se realizan inspecciones regulares de los equipos y del inventario del laboratorio?			
11. ¿Se realiza mantenimiento regular a los sistemas de seguridad física?			
12. ¿El área del laboratorio está completamente cerrada?			
13. ¿Se monitorean y controlan las salidas de emergencia y otras vías de escape durante el horario de operación del laboratorio?			
14. ¿Se revisan regularmente las cerraduras y sistemas de seguridad del laboratorio?			
15. ¿Las computadoras tienen configurado el bloqueo automático tras un periodo de inactividad?			
16. ¿Se realiza un registro de las actividades de los usuarios en las computadoras?			
17. ¿El laboratorio cuenta con acceso mediante tarjeta al personal autorizado?			
18. ¿El laboratorio ha sido víctima de robos?			
19. ¿Existe un plan de respuesta a incidente que se activan en caso de robo y acceso no autorizado?			
20. ¿Existe un registro de los incidentes relacionados con robos o intentos de robo en el laboratorio?			
21. ¿Realizan capacitaciones para la concientización al personal sobre las pérdidas y protocolos en caso de robo?			
22. ¿La infraestructura del laboratorio es segura?			
23. ¿Cuentan con políticas para el manejo de llaves y acceso al laboratorio?			
24. ¿Están los equipos de computación asegurados físicamente (con cadenas de seguridad, soportes de anclaje, etc.) para prevenir su robo?			
25. ¿Cuentan con un laboratorista que sea responsable de cuidar el laboratorio?			

REALIZADO POR:	REVISADO POR:
FECHA:	FECHA:

CONCLUSIONES

OBSERVACIONES

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 2-5

- **Daños de equipo**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿Se realiza un mantenimiento preventivo regular de los equipos?			
2. ¿Existe un registro de mantenimiento y reparaciones de cada equipo?			
3. ¿Los dispositivos que se conectan a los equipos recibe una revisión mediante antivirus antes de ser conectados a los equipos del laboratorio?			
4. ¿Se utilizan herramientas y métodos adecuados para la limpieza de los equipos?			
5. ¿Los usuarios reciben capacitación sobre el manejo adecuado de los equipos?			
6. ¿Se utilizan fundas o protecciones para los equipos cuando no están en uso?			
7. ¿Los equipos están correctamente etiquetados e inventariados?			
8. ¿Hay políticas para el uso adecuado y responsable de los equipos?			
9. ¿Se realizan inspecciones periódicas para detectar daños o desgaste en los equipos?			
10. ¿Se utilizan unidades de respaldo de energía (UPS) para proteger contra cortes de electricidad?			
11. ¿El laboratorio cuenta con una adecuada ventilación y control de temperatura?			
12. ¿Se mantienen niveles adecuados de humedad para evitar daños por condensación?			
13. ¿El laboratorio está libre de polvo y otros contaminantes que puedan dañar los equipos?			
14. ¿Se cuenta con sistemas de protección contra incendios?			
15. ¿Los equipos están protegidos contra sobrecargas eléctricas y picos de voltaje?			
16. ¿El mobiliario del laboratorio es adecuado para soportar los equipos sin dañarlos?			
17. ¿Se utilizan protectores contra sobretensiones en todas las conexiones eléctricas?			
18. ¿Se controla el acceso al laboratorio para evitar el uso no autorizado de los equipos?			
19. ¿Los equipos están ubicados en áreas seguras, lejos de zonas de alto tráfico?			
20. ¿Está prohibido el ingreso de alimentos y bebidas en el laboratorio para prevenir derrames sobre los equipos?			
21. ¿Existe un protocolo para el reporte de daños a los equipos?			
22. ¿Se lleva un registro de incidentes de daño a los equipos y las medidas tomadas?			
23. ¿Se actualiza periódicamente el software de los equipos y los controladores para prevenir daños en los equipos de computación?			
24. ¿Se utilizan cables de seguridad para anclar los equipos más valiosos?			
25. ¿Se inspeccionan regularmente los cables y conexiones eléctricas para detectar desgaste?			

REALIZADO POR: FECHA:	REVISADO POR: FECHA:

CONCLUSIONES

OBSERVACIONES

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 3-5

- **Incendio**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿El laboratorio de computación cuenta con detectores de humo?			
2. ¿Se realizan inspecciones regulares de los detectores de humo para asegurar su funcionamiento?			
3. ¿Hay extintores de incendios disponibles en el laboratorio?			
4. ¿Los extintores de incendios están ubicados en lugares accesibles y visibles?			
5. ¿Se realiza el mantenimiento regular de los extintores de incendios?			
6. ¿El laboratorio tiene un sistema de rociadores automáticos contra incendios?			
7. ¿Se revisa y prueba periódicamente el sistema de rociadores automáticos?			
8. ¿El laboratorio cuenta con alarmas de incendio?			
9. ¿Las alarmas de incendio son probadas regularmente para asegurar su funcionamiento?			
10. ¿Se mantienen libres de obstáculos las salidas de emergencia?			
11. ¿Se almacenan correctamente los materiales inflamables lejos de fuentes de calor?			
12. ¿Los cables eléctricos están en buen estado y libres de daños?			
13. ¿Se utilizan regletas y protectores contra sobretensiones certificados?			
14. ¿Los equipos eléctricos están apagados cuando no están en uso?			
15. ¿Se evita la sobrecarga de las tomas eléctricas?			
16. ¿Se inspeccionan regularmente los sistemas eléctricos para detectar posibles riesgos?			
17. ¿Los muebles del laboratorio son resistentes al fuego?			
18. ¿El laboratorio cuenta con señalización adecuada sobre los riesgos de incendio?			
19. ¿Se mantienen los documentos y materiales combustibles en archivadores metálicos?			
20. ¿Está prohibido el uso de dispositivos electrónicos no autorizados, como teléfonos móviles, tabletas, y unidades USB, en el laboratorio?			
21. ¿Las personas que utilizan el laboratorio están capacitados en el uso de extintores de incendios?			
22. ¿El laboratorio cuenta con un sistema de alarma conectado a una estación de bomberos local?			
23. ¿Hay un sistema de comunicación interna para alertar rápidamente al personal en caso de incendio?			
24. ¿El laboratorio cuenta con un plan de recuperación post-incendio?			
25. ¿El laboratorio cuenta con material e ignífugos (detiene las llamas) en áreas de almacenamiento?			

REALIZADO POR:	REVISADO POR:
FECHA:	FECHA:

CONCLUSIONES

OBSERVACIONES

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 4-5

- **Malware**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿Todos los equipos del laboratorio tienen instalado un software antivirus?			
2. ¿El software antivirus está actualizado regularmente en todos los equipos?			
3. ¿Se realizan escaneos de malware de manera regular en los equipos?			
4. ¿El laboratorio cuenta con una política de instalación de software?			
5. ¿Se restringe la instalación de software no autorizado en los equipos?			
6. ¿Se utilizan programas de anti-malware además del antivirus estándar?			
7. ¿Se aplican actualizaciones de seguridad y parches regularmente a todos los sistemas operativos?			
8. ¿Se utilizan firewalls para proteger la red del laboratorio?			
9. ¿Se tiene implementado un sistema de prevención de intrusiones (IPS)?			
10. ¿Se controlan y registran las conexiones USB y otros dispositivos externos?			
11. ¿El software antivirus está configurado para escanear automáticamente los archivos descargados?			
12. ¿Se supervisa la red del laboratorio para detectar actividad sospechosa?			
13. ¿Se tienen políticas claras para la respuesta rápida a infecciones de malware?			
14. ¿El personal del laboratorio está capacitado para reconocer los signos de una infección por malware?			
15. ¿Hay un procedimiento documentado para el aislamiento de equipos infectados?			
16. ¿Se restringe el acceso a los puertos de red?			
17. ¿Se utiliza algún sistema de detección de intrusos (IDS) en la red del laboratorio?			
18. ¿Se revisan los registros de seguridad (logs) para detectar posibles infecciones?			
19. ¿El personal y los usuarios del laboratorio reciben capacitación sobre seguridad informática?			
20. ¿El personal sabe cómo reportar incidentes de seguridad y posibles infecciones?			
21. ¿Se restringe el uso de servicios de descarga de archivos?			
22. ¿Se promueve el uso de contraseñas seguras y su gestión adecuada?			
23. ¿Existe una política de seguridad de la información en el laboratorio?			
24. ¿Se revisan y actualizan regularmente las políticas de seguridad?			
25. ¿Se prohíbe el uso de software pirateado en los equipos del laboratorio?			

REALIZADO POR:	REVISADO POR:
FECHA:	FECHA:

CONCLUSIONES:

OBSERVACIONES:

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 5-5

- **Phishing**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿Tiene el laboratorio políticas claras contra el phishing?			
2. ¿Se proporciona formación regular sobre detección de phishing al personal del laboratorio?			
3. ¿El laboratorio utiliza filtros de correo electrónico para detectar posibles correos de phishing?			
4. ¿Se limpia el historial de navegación?			
5. ¿El personal del laboratorio está capacitado para identificar enlaces sospechosos en correos electrónicos?			
6. ¿Se utilizan herramientas de autenticación de dos factores para acceder a sistemas críticos?			
7. ¿Se han implementado políticas de contraseñas seguras en el laboratorio?			
8. ¿El laboratorio realiza auditorías periódicas de seguridad para identificar posibles vulnerabilidades de phishing?			
9. ¿Se utilizan herramientas de monitoreo de red para detectar posibles ataques de phishing?			
10. ¿El personal del laboratorio está al tanto de los riesgos del phishing a través de redes sociales?			
11. ¿El laboratorio tiene procedimientos claros para reportar correos electrónicos sospechosos?			
12. ¿El laboratorio utiliza software actualizado para protegerse contra exploits de phishing conocidos?			
13. ¿Se dejan abiertas las sesiones cuando se ingresa a internet?			
14. ¿El laboratorio tiene un proceso claro para verificar la autenticidad de correos electrónicos sospechosos?			
15. ¿Se realizan pruebas de penetración periódicas para evaluar la resistencia del laboratorio al phishing?			
16. ¿El laboratorio utiliza firewalls y sistemas de detección de intrusos para proteger contra ataques de phishing?			
17. ¿El personal del laboratorio sabe cómo diferenciar entre sitios web legítimos y fraudulentos?			
18. ¿Se realizan evaluaciones de riesgos periódicas para identificar posibles áreas de vulnerabilidad al phishing?			
19. ¿El laboratorio tiene procedimientos claros para la gestión de contraseña comprometidas?			
20. ¿Se utiliza cifrado para proteger la comunicación por correo electrónico dentro del laboratorio?			
21. ¿El laboratorio tiene un plan de respuesta a incidentes específicos para ataques de phishing?			
22. ¿El laboratorio cuenta con bloqueo para paginas privadas?			
23. ¿El laboratorio utiliza herramientas de seguridad web para bloquear el acceso a sitios de phishing conocidos?			
24. ¿El laboratorio tiene políticas claras sobre el intercambio de información sensible a través del correo electrónico?			
25. ¿Se realizan actualizaciones regulares de seguridad en todos los sistemas y aplicaciones de laboratorio?			

REALIZADO POR:	REVISADO POR:
FECHA:	FECHA:

CONCLUSIONES:

OBSERVACIONES:

4.4.4 Valoración de amenazas

Evaluamos estos factores estimando el porcentaje de degradación y la frecuencia de ocurrencia. El porcentaje de degradación se refiere al grado de daño causado cuando se materializa una amenaza, mientras que la frecuencia de ocurrencia indica la probabilidad de que una amenaza se materialice anualmente. Este análisis tiene como objetivo determinar el impacto y el riesgo potencial de la amenaza sobre el activo.

Valor		Criterio
5	Extremo	Daño extremadamente grave
4	Muy Alto	Daño muy grave
3	Alto	Daño grave
2	Medio	Daño importante
1	Bajo	Daño menor

Tabla 13 Valoración de amenazas

4.4.5 Fase 03 Impacto residual

El próximo paso consiste en estimar el impacto residual, es decir, el daño que puede sufrir un activo como resultado de la materialización de una amenaza. Este valor se obtiene considerando la valoración de los activos y el porcentaje de degradación de las amenazas, excluyendo las salvaguardas actualmente implementadas.

4.5 APLICACIÓN DE LA AUDITORÍA

4.5.1.1 FOTOGRAFIAS DE LA APLICACIÓN DE LA ENTREVISTA Y LOS CONTROLES EVALUADOS, EXPLICACIÓN.

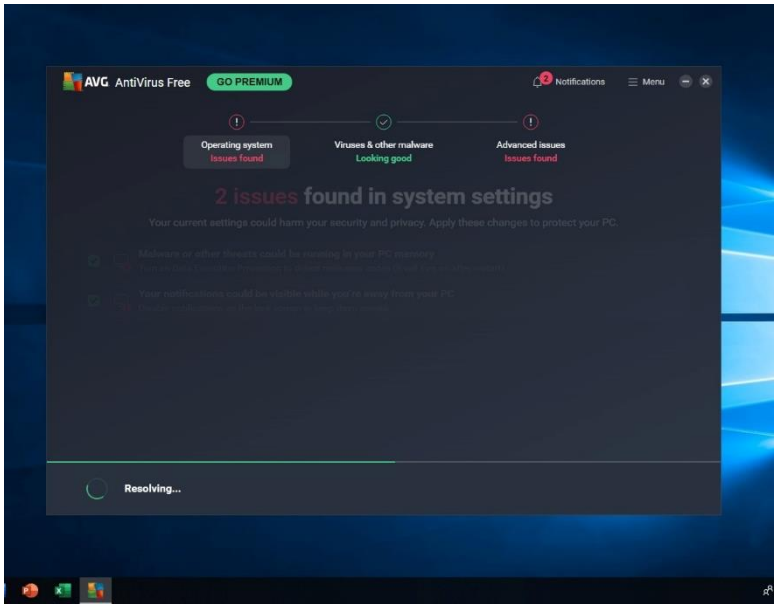
Ilustración 1. Fotografía de entrevista con la Rectora

Como parte de la ejecución de la Auditoría se aplicó técnicas de investigación lo primero fue entrevistar a la Rectora de la institución, sobre información relacionada a controles existentes en el laboratorio de computación para garantizar la seguridad de los activos del laboratorio.

A continuación, se procedió a realizar una inspección del laboratorio para verificar visualmente la existencia de algunos controles como existencia de extintores, reguladores, cajas de breque, sistema de alarma etc.

A continuación, se muestran algunas evidencias de los controles aplicados:

	Ventana con protección con rejas de hierro.
	Polvo en el suelo, el cual afecta a los equipos

	Extintor para protección contra incendios
	Antivirus para garantizar la seguridad de los equipos

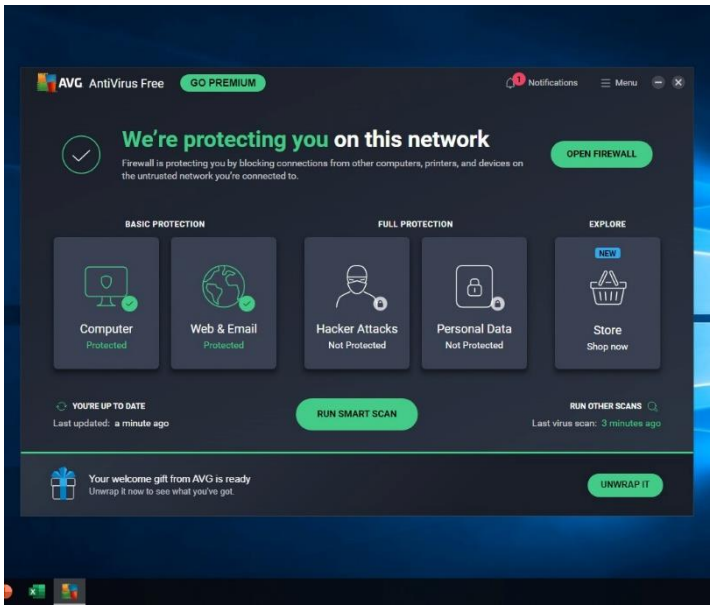
	Antivirus para la protección de los equipos el cual ayuda a proteger los equipos de email maliciosos

Tabla 14. Fotografía de controles aplicados

4.5.1.2 TABULACIÓN DE DATOS

Una vez llenado los instrumentos de los controles se procedió a utilizar una matriz de Excel en la cual se tomó la siguiente consideración, se registró como 1 cuando el control existe o representa seguridad, se registró como 0 cuando no existe el control y representa riesgo, se registró como 2 cuando el control no aplica.

	RIESGO ROBO				
	PREGUNTA	RESPUESTA		1	seguro
1	¿El laboratorio de computación cuenta con cerraduras en las puertas?	1		0	riesgo
2	¿Hay cámaras de seguridad instaladas en el laboratorio y sus alrededores?	0		2	no aplica
3	¿Existen detectores de movimiento en el laboratorio?	0			
4	¿Las ventanas del laboratorio tienen rejas o algún tipo de protección?	1			
5	¿El acceso al laboratorio está restringido al personal no autorizado?	1			
6	¿Se realiza un registro de las personas que entran y salen del laboratorio?	1			
7	¿Hay personal de seguridad que supervise el laboratorio?	1			
8	¿Se cuenta con un sistema de alarma en caso de intrusión?	1			
9	¿Los equipos están anclados o asegurados físicamente para evitar su fácil sustracción?	1			
10	¿Se realizan inspecciones regulares de los equipos y del inventario del laboratorio?	1			
11	¿Se realiza mantenimiento regular a los sistemas de seguridad física?	0			
12	¿El área del laboratorio está completamente cerrada?	1			

Ilustración 4. Valoración de riesgo

4.5.1.3 ANALIZAR RIESGOS

GRAVEDAD (IMPACTO)		CONSIDERACIONES
1	MAS BAJO	Las instalaciones quedan temporalmente cerrada o no puede operar, pero puede
2	BAJO	e ven afectadas de manera pero se puede seguir realizando las actividades, pero no con la
3	MEDIO	amente afectadas ya que al no contar con la disponibilidad de los equipos e inmuebles no se
4	ALTO	ctan de manera irreparable, ya que afecta a la continuidad de las actividades el cual afecta
5	MÁS ALTO	Daños irreparables en instalaciones / afectada más allá del uso habitable. La mayoría de

Ilustración 5. Tabla de Análisis de riesgo. (Gravedad)

En esta tabla de riesgo se utilizó para calcular el impacto que puede ocasionar y que tan grave puede ser si llega a suceder algún incidente dentro de la matriz de riesgo, esto con la finalidad de calcular el valor riesgo y ver el nivel de riesgo que enfrenta.

ESCALA PARA ASIGNAR VALOR DE APARICIÓN		
NIVEL DE APARICIÓN (PROBABILIDAD)		
1	MAS BAJO	1%-10%
2	BAJO	10%-30%
3	MEDIO	30%-50%
4	ALTO	50%-75%
5	MÁS ALTO	75%-100%

Ilustración 6. Tabla para analizar el nivel de aparición. (Probabilidad)

Esta tabla es para calcular el nivel de aparición y la probabilidad que un riesgo llegue a ocurrir, éste se puede calcular con el porcentaje de riesgo que tenga cada control.

LEYENDA							
			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
APARICIÓN (probabilidad)	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	10
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Tabla 15. Leyenda (Probabilidad e Impacto)

En esta tabla se puede ver nivel de impacto y probabilidad, se puede saber si el impacto es bajo o alto mediante el resultado que obtenemos en la matriz en el valor de riesgo.

MATRIZ DE RIESGOS				
RIESGO	Aparición	Gravedad	Valor del Riesgo	Nivel de Riesgo
ROBO	3	2	6	Apreciable
DAÑO DE EQUIPOS	4	5	20	Muy grave
INCENDIO	3	3	9	Importante
MALWARE	4	4	16	Muy grave
PHISHING	5	4	20	Muy grave

Tabla 16. Matriz de Riesgos

En esta tabla de matriz de riesgos, se puede analizar la aparición, gravedad y calcular el valor del riesgo también se puede visualizar el nivel de riesgo. La aparición se calcula mediante de 1 que representa más bajo y 5 que representa más alto, y para sacar estos valores nos fijamos en el porcentaje obtenido de cada uno de los controles aplicados.

CAPÍTULO V

5 EVALUACIÓN DE RESULTADOS

5.1 Informe de Auditoría

5.1.1.1 Dirigido a:

A la rectora de la Unidad Educativa "Dr. José María Velasco Ibarra", la cual está encargada del laboratorio de computación.

5.1.1.2 Motivo:

Para cumplir los requerimientos académicos

5.1.1.3 Objetivos:

1. Identificar los riesgos de seguridad física del Laboratorio de la Unidad Educativa "Dr. José María Velasco Ibarra"
2. Evaluar el nivel de seguridad informática física del Laboratorio de la Unidad Educativa "Dr. José María Velasco Ibarra"

5.1.1.4 Alcance:

Técnicas y procedimientos:

- Identificación de activos
- Valoración de activos
- Cuestionario para analizar riesgos
- Realizar entrevista a la rectora de la institución
- Inspección del laboratorio
- Analizar cuestionario e identificar riesgos
- Analizar riesgos y calcular impacto
- Valoración de riesgo
- Elaborar plan de medida
- Elaborar informe

Se realizó la identificación de activos, después se realizó la valoración de los activos, también se realizó el cuestionario para analizar los riesgos, se realizó una inspección en la institución, después se realizó una entrevista a la rectora de la institución, luego se analizó el cuestionario y se identificó los riesgos, después se analizó los riesgos y se calculó el impacto, también se realizó la valoración de riesgo.

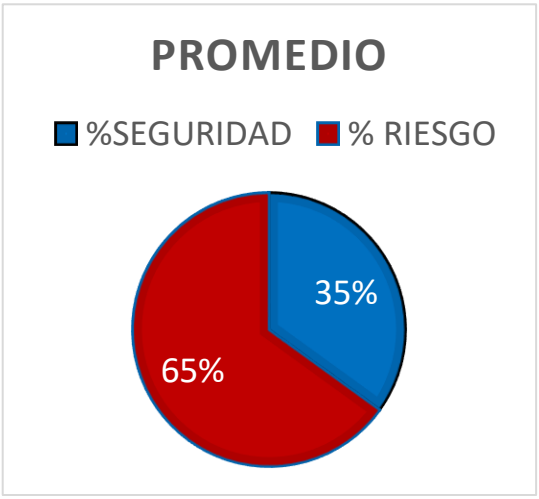
5.1.1.5 Personal relacionado:

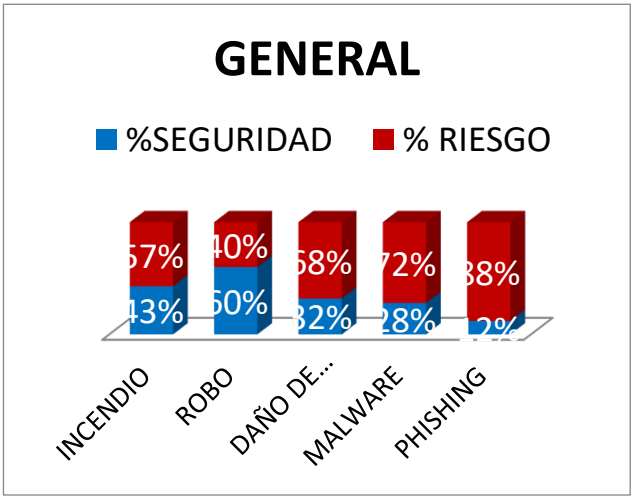
La rectora de la Institución, la inspectora y secretaria

5.1.1.6 Hallazgos:

Al aplicar la auditoría en la Institución se pudo identificar los riesgos que existen y se pudo obtener los siguientes resultados:

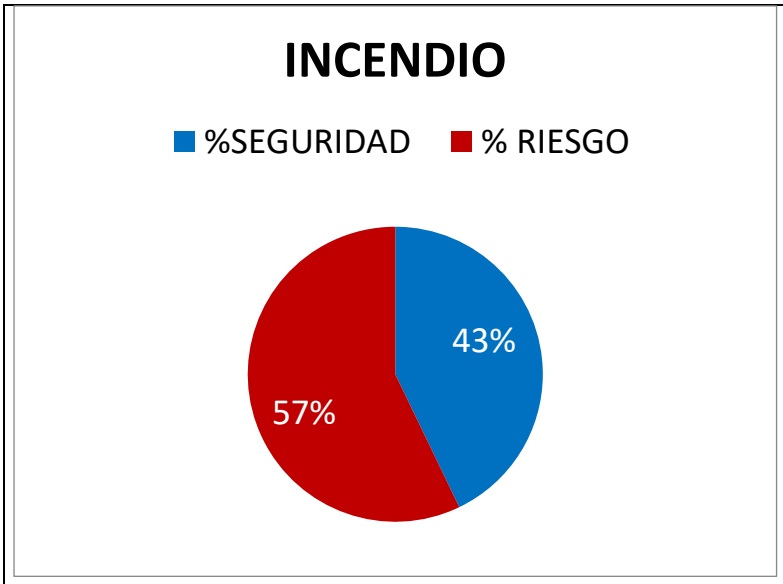
5.2 NIVEL DE SEGURIDAD GENERAL





INTERPRETACIÓN: El nivel de seguridad de laboratorio es del 35% que corresponde a un nivel bajo.

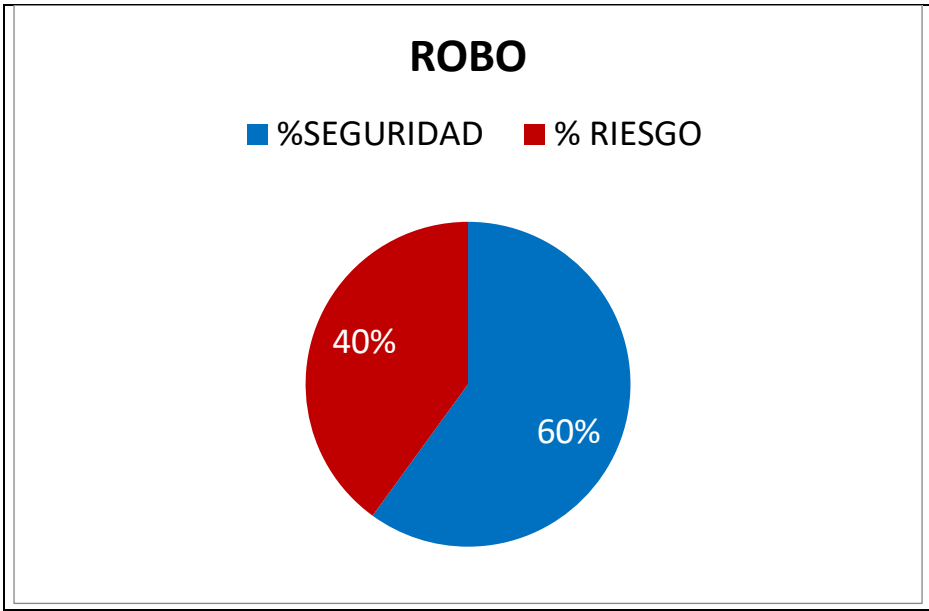
El nivel de riesgo en el gráfico general es el más alto y se pudo identificar que hay mayor exposición en el riesgo de phishing con 88% de porcentaje que representa el nivel más alto de riesgo, también el riesgo de malware con un 72% de porcentaje que representa un nivel alto de riesgo, en daños de equipo también tenemos un 68% de porcentaje que representa un nivel alto de riesgo y el control más seguro es el control de robo con el 60% de porcentaje que representa un nivel alto de seguridad.



Interpretación: El nivel de riesgo de incendio es del 57% que representa un tipo de riesgo importante

Causas:

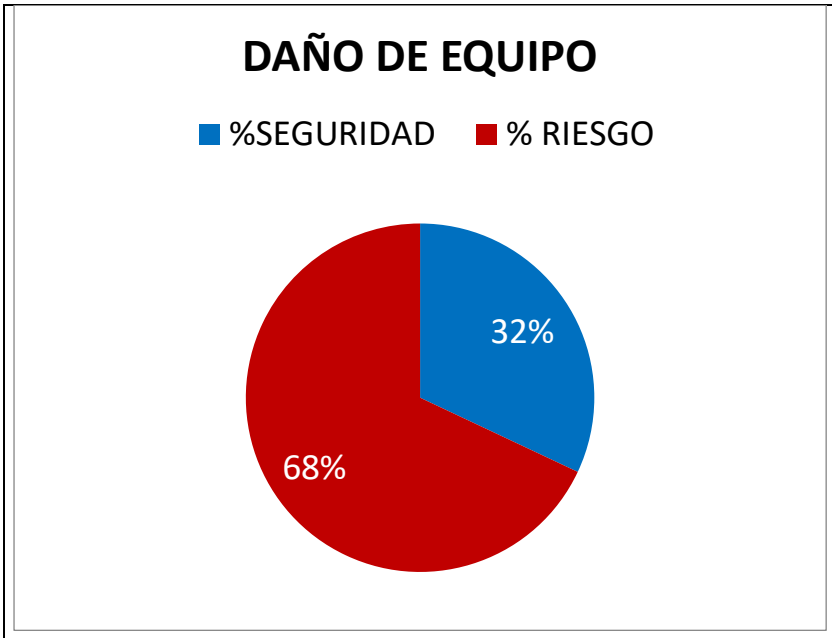
- No hay detectores de humo
- No se realizan mantenimiento a los extintores
- No cuenta con sistema de rociadores automáticos contra incendio
- No se almacenan correctamente los materiales inflamables lejos de fuentes de calor
- No se encuentran en buen estado tampoco libre de daños los cables eléctricos
- No se evitan las sobrecargas de las tomas eléctricas
- No son resistentes al fuego los muebles del laboratorio
- No cuenta con señalización adecuada sobre los riesgos de incendio
- No hay un sistema de comunicaciones interna para alertar rápidamente al personal en caso de incendio
- No cuenta con un plan de recuperación post-incendio
- No cuenta con material e ignífugos en áreas de almacenamiento.



Interpretación: El nivel de riesgo de robo es del 40 % de porcentaje que representa un tipo de riesgo apreciable.

Causas:

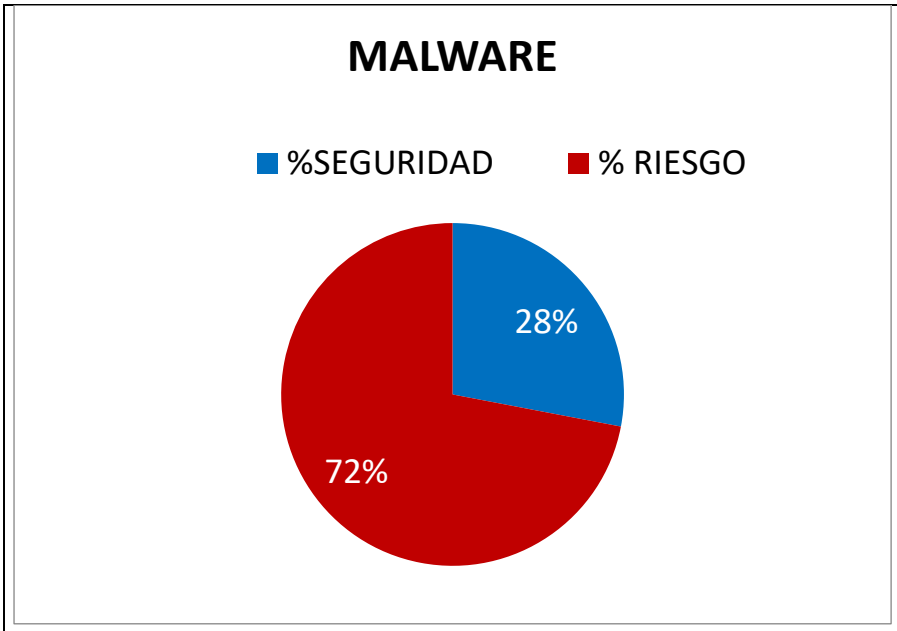
- No hay cámaras de seguridad instaladas en el laboratorio y sus alrededores
- No existen detectores de movimiento en el laboratorio
- No se realizan mantenimientos regulares a los sistemas de seguridad física
- No tienen configurado el bloqueo automático tras un periodo de inactividad
- No se realiza un registro de las actividades de los usuarios en las computadoras
- No cuenta con acceso mediante tarjeta al personal autorizado
- No existe un plan de respuesta a incidentes relacionados con robos o intento de robo en el laboratorio
- No se realizan capacitaciones para la concientización al personal sobre las pérdidas y protocolos en caso de robo
- No cuenta con un laboratorista que sea responsable de cuidar el laboratorio



Interpretación: El nivel de riesgo de daños de equipo es del 68% de porcentaje que representa un tipo de riesgo muy grave de riesgo.

Causas:

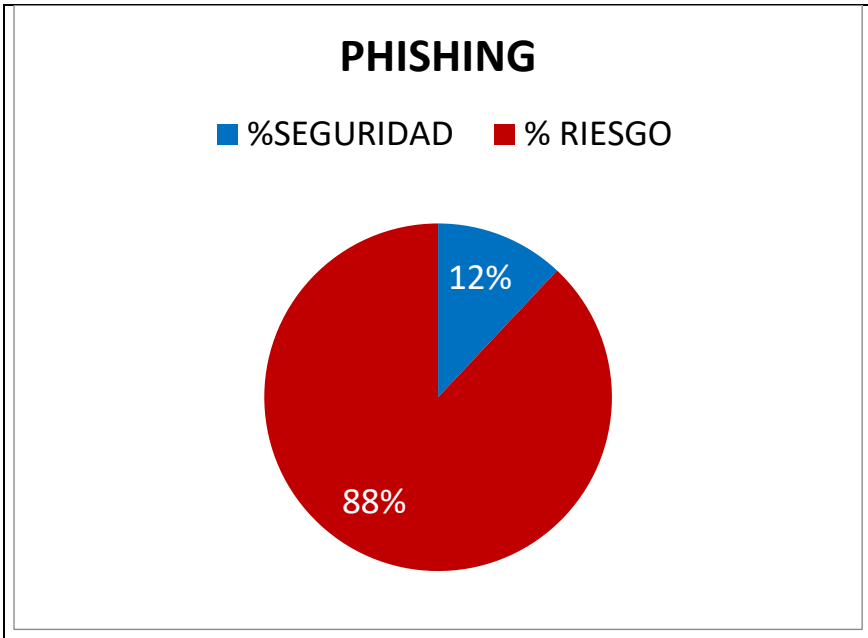
- No se realizan mantenimiento preventivo regular de los equipos
- No existe un registro de mantenimiento y reparaciones de cada equipo
- No reciben revisión mediante antivirus los dispositivos antes de ser conectados a los equipos del laboratorio
- No utilizan herramientas ni métodos adecuados para la limpieza de los equipos
- No reciben capacitación sobre el manejo adecuado de los equipos
- No se utilizan fundas o protecciones para los equipos cuando no están en uso
- No estan los equipos correctamente etiquetados e inventariados
- No se realizan inspecciones periódicas para detectar daños o desgaste en los equipos
- No se utilizan unidades de respaldo de energía (UPS) para proteger contra cortes de electricidad
- No cuenta el laboratorio con una adecuada ventilación y control de temperatura
- No se mantiene el nivel adecuado de humedad para evitar los daños por condensación
- No está el laboratorio libre de polvo y otros contaminantes que puede dañar los equipos
- No cuenta con una protección contra incendios
- No se lleva un registro de incidentes de daños a los equipos y a las medidas tomadas
- No se actualiza periódicamente el software de los equipos y los controladores para prevenir daños en los equipos de computación
- No se utilizan cables de seguridad para anclar los equipos más valiosos
- No se inspeccionan regularmente los cables y conexiones eléctricas para detectar desgaste



Interpretación: El nivel de riesgo de malware es del 72% de porcentaje que representa un tipo de riesgo muy grave de riesgo.

Causas:

- No se realizan escaneos de malware de manera regular en los equipos
- No cuenta con políticas de instalación de software
- No se utilizan programas de anti-malware además del antivirus estándar
- No se aplican actualizaciones de seguridad y parches regularmente a todos los sistemas operativos
- No se utilizan firewalls para proteger la red del laboratorio
- No se tiene implementado un sistema de prevención de instrusos
- No se controlan y registran las conexiones USB y otros dispositivos externos
- No se supervisa la red del laboratorio para detectar actividades sospechosas
- No se tiene políticas claras para la respuesta rápida a infecciones de malware
- No hay un procedimiento documentado para el aislamiento de equipos infectados
- No se restringe el acceso a los puertos de red
- No se utiliza algún sistema de detección de intrusos (IDS) en la red del laboratorio
- No se revisan los registros de seguridad (logs) para detectar posibles infecciones
- No reciben capacitación sobre seguridad informática el personal ni los usuarios
- No saben como reportar incidentes de seguridad y posibles infecciones
- No se restringe el uso de servicios de descarga de archivo
- No se revisan y actualizan regularmente las políticas de seguridad



Interpretación: El nivel de riesgo es del 88% de porcentaje que representa un tipo de riesgo muy grave de riesgo.

Causas:

- No se proporciona formación regular sobre detección de phishing al personal del laboratorio
- No utilizan filtros de correos electrónicos para detectar posibles correos de phishing
- No se limpia el historial de navegación
- No está capacitado el personal para identificar enlaces sospechosos en correos electrónicos
- No se utilizan herramientas de autenticación de dos factores para acceder a sistemas críticos
- No se han implementado políticas de contraseñas seguras en el laboratorio
- No se realizan auditorías periódicas de seguridad para identificar posibles vulnerabilidades de phising
- No se utilizan herramientas de monitoreo de red para detectar posibles ataques de phishing
- No están al tanto el personal de laboratorio de los riesgos de phishing a través de redes sociales
- No tiene procedimientos claros para reportar correos electrónicos sospechosos
- No utilizan software actualizado para protegerse contra exploits de phishing conocidos
- No tienen un proceso claro para verificar la autenticidad de correos electrónicos sospechosos
- No se realizan pruebas de penetración periódicas para evaluar la resistencia del laboratorio al phishing
- No utilizan firewalls y sistemas de detección de intrusos para proteger contra ataques de phishing
- No tienen procedimientos claros para la gestión de contraseñas comprometidas

- No se utilizan cifrados para proteger la comunicación por correos electrónicos dentro del laboratorio
- No tienen un plan de respuesta a incidentes específicos para ataques de phishing
- No tienen políticas claras sobre el intercambio de información sensible a través de correos electrónicos
- No se realizan actualizaciones regulares de seguridad en todos los sistemas y aplicaciones del laboratorio

5.2.1 OPINIÓN

Los riesgos de seguridad de informática encontrados fueron:

RIESGO	Nivel de riesgo
ROBO	Bajo
DAÑO DE EQUIPOS	Muy Alto
INCENDIO	Medio
MALWARE	Muy Alto
PHISHING	Muy Alto

Tabla 17. Riesgos encontrados

El nivel de seguridad del laboratorio es del 35 % de porcentaje que representa un nivel medio de seguridad.

5.3 CONCLUSIONES DE LA AUDITORÍA

- En conclusión, a través de toda la información recopilada se pudo ejecutar una guía de recomendaciones que servirán para prevenir incidentes tanto en la infraestructura como en los equipos de la Unidad Educativa Dr. José María Velasco Ibarra.

- Al concluir con la investigación de cada uno de los controles se detectó el nivel de riesgo, tenemos que el riesgo de phishing tiene un nivel muy grave el cual se encuentra expuesto a los equipos sean interferidos por terceros.

- En base a toda la información recopilada se pudo ejecutar una guía de buenas prácticas que ayudará a cuidar y prevenir daños o incidentes en la infraestructura y dentro de ella de la Unidad Educativa "Dr. José María Velasco Ibarra".

5.4 RECOMENDACIÓNES DE LA AUDITORÍA

- En base al resultado de la auditoría de seguridad informática se sugiere a los docentes y estudiantes de la institución a tomar medidas preventivas para garantizar la seguridad del laboratorio de computación.

- Se recomienda poner en práctica las siguientes indicaciones de la guía de buenas prácticas que se formuló con la finalidad de reducir que haya alguna probabilidad de que ocurran alguno de los riesgos que han sido identificados, esto se logrará con ayuda de las autoridades de la institución y estudiantes.

GuiA

GUIA DE BUENAS PRACTICAS PARA EL LABORATORIO INFORMÁTICO DE LA UNIDAD EDUCATIVA "DR. JOSÉ MARÍA VELASCO IBARRA"

Ilustración 7. Guía de buenas prácticas

ÍNDICE

1. GUIA DE BUENAS PRACTICAS PARA EL LABORATORIO INFORMÁTICO DE LA UNIDAD EDUCATIVA "DR. JOSÉ MARÍA VELASCO IBARRA" 3

1.1 INTRODUCCIÓN 3

1.2 OBJETIVO DE LA GUÍA 4

1.3 ALCANCE 4

2. RECOMENDACIONES 5

2.1.2 MANTENIMIENTO DE LOS EQUIPOS 5

2.1.3 USO DE EQUIPOS 5

2.1.4 USO DE PROGRAMA 5

2.1.5 USO DE CONTRASEÑAS 6

2.1.6 CONTROL DE RED DE WIFI 6

Ilustración 8. Índice de guía de buenas practicas

1.2 OBJETIVO DE LA GUÍA

Establecer medidas preventivas para garantizar la seguridad y buen funcionamiento del laboratorio de computación.

1.3 ALCANCE

Esta guía esta dirigida a los docentes y estudiantes de la institución, ya que la seguridad, integridad y disponibilidad de los equipos ya que es uno de los recursos más importantes de la institución, sin embargo, no todos los docentes están al tanto de los métodos y técnicas que se pueden utilizar para garantizar la seguridad y brindarle mayor duración.

Ilustración 9. Objetivo de la Guía

1. GUIA DE BUENAS PRACTICAS PARA EL LABORATORIO INFORMÁTICO DE LA UNIDAD EDUCATIVA "DR. JOSÉ MARÍA VELASCO IBARRA"

1.1 INTRODUCCIÓN

Se recomienda aplicar la siguiente guía de buenas practicas para prevenir los riesgos encontrados en la auditoría, con la finalidad de mejorar la seguridad y dentro del laboratorio, y así esta guía sirva como recurso valioso para los docentes y estudiantes que utilizan el laboratorio de computación.

Aplicando las guías también la institución puede mejorar el rendimiento de los usuarios que utilizan los equipos del laboratorio, ya que se puede reducir los riesgos, optimizar los recursos y elevar la calidad de aprendizaje.

A continuación, se presentará las principales recomendaciones que deben considerarse para su implementación en los equipos informáticos y en la infraestructura con la finalidad de proporcionar una mayor protección a su información.

Ilustración 10. Introducción de la Guía

2. RECOMENDACIONES

2.1.1.1 CONTROLES DE SEGURIDAD FÍSICO

- Instalar cámaras de seguridad para vigilar el laboratorio y sus alrededores
- Instalar sensores de movimiento para controlar sucesos que pueden ocurrir
- Configurar el bloqueo automático tras un periodo de inactividad
- Implementar un plan de respuesta a incidentes relacionados con robos
- Realizar capacitaciones para la concientización al personal sobre pérdidas y protocolos en caso de robo
- Tener cerraduras en las puertas para garantizar la seguridad
- Restringir el acceso al personal no autorizado
- Utilizar protección en las ventanas del laboratorio para evitar una intervención forzosa
- Tener los equipos anclados y asegurados físicamente para evitar la fácil sustracción
- Realizar inspecciones regulares de los equipos para verificar daños
- Revisar regularmente las cerraduras para evitar incidentes
- Mantener una adecuada ventilación y control de temperatura para evitar daños en los equipos
- Utilizar protectores contra sobretensiones en todas las conexiones
- Prohibir el ingreso con alimentos y bebidas al laboratorio
- Tener como mínimo dos extintores dentro del laboratorio para prevenir cualquier tipo de incendio
- Está prohibido ingresar al laboratorio con mochila, esto para preservar la seguridad de los equipos
- Está prohibido correr dentro del laboratorio para evitar tropezar y dañar algún equipo
- Mantener limpio el laboratorio para evitar que los equipos se dañen
- Llevar un registro de los usuarios que ingresan y salen del laboratorio
- Revisar los equipos antes que los estudiantes salgan, para prevenir perdidas
- Dejar barrido el laboratorio después de ser utilizado por los usuarios para evitar el ingreso de insectos
- Revisar continuamente la caja de RACK y limpiarla para evitar el ingreso de insectos

Ilustración 11. Recomendaciones sobre los controles de seguridad

2.1.2 MANTENIMIENTO FÍSICO DE LOS EQUIPOS

- Realizar mantenimiento a los equipos
- Utilizar fundas de protección para los equipos cuando están inactivos
- Utilizar herramientas adecuadas para la limpieza de los equipos
- Realizar políticas para el uso de los equipos del laboratorio
- Revisar los dispositivos antes de ser conectados a los equipos del laboratorio por un software
- Utilizar unidades de respaldo de energía para proteger contra cortes de electricidad
- Evitar que los cables estén regados en el suelo para evitar que estos se dañen y no cumplan su vida útil
- Mantener limpia el área donde se encuentran los equipos de computación
- Implementar un sistema de registro de incidentes
- Realizar limpieza a los NUC con más frecuencia

2.1.3 USO DE EQUIPOS

- Los estudiantes podrán utilizar los equipos con la supervisión de un docente
- Los equipos no serán utilizados fuera de las horas de clases
- Los equipos deben mantenerse apagado mientras nadie los esté ocupando
- Los usuarios deberán recibir capaciones para el uso de los equipos
- Los equipos no pueden ser extraídos fuera del laboratorio por ninguna persona al menos que esté autorizado
- Revisar las memorias USB antes de ser utilizadas por medio de un programa
- No mover los equipos del puesto en que están ubicados
- Está prohibido desconectar los equipos para no generar daños
- Utilizar cuidadosamente las computadoras para evitar que éstas se dañen
- Los equipos no pueden ser apagados sin antes haber cerrado todas las pestañas abiertas
- Los estudiantes deberán utilizar los equipos únicamente para realizar tareas e investigaciones
- Esta prohibido el ingreso a páginas prohibidas, los docentes deberán vigilar para prevenir esta acción
- No recargar los enchufes con demasiados cables conectados para evitar daños en los equipos
- Está prohibido modificar o intentar modificar la configuración de los equipos
- Está estrictamente prohibido utilizar los equipos para videojuegos, redes sociales, etc.

Ilustración 12. Recomendaciones sobre Mantenimiento Físico y Uso de equipos

2.1.4 USO DE PROGRAMA

- Instalar programa antimalware que permita detectar códigos maliciosos para esto se sugiere utilizar las siguientes herramientas:
    - Microsoft Defender es un software antimalware gratuito que se incluye con Windows y se actualiza automáticamente
    - Malwarebytes es una herramienta de seguridad personal que protege de virus, malware y más.
    - Avast también es uno de los softwares de seguridad más eficiente para equipos
    - AVG es un antivirus que brinda una licencia gratuita que es muy beneficiosa para detectar virus, y con la licencia pagada se los puede combatir
    - VIPRE es una de las mejores soluciones de seguridad, ya que ofrece una herramienta gratis para eliminar malware y phishing
- Instalar un programa para revisar las memorias USB que estén limpias antes de utilizar para esto se sugiere utilizar las siguientes herramientas:
    - Panda es otro de los softwares seguros ya que permite escanear USB, también brinda un modo de juego para reducir su consumo cuando se usa videojuegos.
    - USBView es una aplicación de Windows que se utiliza para examinar todos los controladores USB y los dispositivos USB conectados en el equipo
    - USB Master Clean es un antivirus en el que también se puede limpiar a fondo la memoria USB
- Utilizar programas educativos para realizar presentaciones, por ejemplo:
    - Canva es uno de los programas de diseño gráfico más consolidados del mercado, el cual es muy útil ya que ofrece miles de plantillas para ser editadas y crear presentaciones atractivas
    - Visme es un software de diseño y cuenta con decenas de herramientas para crear todo tipo de proyecto
    - Prós Es un editor en el cual ofrece miles de plantillas que permiten a usuarios crear presentaciones atractivas

Ilustración 13. Recomendaciones sobre el Uso de programas

2.1.5 USO DE CONTRASEÑAS

- No dejar las contraseñas guardadas en páginas web
- Cambiar las contraseñas frecuentemente para evitar que las cuentas sean intervenidas
- No utilizar la misma contraseña para todas las cuentas que sean creadas por los usuarios
- No compartir la contraseña con nadie y evitar el acceso no autorizado
- Usar diferentes contraseñas para cada cuenta que sea creada
- Las contraseñas son intransferibles
- Las contraseñas son responsabilidad únicamente del propietario

2.1.6 INDICACIONES PARA CREAR CONTRASEÑAS SEGURAS

- Utilizar contraseñas largas para garantizar que las cuentas estén seguras
- No usar la misma contraseña en todos lados
- No usar datos personales como contraseña
- Crear patrones para recordarlas
- Utilizar números en lugar de letra
- Crear contraseñas que tengan letras mayúsculas y minúsculas, espacios, símbolos y números
- Evitar utilizar nombres en las contraseñas ya que pueden ser fácil de descifrar
- Utilizar gestor de contraseña para crear una contraseña más segura
- Crear contraseñas con una longitud mínima de (8) caracteres
- Utilizar autenticación en las contraseñas para mayor seguridad
- La contraseña solo la debe saber el usuario que la crea
- Evitar el uso de contraseña por defecto ya que son muy débiles.

2.1.7 CONTROL DE RED DE WIFI

- Instalar software para monitorear la red del wifi, se sugiere utilizar las siguientes herramientas:
    - Wifi Protector es una aplicación que añade seguridad a las conexiones inalámbricas usando VPN, Estableciendo una conexión directa y encriptada.
- Instalar un software para visualizar quien utiliza la red, se sugiere utilizar la siguiente herramienta:
    - Fing esta herramienta que se utiliza para saber quién está usando la red de Wifi, y se puede controlar a los usuarios conectados.
    - Smart Wifi se puede ver la contraseña, ver cuántos dispositivos hay conectados y se puede pausar la conexión o incluso bloquearlos

Ilustración 14. Recomendaciones sobre el Uso de contraseñas, Indicadores para crear contraseñas y control de red de wifi

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Al concluir el proyecto de revisión general de la infraestructura del laboratorio de cómputo, hemos logrado identificar de manera precisa las principales problemáticas que afectan su funcionamiento y eficiencia.

- En el marco del proyecto cuyo objetivo principal fue investigar en diferentes libros para fundamentar la auditoría informática y comprender la infraestructura tecnológica, proporcionando una base teórica que sirvió de apoyo para la realización de auditorías informáticas.

- En primer lugar, se llevaron a cabo estudios exploratorios que permitieron definir y comprender el contexto del problema posteriormente, se utilizaron técnicas como encuesta y entrevista para recopilar y analizar datos y que nos permitió obtener una visión integral y detallada de la situación.

- La seguridad del laboratorio y los sistemas informáticos de la institución presentan un nivel adecuado de protección, pero con áreas de mejora importantes que deben ser abordadas de manera prioritaria, la implementación de la guía propuesta contribuirá significativamente a elevar el nivel de seguridad y reducir los riesgos asociados, garantizando así la integridad y disponibilidad de los recursos y datos de la institución.

- El proyecto de auditoría se llevó a cabo con el objetivo de elaborar un informe detallado que presentara los hallazgos y los resultados más relevantes. A lo largo de este proceso, se identificaron diversas áreas de mejora y se formularon recomendaciones específicas para fortalecer la seguridad y la eficiencia operativa de la institución auditada.

6.2 Recomendaciones

A los docentes de la Institución “Dr. José María Velasco Ibarra” se le recomienda que deben tener mayor precaución con los equipos informáticos, ya que hoy en día estamos expuestos al peligro y principalmente los equipos por eso es necesario combatir cualquier tipo de ataque o amenazas que se encuentren expuestos.

A la Universidad Laica Eloy Alfaro implementar un marco institucional para tratar sobre las seguridades informáticas en la cual las instituciones sean tomadas en cuenta para que los docentes reciban capacitaciones sobre temas de seguridad informática y estén prevenidos ante situaciones de peligro.

A los docentes de la Universidad se les recomienda realizar brigadas en las instituciones cercanas para que los docentes de la institución puedan estar tener conocimiento claro sobre los riesgos que existen en los laboratorios de computación y saber cómo actuar en caso de que uno de estos riesgos llegue a ocurrir.

6.3 BIBLIOGRAFÍA

Alchundia, I. M. (2018). *EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT.*

Alchundia, I. M. (2018). *El análisis y gestión, enfoque de la metodología magerit.*

Amendaño, J. P. (2018). Incidencias del uso de infraestructura tecnológica en el proceso de inter-aprendizaje, en la escuela julio matovelle en el septimo grado, sección vespertina. 69.

Antonio, G. M. (2019). Auditoría Informática. Guayaquil.

Arantes, S. C. (2022). *Auditoría de seguridad informática.* Quito.

Barroso, J. G. (2015). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*

Cabuto, B. G. (03 de Marzo de 2018). *Sutori*. Obtenido de https://www.sutori.com/es/historia/infraestructura-de-ti--KBDrRn3tukJLi8SinUJ3W495

Caccuri, V. (2018). *Computación para docentes.* Cuenca.

Campos, C. M. (2023). Sistemas operativos. Cuenca.

Carlos, M. P. (2015). *Fundamentos del Hardware.* Texas, EEUU.

Castro, M. I. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Sevilla, España.

Chávez Tisalema, S. A. (2022). Auditoría informática en la empresa distribuidora Los Paisas. 191.

Chávez Tisalema, S. A. (Marzo de 2022). *Repositorio en Digital Universidad Técnica de Ambato*. Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/34791

Chulde, M. R. (2017). *Fundamentos de Auditoría Informática basada en riesgos.* Ibarra.

Cruzatti, J. E. (2018). *Introducción a la seguridad informática y el análisis de las vulnerabilidades.* Sevilla, España.

Fortes, B. G. (2016). *Infraestructura tecnológica.* Caracas.

Gómez, M. A. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* . Madrid.

Gómez, M. A. (2015). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* .

Guzmán, J. P. (2018). *EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT.*

Guzmán, J. P. (2018). *EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT.*

Jorge, C. M. (2015). *Auditoría Informática.* Ambato.

Laudon, K. C. (2019). *Sistemas de Información Gerencia.* Ciudad de Mexico.

León Amendaño, J. P. (Julio de 2018). *Universidad Politécnica Salesiana*. Obtenido de https://dspace.ups.edu.ec/handle/123456789/16002

León, J. G. (2017). *Fundamentos de Auditoría Informática basada en riesgos.* Ibarra.

LLOREDA, B. J. (2018). Auditoria Informática a la infraestructura tecnológica y sistemas de información bajo el estándar cobit en la institución educativa escuela normal superior de quidó. 76.

Loor, P. J. (2021). *Seguridad Informática.* Cuenca.

Lopez, P. J. (2019). *Fundamentos del hardware.* Texas, EEUU.

Machado Lloreda, B. J. (5 de Mayo de 2018). *Universidad Nacional Abierta y a Distancia*. Obtenido de https://repository.unad.edu.co/handle/10596/18042

Maria, P. R. (2019). *Metodologia Magerit.*

Mayorga Mayorga, F. O. (Septiembre de 2023). *Repositorio Digital Universidad Tecnica de Ambato*. Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/39518

Mejía, E. M. (2014). *Metodología de la investigación* .

Merino, M. A. (2020). Introducción a la Seguridad Informática y el análisis de vulnerabilidades. Santo Domingo.

Mero, C. J. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Lima, Perú.

Mite, J. F. (2019). *Metodología Magerit.*

Moguel, E. R. (2005). La creatividad, el rigor del estudio y la integridad son factores que transforman al estudiante en un profesional de éxito. En *Metodología de la información.* Tabasco: en la Colección Hector Marino Rodríguez.

Monge, E. M. (2023). Sistemas operativos, sistemas informáticos y lenguajes de programación. Bogotá, Colombia.

Morán, G. L. (2018). Introducción a la Seguridad Informática y el análisis de vulnerabilidades. Barcelona, España.

Navarrete, D. S. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Quito.

Neill, D. A. (2018). *Procesos y Fundamentos de la investigación cientifica.*

Ordoñes, O. O. (2019). *Meotodogía Magerit.*

Paul, R. R. (2021). *Auditoría informática, para la evaluación de riesgos en la seguridad de la información en la cooperativa de ahorro y creditos prodvisión de la provincia de tungurahua, cantón Pelileo.* Ambato.

Paul, R. R. (Abril de 2021). *Repositorio Digital Universidad Tecnica de Ambato*. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/32712

Pérez Tejada, J. S. (2015). Hardware. Mexicali, Mexico.

Pérez, J. C. (2015). *Componentes del Harware.* Bogotá, Colombia.

Pérez, J. S. (2015). *Fundamentos del Hardware.* Texas, EEUU.

Ppito. (2017). *la auditoria.* Cuenca.

Quimiz, Á. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Quito.

Solorzano, I. M. (2020). *Auditoría Informática* .

Tejada, E. C. (2015). *Auditorí de seguridad informática.* Quito.

Uribe, J. R. (Agosto a Diciembre de 2000). *ART9*. Obtenido de https://www.ipn.mx/assets/files/investigacion-administrativa/docs/revistas/87/ART9.pdf

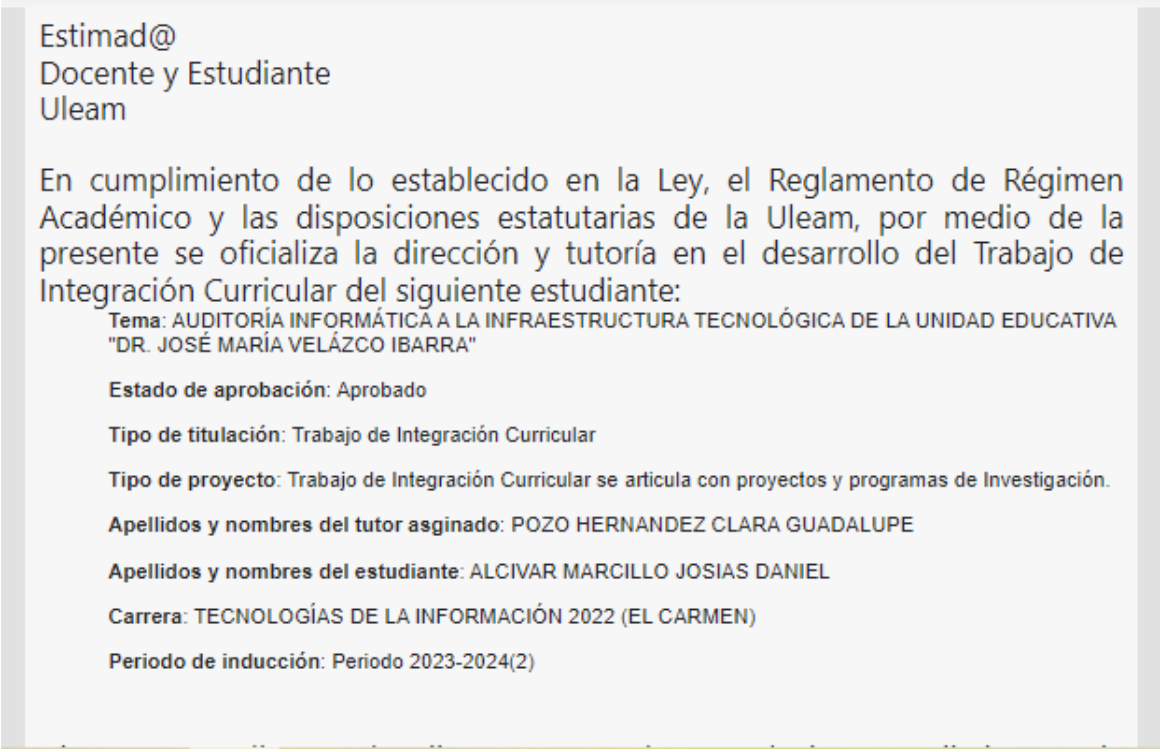
Verduga, J. L. (2020). *Auditoria y controles de TI.* Barcelona, España.

Victor, C. A. (2018). *Metodología Magerit.*

Zabala, J. A. (2018). *EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT*. Ibarra.

6.4 ANEXOS

Anexo A: Asignación de tutor



Estimad@
Docente y Estudiante
Uleam

En cumplimiento de lo establecido en la Ley, el Reglamento de Régimen Académico y las disposiciones estatutarias de la Uleam, por medio de la presente se oficializa la dirección y tutoría en el desarrollo del Trabajo de Integración Curricular del siguiente estudiante:

Tema: AUDITORÍA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIDAD EDUCATIVA "DR. JOSÉ MARÍA VELÁZCO IBARRA"

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

Tipo de proyecto: Trabajo de Integración Curricular se articula con proyectos y programas de Investigación.

Apellidos y nombres del tutor asginado: POZO HERNANDEZ CLARA GUADALUPE

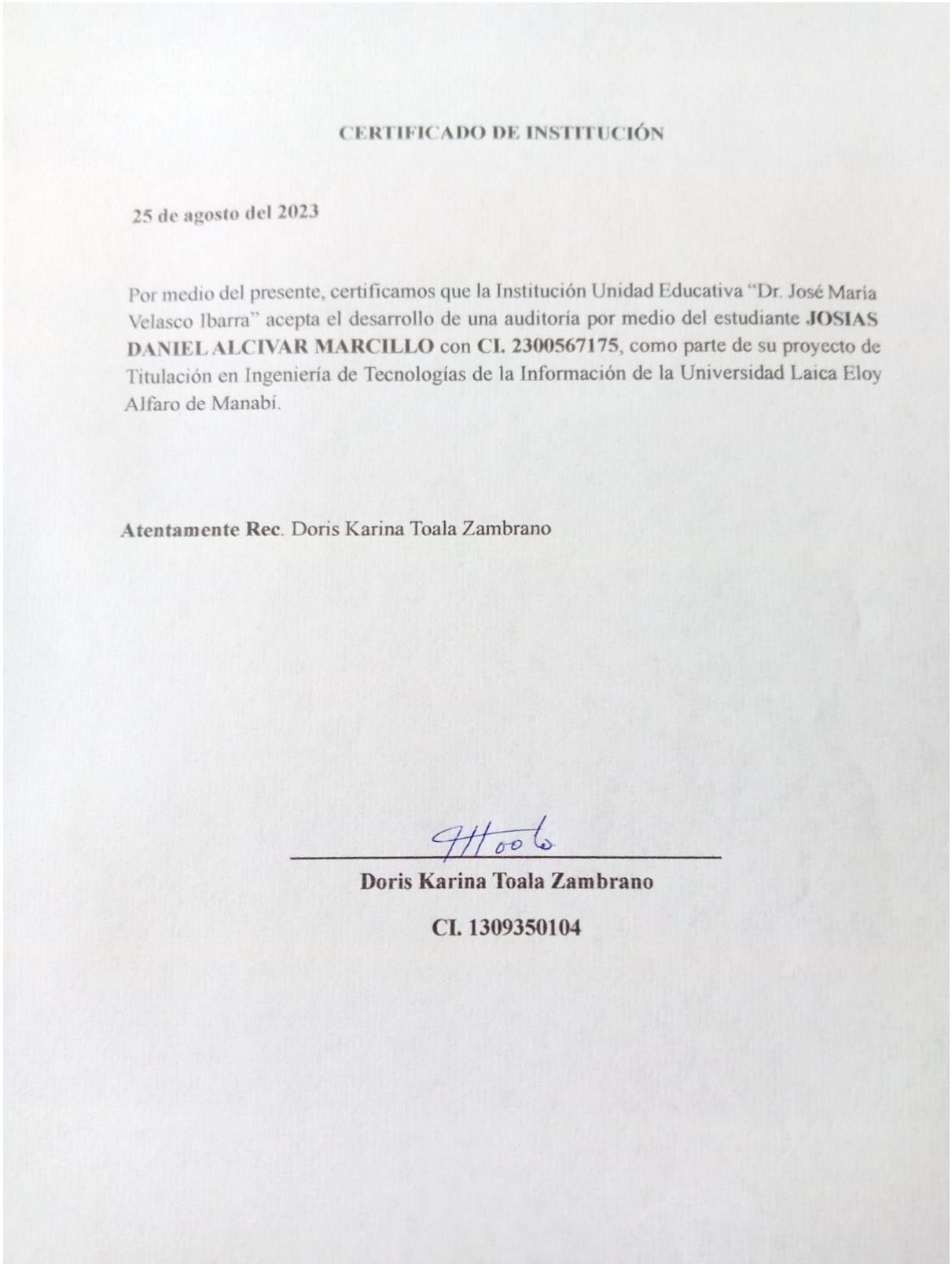
Apellidos y nombres del estudiante: ALCIVAR MARCILLO JOSIAS DANIEL

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2023-2024(2)

Anexo A: Asignación de tutor

Anexo B: Certificado de la empresa



CERTIFICADO DE INSTITUCIÓN

25 de agosto del 2023

Por medio del presente, certificamos que la Institución Unidad Educativa "Dr. José María Velasco Ibarra" acepta el desarrollo de una auditoría por medio del estudiante **JOSIAS DANIEL ALCIVAR MARCILLO** con **CI. 2300567175**, como parte de su proyecto de Titulación en Ingeniería de Tecnologías de la Información de la Universidad Laica Eloy Alfaro de Manabí.

Atentamente Rec. Doris Karina Toala Zambrano

Doris Karina Toala Zambrano

CI. 1309350104

Anexo B: Certificado de la empresa

Anexo D: Reporte del sistema antiplagio

CERTIFICADO DE ANÁLISIS
magister

Tesis Alcivar Josias

3% Textos sospechosos

3% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos

Nombre del documento: Tesis Alcivar Josias.pdf
ID del documento: 157adbb09d51e20b8f68ed8d43d7a824fad57c38
Tamaño del documento original: 1,41 MB

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 23/7/2024
Tipo de carga: interface
fecha de fin de análisis: 23/7/2024

Número de palabras: 17.924
Número de caracteres: 121.214

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	compite.com.co https://compite.com.co/wp-content/uploads/2020/11/20.-MATRIZ-DE-IDENTIFICACIÓN-Y-GESTIÓN-D... 6 fuentes similares	< 1%		Palabras idénticas: < 1% (103 palabras)
2	Tesis completa Micaela Demera.pdf | Tesis completa Micaela Demera #95e882 El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (73 palabras)
3	Tesis Katty Fuertes Gomez.pdf | Tesis Katty Fuertes Gomez #c63869 El documento proviene de mi biblioteca de referencias 4 fuentes similares	< 1%		Palabras idénticas: < 1% (71 palabras)
4	Tesis Gina Zambrano.pdf | Tesis Gina Zambrano #6c3e42 El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (68 palabras)
5	dspace.espoch.edu.ec http://dspace.espoch.edu.ec/bitstream/123456789/5311/3/82T00306.pdf.txt	< 1%		Palabras idénticas: < 1% (54 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario #a4ea5e El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (31 palabras)
2	www.eumed.net | El análisis y gestión de riesgos en gobiernos de ti desde el enfo... https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html#:~:text=Respecto al análisi...	< 1%		Palabras idénticas: < 1% (24 palabras)
3	dspace.tdea.edu.co https://dspace.tdea.edu.co/bitstream/handle/tdea/1391/Informe Auditoria seguridad.pdf	< 1%		Palabras idénticas: < 1% (19 palabras)
4	repository.unad.edu.co https://repository.unad.edu.co/jspui/bitstream/10596/18042/4/26274426.pdf	< 1%		Palabras idénticas: < 1% (12 palabras)
5	TESIS APQC 20_7_2023 correcion(1).docx | TESIS APQC 20_7_2023 correcio... #0b8bfb El documento proviene de mi grupo	< 1%		Palabras idénticas: < 1% (10 palabras)

23-07-2024

Anexo C: Reporte del sistema antiplagio

6.5 Anexo E: Fotografías

Identificación de riesgos por robo.

Ilustración 2. Cerraduras de puertas

Ilustración 3. Ventanas con rejas

Ilustración 4. Equipos asegurados

Ilustración 5 La infraestructura es segura

Identificación de riesgo por Daños de equipo

Ilustración 6. Control de temperatura

Ilustración 7 Protección sobre cargas eléctricas

Ilustración 8. Mobiliario adecuado para los equipos

Ilustración 9. Equipos lejos de zona de alto tráfico

Identificación de riesgos sobre incendio

Ilustración 10. Extintor contra incendio

Ilustración 11. El extintor se encuentra en un lugar visible

Ilustración 12. Se utilizan regletas

Ilustración 13. Equipos eléctricos apagados

Identificación de amenazas sobre malware

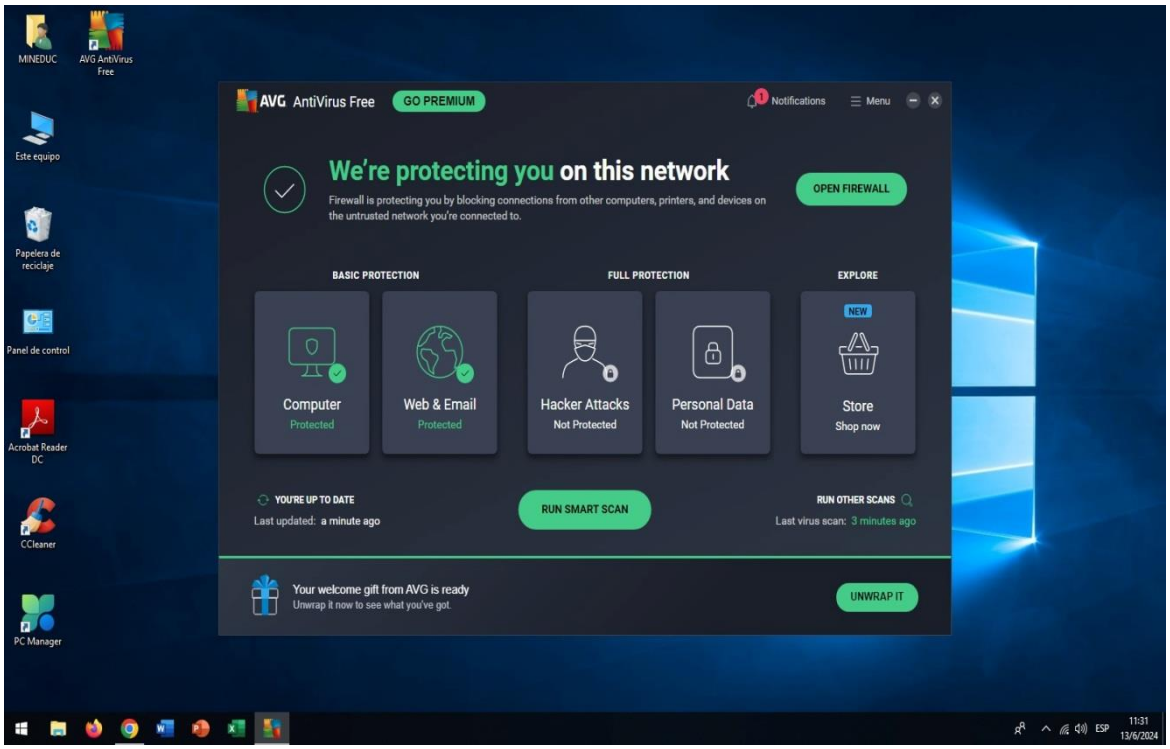


Ilustración 14. Software antivirus AVG

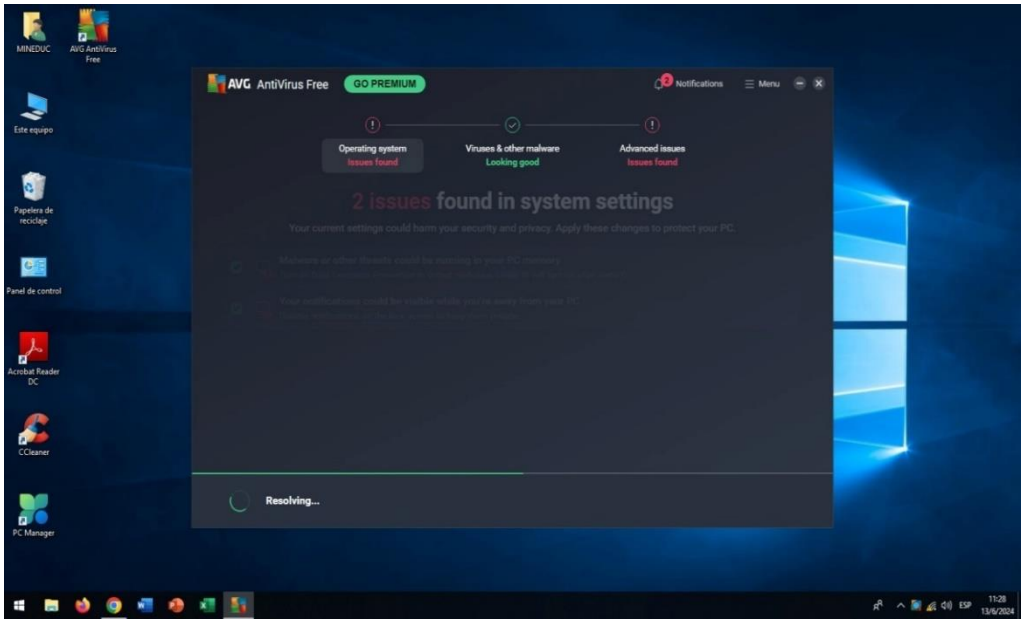


Ilustración 15. Configurado para escanear archivos descargados

Identificación de riesgos por Phishing

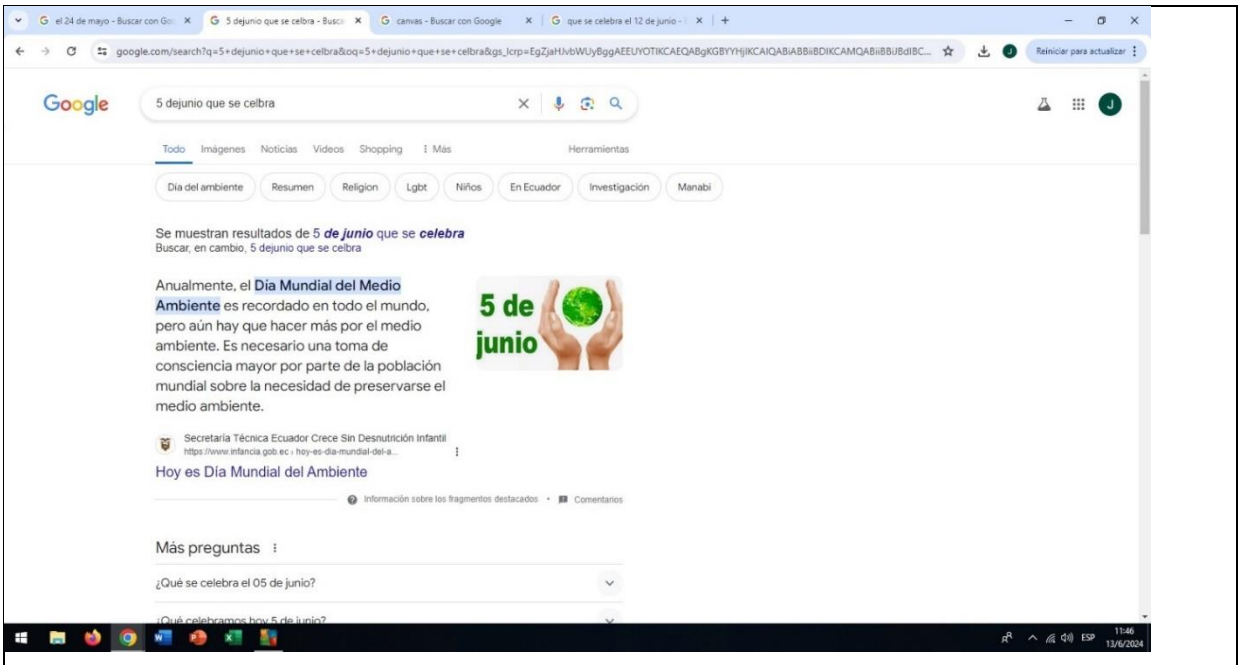


Ilustración 16. Se dejan abiertas sesiones y pestañas de navegación

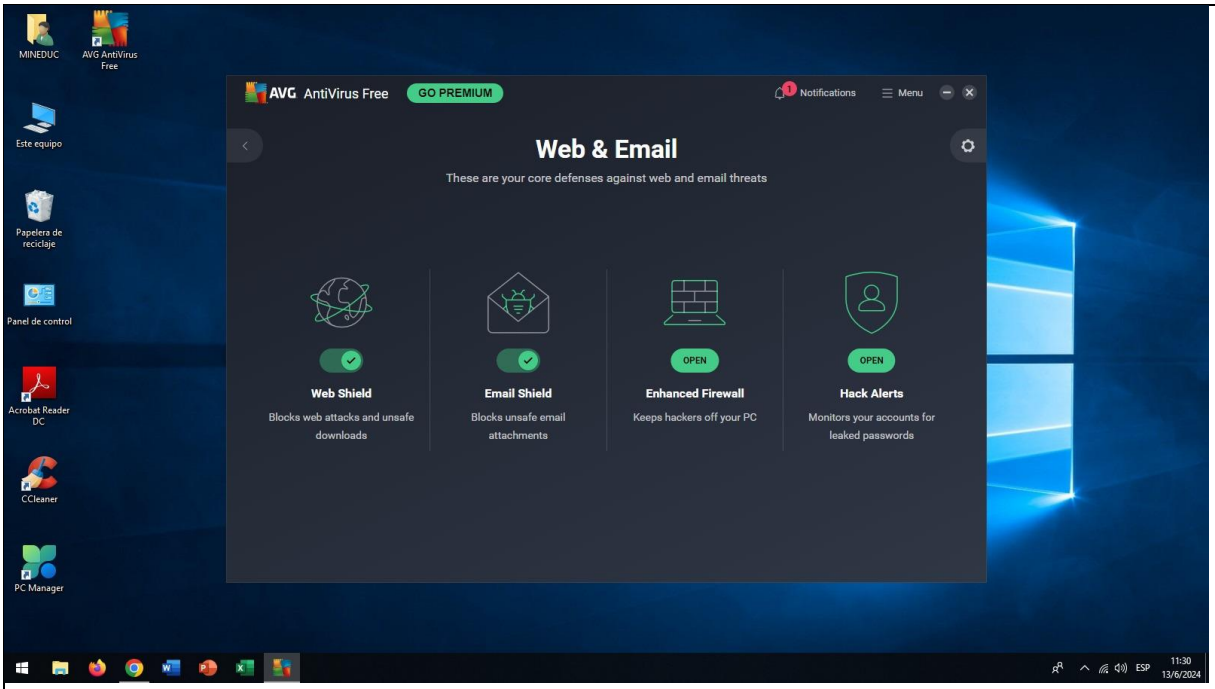
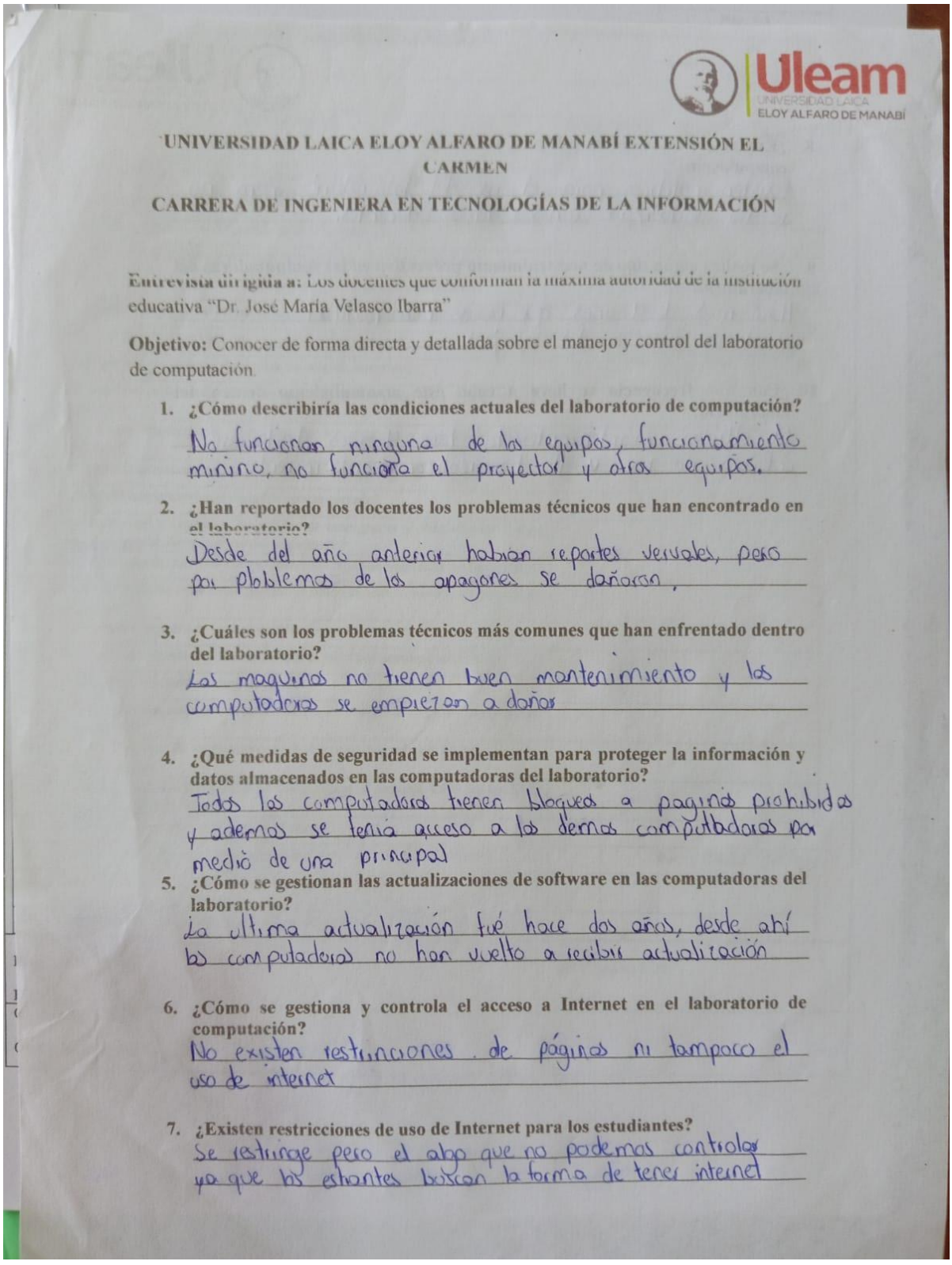


Ilustración 17. Bloqueo de páginas privadas

Anexo F: Evidencia de aplicación de encuestas y entrevistas



UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

Entrevista dirigida a: Los docentes que conforman la máxima autoridad de la institución educativa "Dr. José María Velasco Ibarra"

Objetivo: Conocer de forma directa y detallada sobre el manejo y control del laboratorio de computación.

1. **¿Cómo describiría las condiciones actuales del laboratorio de computación?**
   No funcionan ninguna de las equipos, funcionamiento mínimo, no funciona el proyector y otros equipos.
2. **¿Han reportado los docentes los problemas técnicos que han encontrado en el laboratorio?**
   Desde del año anterior habían reportes verbales, pero por problemas de los apagones se dañaron.
3. **¿Cuáles son los problemas técnicos más comunes que han enfrentado dentro del laboratorio?**
   Las maquinas no tienen buen mantenimiento y las computadoras se empiezan a dañar
4. **¿Qué medidas de seguridad se implementan para proteger la información y datos almacenados en las computadoras del laboratorio?**
   Todos los computadoras tienen bloqueo a paginas prohibidas y además se tenía acceso a los demas computadoras por medio de una principal
5. **¿Cómo se gestionan las actualizaciones de software en las computadoras del laboratorio?**
   La ultima actualización fué hace dos años, desde ahí los computadoras no han vuelto a recibir actualización
6. **¿Cómo se gestiona y controla el acceso a Internet en el laboratorio de computación?**
   No existen restricciones de páginas ni tampoco el uso de internet
7. **¿Existen restricciones de uso de Internet para los estudiantes?**
   Se restringe pero el abo que no podemos controlar ya que los estantes buscan la forma de tener internet

Ilustración 18Aplicación de Entrevista a la Rectora

8. **¿Existen políticas claras sobre el uso de los equipos en el laboratorio de computación?**

Existen políticas para el uso del laboratorio pero no se ha socializado con los demás docentes.

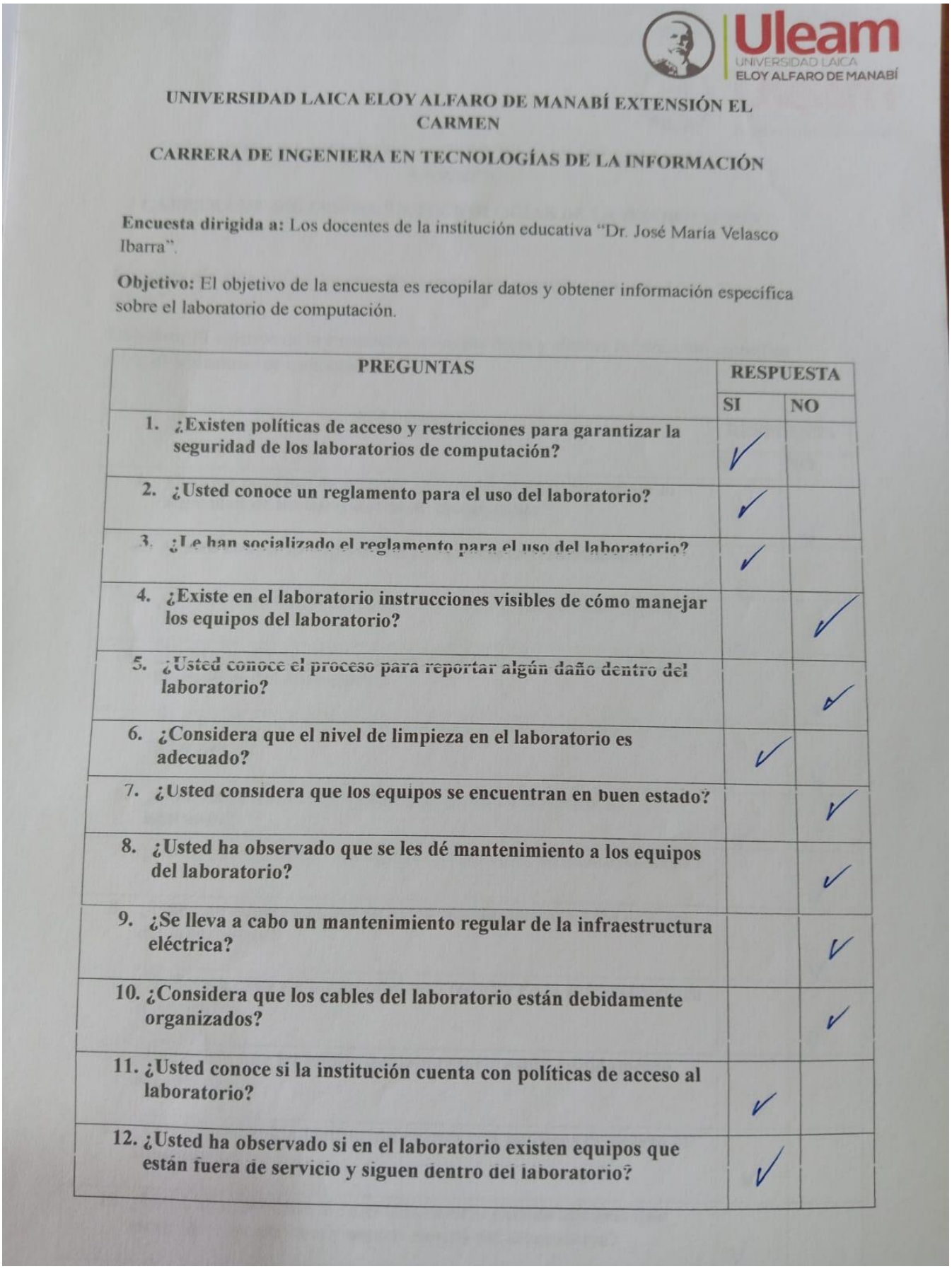
9. **¿Se realiza algún tipo de mantenimiento preventivo en las computadoras del laboratorio?**

Hace más de 4 años que no se han realizado mantenimiento en los equipos.

10. **¿Con qué frecuencia se lleva a cabo este mantenimiento dentro del laboratorio?**

El último mantenimiento fué hace 4 años desde ese entonces no han vuelto ha realizar mantenimiento

Ilustración 19. Aplicación de Entrevista a la Rectora



UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

Encuesta dirigida a: Los docentes de la institución educativa "Dr. José María Velasco Ibarra".

Objetivo: El objetivo de la encuesta es recopilar datos y obtener información específica sobre el laboratorio de computación.

PREGUNTAS	RESPUESTA	
	SI	NO
1. ¿Existen políticas de acceso y restricciones para garantizar la seguridad de los laboratorios de computación?	✓	
2. ¿Usted conoce un reglamento para el uso del laboratorio?	✓	
3. ¿Le han socializado el reglamento para el uso del laboratorio?	✓	
4. ¿Existe en el laboratorio instrucciones visibles de cómo manejar los equipos del laboratorio?		✓
5. ¿Usted conoce el proceso para reportar algún daño dentro del laboratorio?		✓
6. ¿Considera que el nivel de limpieza en el laboratorio es adecuado?	✓	
7. ¿Usted considera que los equipos se encuentran en buen estado?		✓
8. ¿Usted ha observado que se les dé mantenimiento a los equipos del laboratorio?		✓
9. ¿Se lleva a cabo un mantenimiento regular de la infraestructura eléctrica?		✓
10. ¿Considera que los cables del laboratorio están debidamente organizados?		✓
11. ¿Usted conoce si la institución cuenta con políticas de acceso al laboratorio?	✓	
12. ¿Usted ha observado si en el laboratorio existen equipos que están fuera de servicio y siguen dentro del laboratorio?	✓	

Ilustración 20. Aplicación de Encuesta a los docentes de la institución

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

Encuesta dirigida a: Los docentes de la institución educativa "Dr. José María Velasco Ibarra".

Objetivo: El objetivo de la encuesta es recopilar datos y obtener información específica sobre el laboratorio de computación.

PREGUNTAS	RESPUESTA	
	SI	NO
1. ¿Existen políticas de acceso y restricciones para garantizar la seguridad de los laboratorios de computación?		✓
2. ¿Usted conoce un reglamento para el uso del laboratorio?	✓	
3. ¿Le han socializado el reglamento para el uso del laboratorio?	✓	
4. ¿Existe en el laboratorio instrucciones visibles de cómo manejar los equipos del laboratorio?		✓
5. ¿Usted conoce el proceso para reportar algún daño dentro del laboratorio?		✓
6. ¿Considera que el nivel de limpieza en el laboratorio es adecuado?	✓	
7. ¿Usted considera que los equipos se encuentran en buen estado?		✓
8. ¿Usted ha observado que se les dé mantenimiento a los equipos del laboratorio?		✓
9. ¿Se lleva a cabo un mantenimiento regular de la infraestructura eléctrica?		✓
10. ¿Considera que los cables del laboratorio están debidamente organizados?	✓	
11. ¿Usted conoce si la institución cuenta con políticas de acceso al laboratorio?	✓	
12. ¿Usted ha observado si en el laboratorio existen equipos que están fuera de servicio y siguen dentro del laboratorio?	✓	

Ilustración 21. Aplicación de Encuesta a los docentes de la institución

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

Encuesta dirigida a: Los docentes de la institución educativa "Dr. José María Velasco Ibarra".

Objetivo: El objetivo de la encuesta es recopilar datos y obtener información específica sobre el laboratorio de computación.

PREGUNTAS	RESPUESTA	
	SI	NO
1. ¿Existen políticas de acceso y restricciones para garantizar la seguridad de los laboratorios de computación?	√	
2. ¿Usted conoce un reglamento para el uso del laboratorio?		√
3. ¿Le han socializado el reglamento para el uso del laboratorio?		√
4. ¿Existe en el laboratorio instrucciones visibles de cómo manejar los equipos del laboratorio?		√
5. ¿Usted conoce el proceso para reportar algún daño dentro del laboratorio?	√	
6. ¿Considera que el nivel de limpieza en el laboratorio es adecuado?		√
7. ¿Usted considera que los equipos se encuentran en buen estado?		√
8. ¿Usted ha observado que se les dé mantenimiento a los equipos del laboratorio?		√
9. ¿Se lleva a cabo un mantenimiento regular de la infraestructura eléctrica?		√
10. ¿Considera que los cables del laboratorio están debidamente organizados?		√
11. ¿Usted conoce si la institución cuenta con políticas de acceso al laboratorio?	√	
12. ¿Usted ha observado si en el laboratorio existen equipos que están fuera de servicio y siguen dentro del laboratorio?	√	

Ilustración 22. Aplicación de Encuesta a los docentes de la Institución

6.6 Glosario

A

auditoría
Revisión de los procedimientos que se llevan en una empresa a nivel contable o laboral entre otros, 5

C

ciberseguridad
es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos, 13
confidencialidad
garantiza que está accesible únicamente a personal autorizado, 1
controles
controlar que todas las actividades relacionadas a los sistemas de información automatizados, 13

D

disponibilidad
situación en la que se encuentra un recurso cuando se puede utilizar para los fines a los que está destinado., 1
dispositivos físicos
partes físicas tangibles de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos., 8

E

evaluación de los controles
proceso realizado por una organización para proporcionar cierto nivel de seguridad, 12

I

infraestructura
Es un conjunto de software, hardware, redes y servicios conectados que componen el entorno de TI de una organización, 6
integridad
cualidad de ser honesto, 1

S

seguridad
ausencia de riesgo, 13
seguridad informática
se encarga de mantener la confidencialidad de los datos de tu organización, 13

A

amenazas
como un peligro latente de que un evento físico de origen natural, 31
auditoría
Revisión de los procedimientos que se llevan en una empresa a nivel contable o laboral entre otros, 21

C

ciberseguridad
es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos, 29
controles
controlar que todas las actividades relacionadas a los sistemas de información automatizados, 85

D

dispositivos físicos

partes físicas tangibles de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos., 24

E

evaluación de los controles
proceso realizado por una organización para proporcionar cierto nivel de seguridad, 28

H

hallazgos
El que encuentra una cosa inanimada, que no pertenece a nadie, adquiere su dominio apoderándose de ella., 21

I

infraestructura
Es un conjunto de software, hardware, redes y servicios conectados que componen el entorno de TI de una organización, 22

M

mainframes
son computadoras de alto rendimiento con grandes cantidades de memoria y procesadores que procesan miles de millones de cálculos, 24
minicomputadoras
son un tipo específico de computadora multiusuario, ubicadas, en términos de proceso computacional, entre los grandes sistemas, 24

P

problemática
Que presenta un problema, que es difícil de solucionar o resolver., 21

R

riesgo
se define como el potencial de pérdida o daño cuando una amenaza detona una vulnerabilidad., 31

S

seguridad
ausencia de riesgo, 29
seguridad informática
se encarga de mantener la confidencialidad de los datos de tu organización, 29
sistemas
conjunto de elementos interrelacionados entre si para lograr un mismo objetivo, 23
software
Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora, 24

T

tecnologías
Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico., 26

V

valoración
revisión de todos los problemas de salud de los sistemas corporales, 23

A

amenazas
como un peligro latente de que un evento físico de origen natural, 31
auditoría
Revisión de los procedimientos que se llevan en una empresa a nivel contable o laboral entre otros, 21

C

ciberseguridad
es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos, 29
computación descentralizada
es un paradigma que permite el procesamiento distribuido y colaborativo de datos y tareas sin depender de una autoridad central o intermediario, 24
controles
controlar que todas las actividades relacionadas a los sistemas de información automatizados, 85

D

dispositivos físicos
partes físicas tangibles de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos., 24

E

eficiencia
Capacidad de disponer de alguien o de algo para conseguir un efecto determinado., 23
evaluación de los controles
proceso realizado por una organización para proporcionar cierto nivel de seguridad, 28

H

hallazgos
El que encuentra una cosa inanimada, que no pertenece a nadie, adquiere su dominio apoderándose de ella., 21

I

infraestructura
Es un conjunto de software, hardware, redes y servicios conectados que componen el entorno de TI de una organización, 22

M

mainframes
son computadoras de alto rendimiento con grandes cantidades de memoria y procesadores que procesan miles de millones de cálculos, 24
malware
Un programa malicioso, también conocido como programa maligno, 17
mantenimiento
Conjunto de operaciones y cuidados necesarios para que instalaciones, edificios, industrias, etcétera, puedan seguir funcionando adecuadamente., 19
minicomputadoras
son un tipo específico de computadora multiusuario, ubicadas, en términos de proceso computacional, entre los grandes sistemas, 24

P

problemática
Que presenta un problema, que es difícil de solucionar o resolver., 21

R

riesgo
se define como el potencial de pérdida o daño cuando una amenaza detona una vulnerabilidad., 31

S

seguridad
ausencia de riesgo, 29
seguridad informática
se encarga de mantener la confidencialidad de los datos de tu organización, 29
sistemas
conjunto de elementos interrelacionados entre si para lograr un mismo objetivo, 23
software
Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora, 24

T

tecnologías
Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico., 26

V

valoración
revisión de todos los problemas de salud de los sistemas corporales, 23