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 PREVIO A LA OBTENCIÓN DEL

TÍTULO DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

AUDITORIA INFORMÁTICA FÍSICA Y LÓGICA MEDIANTE EL USO DE METODOLOGÍA MAGERIT EN LA UNIDAD EDUCATIVA "ALESSANDRO VOLTA" PERIODO 2022

AUTORA:

GISSEL DAYANA ENCALADA MAZA

TUTOR:

A.S. WLADIMIR MINAYA MACÍAS, MG.

El Carmen, 2023

CERTIFICACIÓN DEL DIRECTOR DE TRABAJO DE GRADUACIÓN

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 2
		Página 1 de 1

CERTIFICACIÓN

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

Haber dirigido y revisado el trabajo de investigación, bajo la autoría del estudiante **ENCALADA MAZA GISSEL DAYANA**, legalmente matriculado/a en la carrera de Tecnologías de la Información, período académico 2022-2023, cumpliendo el total de 384 horas, bajo la opción de titulación de trabajo de Investigación, cuyo tema del proyecto es "Auditoria Informática para física y lógica mediante el uso de metodología Magerit en la Unidad Educativa "Alessandro Volta" periodo 2022.

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, 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, 22 de Febrero del 2023.

Lo certifico,

A.S. Wladimir Minaya Macías, Mg.
Docente Tutor
Área: Sistemas

DECLARACIÓN DE AUTORÍA

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: Auditoría informática física y lógica mediante el uso de metodología magerit en la Unidad Educativa "Alessandro Volta" periodo 2022, corresponde exclusivamente a: Gissel Dayana Encalada Maza con cédula de ciudadanía N° 230029199-0 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Gissel Encalada.

_____

GISSEL DAYANA ENCALADA MAZA

C.C 230029199-0

DEDICATORIA

El presente trabajo de titulación dedico con mis sentimientos infinito a mis familiares más cercanos, a mi padre Rodrigo Encalada, madre Gabriela Maza y a mi hijo Rodrigo Abad, con mucho amor, lo cual han sido mi motor en esta lucha larga de preparación, con su amor incondicional para lograr mis metas y objetivos. Con la fe y esperanza. Este gran triunfo es para mi padre.

Gracias, padre Rodrigo Encalada

Gissel Encalada.

AGRADECIMIENTO

Retribuyo mis agradecimientos, primeramente, a Dios por permitirme esta gran oportunidad y alcanzar cada objetivo, también mis padres, por la ayuda en todo el camino de preparación, con su ayuda incondicional, el cual me ha instruido de manera fundamental y mentalmente.

Agradezco al tutor a cargo al Ing. Wladimir Minaya por su contribución de sus conocimientos adquiridos profesionalmente, el cual fue fundamental en el proceso de elaboración y capacitación, en el presente trabajo de titulación.

Al rector de la Unidad Educativa “Alessandro Volta” al Mg. Fredy Ramos, por permitir la apertura de información para el proceso de investigación.

Expreso mi gratitud a cada docente por impartir sus conocimientos en mí, en lo largo de mi carrera universitaria.

Gissel Encalada.

Índice de contenidos

Índice tablas

Índice de figuras

Resumen

En el área de informática la auditoría surge cuando las organizaciones comienzan a tomar conciencia de que la información que adquieren, archivan digitalmente, procesan y emiten es un activo de gran importancia. La investigación se realizó con el desarrollo de una auditoría informática en la Unidad Educativa Alessandro Volta ubicada en Santo Domingo de los Tsáchilas. Se propone el desarrollo de una auditoría mediante el uso de la metodología Magerit en la unidad educativa en el periodo 2022. Entre los contenidos que se abordaron en la metodología es el tipo de investigación la cual fue mixta perteneciente al diseño no experimental, de carácter longitudinal y del tipo descriptiva, bibliográfica y de campo. Para calcular la muestra se tomó a las 127 personas que componen la población y como resultado se obtuvo una muestra de 62 personas que quedaron distribuidas de la siguiente manera: Rector, el docente de la materia de informática, 60 estudiantes (20 estudiantes por cada grupo, los tres años de bachillerato). Se utilizaron además como técnicas fundamentales la entrevista y la encuesta y para el desarrollo de la Auditoría informática la ficha de verificación de acuerdo a los principios de la metodología Magerit. Como parte del desarrollo una auditoría informática lógica y física mediante el uso de la metodología Magerit se presentan en la unidad educativa una probabilidad de ocurrencia de riesgo de media a alta y un impacto de media a muy alto en la mayoría de los criterios evaluados.

Palabras clave: auditoría informática, impacto, metodología Magerit, probabilidad de ocurrencia, riesgo.

Abstract

In the IT area, the audit arises when organizations begin to become aware that the information they acquire, digitally archive, process and issue is an asset of great importance. The research was carried out with the development of a computer audit at the Alessandro Volta Educational Unit located in Santo Domingo of the Tsáchilas. The development of an audit is proposed through the use of the Magerit methodology in the educational unit in the period 2022. Among the contents that were addressed in the methodology is the type of research which was mixed belonging to the non-experimental design, of a longitudinal nature. and of the descriptive, bibliographic and field type. To calculate the sample, the 127 people that make up the population were taken and as a result a sample of 62 people was obtained, distributed as follows: Rector, the computer science teacher, 60 students (20 students for each group, the three years of high school). The interview and the survey were also used as fundamental techniques and for the development of the computer audit the verification sheet according to the principles of the Magerit methodology. As part of the development of a logical and physical computer audit through the use of the Magerit methodology, a medium to high probability of risk occurrence and a medium to very high impact is presented in the educational unit in most of the criteria evaluated.

Keywords: computer audit, impact, Magerit methodology, probability of occurrence, risk.

CAPÍTULO I: INTRODUCCIÓN

1.1 Introducción

En el mundo una práctica muy utilizada para mejorar los servicios y la satisfacción de los clientes es realizar Auditoría sean internas o externas. Un caso particular de las auditorías las tiene la de carácter informático, porque se asegura la seguridad de toda la información y se está conectado en red, con todo el entorno productivo, de servicios y empresariales. Estos resultados garantizan mayores reconocimientos y con ello un prestigio superior logrando ser más competitivos en el mercado. De acuerdo con lo planteado con Yangua (2014) en las Auditorías informáticas ocurre un hecho que, en definitiva, las amenazas en una empresa pueden darse de diferentes maneras o situaciones por lo que cada organización tiene la obligación de resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad y la integridad de esta.

En América Latina con el auge de las Tecnologías de Información y las Comunicaciones los Gobiernos establecen leyes y normas legales para la protección de sus informaciones, todo lo cual ayuda con la utilización de Tecnologías de Información robustas para minimizar o controlar las "amenazas tecnológicas que son parte de la cotidianeidad y más aún de la vida organizacional" (Valencia y Orozco, 2017, p. 74). En este sentido desarrollar de forma oportunas las Auditorías informáticas resultan de gran utilidad para la toma de las decisiones siendo un caso poco común en las últimas décadas, pero en la actualidad logran resultados satisfactorios, con estas los directivos, empresarios y líderes logran tomar el rumbo de sus acciones y con ello llevar al éxito de sus instituciones y organizaciones.

Para el caso del Ecuador la auditoría informática, se ha convertido en un factor importante, para las empresas, instituciones y organizaciones, en la actualidad se quiere como en el resto de todo el mundo salvaguardar, proteger la información, los recursos de las empresas y controlar las actividades desarrolladas. La presente investigación se realizó con el objetivo de desarrollar una Auditoría informática física y lógica mediante el uso de la metodología Magerit en la Unidad Educativa "Alessandro Volta" periodo 2022. Para ello se toman en cuenta los elementos metodológicos de la Universidad Laica Eloy Alfaro de Manabí (Uleam) Extensión de "El Carmen" en su carrera de Tecnologías de la Información para la elaboración de este tipo de estudios.

Como principales aspectos de la metodología se resaltan los siguientes: coincidiendo con lo planteado por Hernández y Mendoza (2018), la investigación

pertenece al enfoque mixto (cuali-cuantitativo), es del diseño no experimental, de carácter longitudinal y del tipo descriptiva, bibliográfica y de campo. Entre los Métodos de investigación utilizados se resaltan: Analítico-sintético y el Inductivo –deductivo,

Entre las fuentes de información de datos se encuentra de forma primaria la entrevista, y de forma secundaria la encuesta. Para la fase de recopilación de información se utilizaron las técnicas de la encuesta tipo cuestionario (encuestas semiestructuradas con preguntas abiertas y cerradas) y entrevista (semiestructuradas), el instrumento que se va a utilizar es el cuestionario.

Se tomó como población a los 125 estudiantes de bachillerato (1ro, 2do y 3ro), el Rector y un docente que imparte la materia informática, teniendo un total de 127 personas. Para el presente estudio la unidad educativa "Alessandro Volta" constituyó el proceso segmentado a partir de la muestra utilizada en los laboratorios de informática.

Como parte de la tabulación y análisis de los datos que está dividido por el número, la pregunta, respuesta del entrevistado y la interpretación de las misma por parte de la investigadora y el equipo de investigación. La entrevista fue dirigida al Rector y al encargado de laboratorios de computación con el objetivo de realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad Educativa Alessandro Volta cómo de los programas que se usan.

Los resultados fueron divididos en bloques para conocer la percepción de cada grupo, respecto a sus expectativas, intereses y los ítems que aparecen reflejados en cada una de las cuatro figuras. Este instrumento fue aplicado a 60 estudiantes del 1ero, 2do y 3ro de bachillerato de la unidad educativa, con lo cual se obtienen las figuras. Como consecuencia, los datos observados y los datos de entrevista se codifican y se analizan separadamente, y luego se comparan, sustentados por los fundamentos teóricos, como una manera de validar los hallazgos.

Se reconoce que, como parte de los resultados de los instrumentos aplicados no tiene implementada un plan de control de riesgos sobre todo en la seguridad informática. Un gran porcentaje de sus miembros desconocen de estas prácticas; adicionalmente, se rescata el impacto que tiene la implementación de la auditoría informática como herramienta para mejorar gestión de control de riesgo.

En la investigación se desarrolla una auditoría informática física y lógica para reducir o controlar los riesgos que se manifiesten durante la investigación relacionados con la seguridad informática. Para su desarrollo se empleó la metodología Magerit que permite el análisis y gestión de riesgo del equipamiento tecnológico de la Unidad

Educativa “Alessandro Volta”. En el estudio se revela la realidad sobre la gestión de riesgos y los datos en la unidad educativa, puesto que no tiene implementada un plan de control de riesgos sobre todo en la seguridad informática en los laboratorios de computación. El objetivo específico está fundamentado en calcular la estimación del riesgo modelando impacto, probabilidad y riesgo por medio de escalas cualitativas en la unidad de análisis.

La etapa de planificación en la auditoría se cuenta con cinco pasos fundamentales desde la conceptualización, los instrumentos, los criterios de evaluación según la metodología Magerit, la aplicación y tabulación de datos, por último, el informe de auditoría que culmina en los resultados de la auditoría y las conclusiones. La auditoría está estructurada en el objetivo general, objetivo específico, los procedimientos o pasos de la metodología y los códigos para cada uno de los procedimientos.

1.2 Presentación del tema

El tema planteado se denomina “Auditoría informática física y lógica mediante el uso de la metodología Magerit en la unidad educativa “Alessandro Volta” periodo 2022”.

1.3 Ubicación y contextualización de la problemática

La Unidad Educativa Alessandro Volta fue fundada en el año 1984 con el nombre de Colegio Nacional Santa Martha bajo el Acuerdo Ministerial 3879. La Unidad Educativa es una institución que se encarga de formar y capacitar bachilleres técnicos comprometidos al desarrollo nacional, lo que le ha permitido tener una gran acogida y crecer institucionalmente. Se encuentra ubicada en la Cooperativa Santa Martha sector 3 en la Av. Jacinto Cortez y los Quinches, del cantón de Santo Domingo de los Tsáchilas, cuenta en la actualidad con 47 colaboradores teniendo como actividad principal la educación.

1.4 Planteamiento del problema

En este contexto, la investigación se realizó con el desarrollo de una auditoría informática en la Unidad Educativa Alessandro Volta ubicada en Santo Domingo de los Tsáchilas por medio de un oficio de secretaria se dio el beneplácito para realizar dicha actividad durante el periodo 2022.

Por ello se busca conocer, prevenir, impedir, reducir o controlar los riesgos que se manifiesten durante la investigación relacionados con la seguridad informática de manera que se pueda elaborar un informe de activos que se encuentran en la unidad educativa en donde garantice la autenticación, confidencialidad, integridad y

disponibilidad de los sistemas de información y generen confianza cuando se utilice estos medios.

Por ese motivo, es de suma importancia aplicar una auditoría informática para el desarrollo de un trabajo de titulación, tomando como referencia las medidas que formen parte de las instalaciones informáticas que se aplican en el entorno autorizado para el acceso de los usuarios a la información.

Cualquiera sea la causa de la suspensión de un servicio de tecnología, genera pérdida de recursos, así como malestar entre los clientes internos y proveedores por falta de herramientas y servicios para la ejecución normal de sus actividades.

Los resultados evidencian que las buenas prácticas de enseñanza desarrolladas en los talleres y laboratorios del Bachillerato en Informática son realizadas por docentes que trabajan o trabajaron en un área de informática afín a la asignatura que enseñan y pueden transferir sus experiencias laborales a los jóvenes.

Por consiguiente, los docentes poseen buena capacidad de comunicación, conocen la disciplina técnica que enseñan y planifican para secuenciar los contenidos. Asimismo, evalúan las actividades prácticas, observando como el estudiante aplica los conocimientos en un problema real del campo profesional y realiza un mantenimiento adecuado del equipamiento.

Los docentes, utilizan fundamentalmente estrategias de enseñanza que se explican en el cuerpo del trabajo, y que se ven potenciadas cuando se dispone de talleres y laboratorios bien equipados que cumplen con las normas de seguridad, pero también, cuando el equipo de dirección del centro educativo está comprometido con su mantenimiento.

Para alcanzar la meta de mejorar las prácticas de enseñanza en la Educación Media en el Ecuador, es necesario investigar, encuestando, observando e entrevistando a los docentes que imparten sus clases en los talleres y laboratorios, para conocer las características que presentan las buenas prácticas de enseñanza en esos espacios áulicos donde se desarrollan actividades de la práctica profesional específica, que suelen ser muy diferentes a las que se desarrollan en los salones de clases teóricas.

Se identificó una serie de debilidades, tales como: inexistencia de un plan de contingencia ante cualquier anomalía que presente el área informática y ausencia de un registro de inventarios informáticos. Se determinó que la Unidad Educativa no cuenta con un sistema control interno informático lo que originó el incumplimiento de las normas de control interno de la Contraloría General del Estado.

El procedimiento de auditoría permite extraer tanto las debilidades como fortalezas de las instituciones, con la intención de mejorar constantemente todo lo que involucra la calidad de servicio. Buscando establecer un vínculo cercano entre el servicio y la satisfacción del cliente.

1.4.1 Problematización

En consecuencia, se busca realizar un informe que se lleve a cabo por la administración educativa para el cual mejoren las actividades planificadas por los encargados de los laboratorios, en donde el principal problema es el uso inadecuado y deterioro de los equipos de cómputo con la mala utilización ya sea por la copia de programas para fines comerciales sin reportes de los derechos de autor o ya sea por los tiempos de maquina en el uso de aplicaciones en determinados usos de tiempo. Ante los elementos antes descritos se propone como problema: ¿Cómo reducir o controlar los riesgos relacionados con la seguridad informática de la Unidad Educativa Alessandro Volta ubicada en Santo Domingo de los Tsáchilas?

1.4.2 Génesis del problema

La tecnología es indispensable para el ejercicio de cualquier profesión, el desarrollo de la sociedad y los cambios tecnológicos han ido surgiendo con el tiempo como herramientas facilitadoras del manejo de la información. La génesis del problema es: insuficiencia en el funcionamiento y deterioro de los equipos informáticos en la Unidad Educativa Alessandro Volta ubicada en Santo Domingo de los Tsáchilas

1.4.3 Estado actual del problema

Con el objetivo de satisfacer las necesidades de la Unidad Educativa Alessandro Volta, ubicada en Santo Domingo de los Tsáchilas se busca realizar una auditoría informática lógica y física de los componentes que se encuentran en ese establecimiento, para ello se hizo el oficio correspondiente al rector de la institución, con la intención de analizar todas las actividades, para optimizar todos los procesos que se llevan a cabo en el laboratorio, de otra manera tener presentes los riesgos que se genera en las computadoras tanto en la seguridad física como lógica. Sin embargo, se trata de demostrar de manera verosímil la documentación de modo que se pueda referenciar alguna falencia en los procesos.

De forma probable puede existir: insuficiencia de una planificación y gestión de los equipos informáticos, falta de espacio en las áreas de laboratorios en donde se pueda agilizar las actividades que se realizan a diario, mala configuración en las redes de acceso público, deficiencia de seguridad de los equipos informáticos que se encuentran

vulnerables, error de actualización de los equipos, mala documentación de los equipos en buen y mal estado en donde el personal no cuenta con las herramientas y el tiempo necesario para llevar a cabo la documentación que quiere constatar en la investigación de manera que se pueda mejorar los inconvenientes relacionados con los activos de información que se encuentran en la institución.

Por esa razón, se propone el tema mencionado con la finalidad establecer dicha auditoría con la metodología Magerit, teniendo en claro la recopilación de la información obtenida mediante la secretaria de la institución que proporcionó datos de gran relevancia, cabe destacar también que se realizó una previa documentación establecida durante la investigación.

1.5 Diagrama causa – efecto del problema

En la figura 1 se muestra el diagrama causa –efecto del problema a partir de los resultados diagnosticados en la Unidad Educativa Alessandro Volta ubicada en Santo Domingo de los Tsáchilas.

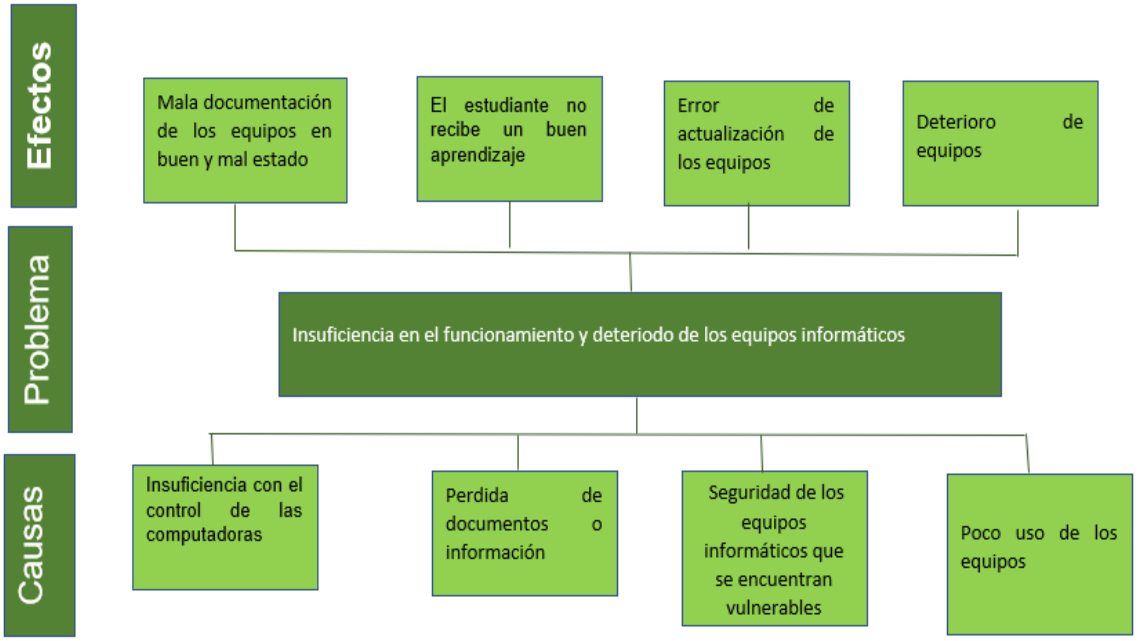


Figura 1. Diagrama causa – efecto del problema en la Unidad Educativa Alessandro Volta" durante el periodo 2022.

Fuente: Elaboración propia.

1.6 Objetivos

1.6.1 Objetivo general

Desarrollar una Auditoría informática lógica y física mediante el uso de la metodología Magerit en la Unidad Educativa "Alessandro Volta" durante el periodo 2022.

1.6.2 Objetivos específicos

- Sistematizar los fundamentos teóricos referidos a las variables de estudio: auditoría informática y equipos informáticos.
- Diagnosticar la situación actual de los laboratorios de la Unidad educativa Alessandro Volta y de los programas que se usan.
- Realizar un análisis de riesgos de los equipos informáticos que se encuentran dentro de la "Unidad Educativa Alessandro Volta" mediante la auditoría informática con el empleo de la metodología Magerit.
- Elaborar el informe de la auditoría.

1.7 Justificación

En los últimos tiempos las instituciones educativas han venido suscitando inconvenientes durante la pandemia, de forma especial en estos últimos dos años, la mayoría de las personas se encontraban con restricciones e inmovilidad al establecimiento para llevar el debido control de los equipos informático de las instituciones.

Según Ferro (2020), define a la auditoría informática como un proceso determinado por profesionales o especialistas que permite la recolección, agrupación y evaluación de seguridades para establecer si un sistema de información cuenta con su respectivo ámbito económico o financiero. Por otra parte, el autor Pintos Gómez, 2022, establece que la auditoría física en redes garantiza la estructura física de la instalación TIC/SI, en la Auditoría lógico es importante monitorizar la error o situaciones anómalas que se ocasionan con la finalidad de evitar un daño interno.

Cabe mencionar, que la Unidad Educativa "Alessandro Volta" no cuenta con su correspondiente control de Auditoría informática debida a la pandemia, con lo cual se determina la necesidad de establecer dicha autoría, con el objetivo que la institución se beneficie. En la búsqueda de las fuentes bibliográficas de la Universidad Laica Eloy Alfaro de Manabí (Uleam) se ha encontrado tesis relacionado con el tema mencionado sobre auditoría informática, pero no se ha encontrado una Auditoría en la Unidad Educativa. Como resultado de la correspondiente búsqueda se puede definir como necesaria y oportuna esta propuesta, porque no cuenta con un trabajo de tesis que pueda ayudar con esta investigación formal.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

El impacto de la tecnología de información en las organizaciones para optimar sus procesos ha llevado a establecer técnicas dentro de una revisión de auditoría, las cuales

ayudan a otorgar confianza en el correcto uso de la tecnología y repercuten en el ambiente de control y en los registros contables financieros (Morales, 2019). Por ello la información digital se ha convertido en un elemento importante dentro de las organizaciones, de ahí la calidad, veracidad y oportunidad de esta, para facilitar la toma de decisiones y correcta disposición de la información.

Los auditores tienen la necesidad de hacer frente a este nuevo reto de la profesión y así poder tomar ventaja en el almacenaje digital de los diferentes sistemas, sin embargo, en esta nueva tendencia relacionada con el manejo de grandes volúmenes de información se observa un escaso desarrollo y entrenamiento en herramientas para los llamados Procedimientos de Auditoría Asistidos por el Computador (PAAC), los cuales son usados en auditoría para:

- ✓ Verificación: comprobación de cálculos y totales.
- ✓ Revisión analítica: comparaciones, variaciones, estadísticas.
- ✓ Validez: duplicados, excepciones, muestreos estadísticos.
- ✓ Integridad: omisiones, duplicidad, coincidencias de datos.
- ✓ Cortes: análisis secuencial de folios y fechas.
- ✓ Valuación: cálculos aritméticos, descuentos, bonificaciones.

1.8.2 Impacto social

El principal impacto social que tiene la auditoría informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos, a partir del juicio crítico de los auditores al analizar las condiciones de una instalación informática sea personal externo o interno quien realiza un dictamen sobre distintos aspectos informáticos (Otero, 2020).

Para ello queda evidenciado el carácter humanista de esta profesión a partir de poner en asiento los principales valores humanos que deben poseer en todo momento, con énfasis en la claridad del trabajo desarrollado, profesionalidad, calidad y transparencia de los informes finales.

A partir de este análisis se deben desarrollar un conjunto de recomendaciones que aborden estas deficiencias y así mejorar la gestión de riesgos de los datos. Estas acciones finalmente llevan al aumento de la confianza en el desarrollo de actividades y un mayor rendimiento de las organizaciones, tales como:

- ✓ Mejora la continuidad del negocio.
- ✓ Reduce significativamente los riesgos con respecto a la gestión de las tecnologías.

- ✓ Contribuye como insumo necesario para la toma de decisiones.
- ✓ Mejora la administración de riesgos de la organización y sus activos.
- ✓ Aumenta de la eficiencia de los servicios informáticos de la organización.
- ✓ Mejora el soporte, es las tareas habituales de la información.
- ✓ Mejora la productividad de la organización, en especial del área en las cuales se enfocó la auditoría.
- ✓ Diferencia de la competencia a nivel local y nacional.
- ✓ Se reducen los costes externos en función de los peligros que se producen en los sistemas de datos.

1.8.3 Impacto ecológico

El impacto ecológico de las tecnologías de la información y las comunicaciones está muy ligado a la definición de la contaminación atmosférica como la presencia en el aire de materias o formas de energía que impliquen riesgo, daño o molestia grave para las personas y bienes de cualquier naturaleza, en este sentido énfasis en las computadores y equipos electrónicos utilizados por el hombre. Como parte de las estrategias para disminuir su impacto se reflejan algunas de las acciones a tener en cuenta:

- ✓ Búsqueda, selección y valoración de las diferentes fuentes de información relacionadas con el medio ambiente y el impacto de las tecnologías (revistas, libros, publicaciones oficiales, internet, etc.)
- ✓ Reducir cada vez se consumen más aparatos y se sustituyen con mayor celeridad.
- ✓ Reutilizar. Los expertos en reciclaje electrónico recomiendan que amigos o familiares hereden los aparatos que todavía funcionan, o que se oferten en el mercado de segunda mano.
- ✓ Configurar al ordenador y dispositivos para que pasen a un modo de bajo consumo cuando lleven un cierto periodo de tiempo sin utilizarse.
- ✓ Para imprimir documentos que no requieren una presentación perfecta, se puede reutilizar papel con sólo una cara impresa
- ✓ Diseñar y fabricar aparatos con una vida útil lo más larga posible y restringir la utilización de determinadas sustancias peligrosas.
- ✓ Reciclar todas las tecnologías disponibles al alcance del hombre.
- ✓ Substituye tus sistemas de archivo en papel por sistemas de archivo en unidades de almacenamiento informático: memorias flash, CD-ROMs, discos duros

CAPÍTULO II: MARCO TEÓRICO DE LA INVESTIGACIÓN (FUNDAMENTACIÓN CONCEPTUAL)

2.1 Antecedentes históricos

En la búsqueda de la literatura, de forma conceptual la auditoría según Piattini et al. (2008), es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Según Sandoval (2012), señala que: el término auditoría, en su acepción más amplia, significa verificar que la información financiera, administrativa y operacional que se genera es confiable, veraz y oportuna. Es revisar que los hechos, fenómenos y operaciones se den en la forma en que fueron planteados, que las políticas y procedimientos establecidos se han observado y respetado. (p. 9)

Por su parte Sunkel et al. (2016), argumentan que la auditoría informática tiende a: "definir políticas más agresivas de equidad en el acceso a las tecnologías de la información y comunicación (TIC) y en su uso efectivo, especialmente en educación". (p. 166 – 167).

En el mismo orden de idea para González (2017), la auditoría informática se define como: un examen metódico, puntual y discontinuo que verifica y evalúa; destinada a la ayuda en la mejora de la seguridad, eficacia, eficiencia y rentabilidad de los sistemas de información de la organización, establece en opinión objetiva fundada en las evidencias, con unos objetivos muy concretos; mejorar la eficacia en la organización de los sistemas de información, para proteger los activos y recursos; garantizando resultados fiables en el tiempo, costos y utilidad. Mejorar los procedimientos, estándares y planificación colaborando en su diseño y en la actualización de sus normas.

La auditoría informática es verificar, evaluar, revisar en el desempeño de todos los sistemas de información de una organización, con el objeto de mejorar su rendimiento, seguridad, e integrar controles para interactuar eficientemente con su entorno a la par de sus fortalezas y debilidades (Arcentales y Caycedo, 2017).

Para Jiménez y Benavides (2012), manifiesta que unos de los objetivos de la Auditoría, "consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades. Para ello la auditoría les proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas". (p. 6)

Es criterio de Iturralde (2018), que en el Ecuador en las tomas de decisiones la auditoría informática se encarga de recopilar información necesaria y así poder evaluar el sistema y controles informáticos; equipos de cómputo y en especial dar seguridad de los recursos informáticos y así obtener información o argumentos críticos en beneficios de las empresas.

2.2 Antecedentes de investigaciones relacionadas al tema presentado

2.2.1 Auditoría informática

2.2.1.1 Introducción de Auditoría

En el área de informática la auditoría surge cuando las organizaciones comienzan a tomar conciencia de que la información que adquieren, archivan digitalmente, procesan y emiten es un activo de gran importancia. Es en este momento cuando las instituciones y empresas comienzan a reconocer que su credibilidad ante la sociedad está muy asociada a la protección que ofrecen a la información de sus usuarios y por ende a los equipos que la conservan (Ortiz y Ayala, 2019).

2.2.1.2 Definición de Auditoría informática

La auditoría informática es entendida como el conjunto de métodos, procedimientos, técnicas y herramientas que permiten a una organización realizar la evaluación de sus controles sobre el sistema informático y determinar el nivel de protección de sus activos y recursos, encontrando anomalías en la seguridad, pues en la mayoría de los casos es esta el área auditable. La auditoría informática tiene sus etapas y cuenta con actividades que se desarrollan basadas en un método de trabajo formal donde los auditores informáticos emplean técnicas y herramientas propias de la auditoría; estás técnicas y herramientas pueden ser tanto las buenas prácticas como los estándares internacionales. En la auditoría la organización verifica si sus actividades se desarrollan eficientemente y si se cumple con la normativa informática estandarizada para el logro de la eficacia (Chuquín, 2020).

2.2.1.3 Tipos de Auditoría informática

2.2.1.3.1 Auditoría Informática de Explotación

La auditoría informática de explotación consiste en auditar las secciones que componen la explotación y sus interrelaciones. La Explotación Informática se concreta en tres áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos, donde todos son auditables. En este tipo de auditoría se evalúan los resultados informáticos de todo tipo: listados impresos, ficheros soportados

magnéticamente para otros informáticos y órdenes automatizadas para lanzar o modificar procesos industriales (Salgado et al., 2017).

2.2.1.3.2 Auditoría Informática de Desarrollo de Proyectos o Aplicaciones

La auditoría informática de desarrollo de proyectos o aplicaciones es la encargada de comprobar la seguridad de los programas con la intención de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros. Una auditoría de Aplicaciones pasa por la observación y el análisis de cuatro consideraciones (Fernández y Casas, 2017).

2.2.1.3.3 Auditoría Informática de Sistemas

La auditoría informática de Sistemas es la que analiza la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Dada la importancia que hoy tienen las telecomunicaciones y su creciente uso al momento de realizar las auditorías ha sido necesario separar el entorno general de sistemas, comprendido por las Comunicaciones y las Líneas y Redes de las instalaciones informáticas, para así poder realizar un control más profundo y obtener mejores resultados (Martínez et al., 2012).

2.2.1.3.4 Auditoría Informática de Comunicaciones y Redes

La conceptualización de la auditaría informática de Comunicaciones y Redes parte de reconocer que al abordar el tema redes en términos informáticos auditables se refiere al soporte físico- lógico del tiempo real, donde el auditor enfrenta dificultades técnicas del entorno. Este tipo de auditoría analiza situaciones y hechos alejados entre sí, por eso requiere de un equipo de especialistas y expertos en comunicaciones y en redes (Rodríguez, 2012).

2.2.1.3.5 Auditoría de la Seguridad Informática

La auditoría de la seguridad informática puede ser una auditoría de seguridad general de una instalación informática o auditorías específicas que se direccionan a la seguridad de un área informática determinada; en ambos casos abarca la seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los contiene, tomando en cuenta las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. La seguridad lógica se refiere a la seguridad uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información (Santana, 2018).

2.2.1.3.6 Auditoría de seguridad física y auditoría de seguridad Lógica

La auditoría en seguridad física es aquella actividad que controla, verifica, califica, supervisa, analiza y recomienda, sobre el estado actual de seguridad en sus instalaciones e infraestructura, sean estas empresariales, industriales, o de cualquier otra naturaleza. En cambio, la auditoría de seguridad lógica es el proceso mediante el cual se controla y verifica aquellos accesos que han sido diseñados para salvaguardar la integridad de la información almacenada en diferentes medios (Párraga y Castillo, 2014). Al concluir cada auditoría se emite un informe con la evaluación de la situación actual en términos de seguridad, este se convierte en una herramienta, pues brinda a los directivos información necesaria para la toma de decisiones (Zambrano, 2020).

2.2.2 Análisis de riesgos

El análisis de riesgos es ampliamente utilizado y considerado como uno de los elementos fundamentales dentro de cualquier proceso de implantación de un sistema de gestión de seguridad de la información, porque es ahí donde se cuantifica la importancia que tienen los activos para la seguridad de cualquier organización. Los resultados del análisis de riesgos permiten a la gestión de los mismos recomendar las medidas adecuadas para controlar los riesgos identificados y poder reducir sus posibles daños. Es aplicado en recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, entre otras áreas (Alvarado et al., 2018).

2.2.3 El plan de la Auditoría

El plan de auditoría inicialmente presenta el tipo de auditoría que se desarrollará, contempla los componentes que serán auditados y determina los procedimientos específicos que se emplearán para cada uno de ellos. Este plan no es más que la descripción de las actividades y de los detalles que se van a examinar en la auditoría, en él se define que se va a auditar, cómo se va a auditar, y el alcance de la misma; además, se mencionan los objetivos de la Auditoría, el tiempo que durará y los responsables de cada acción planificada (Bravo y Giler, 2021).

2.2.4 Ejecución de la Auditoría

Antes de realizar una auditoría informática es necesario organizar correctamente y con una secuencia lógica las actividades que se realizarán. Estas deben plantearse teniendo en cuenta las necesidades específicas de la empresa o institución donde será aplicada. Existen tres etapas generales en la metodología de una auditoría informática: planeación, ejecución y dictamen como se muestra en la siguiente tabla 1 (Tobar y Ordoñez, 2015).

Tabla 1. Etapas de una auditoría informática

Etapas	Pasos a realizar
Planeación de la Auditoría de Sistemas	1. Identificar el origen de la auditoría.
	2. Realizar una visita preliminar al área que será evaluada.
	3. Establecer los objetivos de la auditoría.
	4. Determinar los puntos que serán evaluados en la auditoría.
	5. Elaborar planes, programas y presupuestos para realizar la auditoría.
	6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.
	7. Asignar los recursos y sistemas computacionales para la auditoría.
Ejecución de la Auditoría de Sistemas	1. Realizar las acciones programadas para la auditoría.
	2. Aplicar los instrumentos y herramientas para la auditoría.
	3. Identificar y elaborar los documentos de oportunidades de mejoramiento encontradas.
	4. Elaborar el dictamen preliminar y presentarlo a discusión.
	5. Integrar el legajo de papeles de trabajo de la auditoría
Dictamen de la Auditoría de Sistemas	1. Analizar la información y elaborar un informe de situaciones detectadas.
	2. Elaborar el Dictamen final.
	3. Presentar el informe de auditoría.

Fuente: (Tobar y Ordoñez, 2015)

2.2.5 Definición de la metodología

La metodología es la que ofrece al auditor la posibilidad de proyectar el objetivo de la auditoría, hacia donde deben ir orientadas las actividades, cómo plantearlas, las fechas de inicio y culminación; permite justificar porque se deben desarrollar las actividades planificadas, quienes deben comprometerse con su desarrollo, incluso permite plantear los argumentos que justifican el resultado de la auditoría. Para el empleo de una metodología se requiere de herramientas de apoyo, una de las más efectivas son las buenas prácticas. Puede decirse que se está empleando una adecuada metodología cuando esta ofrece un alto nivel de confiabilidad (Trujillo et al., 2020).

2.2.6 ISO 27001: El método MAGERIT

ISO 27001:2013 es la Norma Internacional que propicia la correcta implementación de un SGSI (sistema de gestión de la seguridad informática), busca la confidencialidad, disponibilidad e integridad de los activos de información. La Norma

ISO 27001 es la apropiada para prevenir la pérdida de la información e indisponibilidad de los equipos tecnológicos; además ofrece al auditor la posibilidad de entregar a los directivos de organizaciones un informe que le genere alertas y le permita tomar decisiones (Solarte y Rosero, 2015; Alvira, 2021).

Puede decirse que este estándar se centra en la búsqueda de la calidad de los procesos de las empresas e instituciones, reduce el impacto de los posibles riesgos y amenazas con la incorporación de medidas de seguridad. Este método garantiza la estabilidad de los procesos y por ende aporta significativamente al prestigio de las organizaciones ante sus clientes.

2.2.6.1 Requisitos principales de la norma ISO 27001

Con la Norma ISO 27001 se evalúa el rendimiento o efectividad del SGSI o de la Seguridad de la información y se tiene a la auditoría como la principal herramienta para medir la calidad y efectividad del SGSI. Para realizar las auditorías se toman como base los requisitos de la Norma porque el proceso de evaluación se centra en medir como se han cumplido en la organización estos requisitos y los requisitos específicos de la seguridad de la información que se hayan desarrollado en la entidad. De los cinco grupos de procesos importantes del SGSI según la norma ISO 27001, tenemos el proceso de auditoría y revisión del sistema, estos siguen siendo métodos importantes para evaluar la estabilidad del SGSI y ofrecer las alternativas para su perfeccionamiento (NORMA ISO 27001, 2020).

2.2.6.2 El método MAGERIT

Las siglas del método Magerit significan Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones. Es preciso destacar que este método abarca la fase AGR (Análisis y Gestión de Riesgos). Si se habla de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, esta influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. El objetivo perseguido en sucesivas versiones de MAGERIT es la evaluación, homologación y certificación de Seguridad de Sistemas de Información (SSI) según ISO 27001 (ISOTools Excellence, 2015).

2.2.6.3 Fases de la metodología MAGERIT

La metodología de Magerit según plantea Avila y Cuenca (2021), se puede dividir en cinco pasos fundamentales tal como se muestra en la ilustración 1.

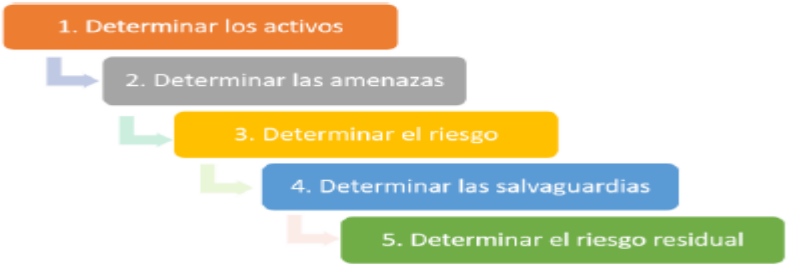


Ilustración 1. Pasos Metodología Magerit.

Fuente: (Avila y Cuenca, 2021)

Para determinar los activos es recomendable realizar una visita técnica a la empresa o institución auditada y así tener un control de sus insumos y organizar en orden de prioridad los activos tomando en cuenta su importancia dentro de la institución, de acuerdo con sus dimensiones de integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad, según lo establece la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012).

El estudio de amenazas y vulnerabilidades de activos se desarrolla separando las amenazas de las vulnerabilidades. Es preciso destacar que estas amenazas y vulnerabilidades pueden estar provocadas por varias causas: desastres naturales, de origen, errores, por fallos, ataques intencionados, correlación de errores y taques, nuevas amenazas y nivel de la amenaza; tal como se establece la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012).

En el caso del análisis y evaluación de riesgos el estándar Magerit facilita la valoración de estos en cada criterio de información evaluado, identificando las posibles causas que los originan de acuerdo con el impacto ponderado con la tasa de ocurrencia; según lo estipula la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012).

Cabe destacar que, en las empresas la reducción de riesgo inherente se realiza desde el análisis de las salvaguardias existentes en la empresa, para ello se emplean procedimientos y se aplican medidas o mecanismos tecnológicos.

En este orden de ideas, luego de realizar las salvaguardas existentes en la empresa, se realiza el proceso de análisis y evaluación de riesgos inherentes, para así determinar el riesgo residual de los activos.

Al concluir con todos los pasos de la metodología Magerit se desarrollan las contramedidas que se concretan en la determinación de posibles soluciones a los riesgos

residuales identificados para su posible mitigación tomando como Norma la ISO-IEC 27001, específicamente enfocados en su anexo A (Objetivos de control y Controles de Referencia).

2.2.7 Equipos informáticos

2.2.7.1 Definición de equipos informáticos

Los equipos informáticos son esos dispositivos que unidos al ordenador conforman un espacio de trabajo. En la actualidad estos equipos son cada vez más portables lo que motiva su uso y existe una gran diversidad de ellos. Se diferencian en forma y funciones y su uso oportuno ha demostrado su efectividad para automatizar y viabilizar procesos (Rodriguez, 2018).

2.2.7.2 Función de los equipos informáticos

El uso de equipos informáticos se hace cada vez más frecuente ante la digitalización de la información y los servicios. Con su empleo se mejora la productividad, pues se logra procesar un gran volumen de información y automatizan los procesos. Es a través de los equipos informáticos que la información puede llegar a cualquier lugar y de manera simultánea a varios usuarios; además propician el intercambio de información entre los usuarios y los dispositivos; facilitan la comunicación tanto personal como académica, administrativa y de otra índole (Cáceres, 2021). Es preciso destacar que los equipos informáticos tienen alta capacidad de funcionamiento por eso procesan cantidades de información a una gran velocidad, así mismo pueden recibir órdenes con respuesta rápida (Pincay, 2021).

2.2.8 Gestión de Tecnología de la Información

Para referirse a la gestión de Tecnología de la Información (TI) antes hay que mencionar que estas son las herramientas y métodos utilizados para recabar, retener, manipular o distribuir información. Mayormente las TI se encuentran relacionadas con las tecnologías asociadas a la toma de decisiones y a las computadoras.

La gestión de TI es el conjunto de procedimientos y acciones que se realizan ajustadas a un estándar con la finalidad de institucionalizar las buenas prácticas de planificación y organización, adquisición e implementación, entrega de servicios, soporte, y monitoreo del rendimiento de TI; todas estas buenas prácticas se gestionan con la intención de asegurar que la información administrada y las tecnologías empleadas en organizaciones soporten los objetivos estratégicos que en esta se plantean (Aponte y Cuenca, 2021).

En una gestión de TI correctamente proyectada se tienen en cuenta los tres pilares de la seguridad: confiabilidad, integridad y disponibilidad (Morán et al., 2018). Esta gestión parte de una evaluación o levantamiento de información, que permita conocer en qué estado se encuentra todo lo correspondiente a las TI en una empresa o institución determinada. Luego de tener el diagnóstico se realiza una proyección de lo que se debe hacer para gestionar las TI y en función de ello se modela o se plantea una estrategia que contiene el procedimiento a seguir, con hojas de ruta o planes de acción que permitan atender las particularidades de las TI en el contexto abordado.

2.2.9 Mantenimiento de equipos informáticos

El mantenimiento de equipos informáticos se enfoca mayormente en mantener un buen funcionamiento de los computadores y en disminuir los gastos por daños que pueden suceder durante la vida útil del equipo. En las empresas e instituciones es muy reconocida esta acción de protección de los equipos por eso en su mayoría contratan personal especializado en el manejo de las tecnologías computacional para lograr el mejor funcionamiento posible de los computadores, sin embargo, existen organizaciones que no aplican esta alternativa y por ende siempre van a estar susceptibles a fallas de algún tipo dentro de su estructura computacional (Rodriguez, 2018).

2.2.9.1 Tipos de mantenimientos

Existen varios tipos de mantenimiento, en esta ocasión se especifica en los planteados por Palacios et al. (2022): mantenimiento preventivo y mantenimiento correctivo.

2.2.9.1.1 Mantenimiento preventivo

Del mantenimiento preventivo es el que asegura un ambiente adecuado para el funcionamiento del sistema y mantiene la limpieza en todas las partes que componen el equipo informático. Este mantenimiento es sumamente importante considerando que el mayor número de fallas que presentan los equipos están dada por la acumulación de polvo en sus componentes internos. Puede decirse que si se quiere prolongar la vida útil del equipo y hacer que permanezca libre de reparaciones por muchos años se debe de realizar la limpieza con frecuencia.

2.2.9.1.2 Mantenimiento correctivo

Para comprender en que consiste el mantenimiento correctivo se debe partir de que la corrección es la reparación de alguno de los componentes de la computadora: una soldadura pequeña, el cambio total de una tarjeta (sonido, video, SIMMS de memoria, entre otras), o el cambio total de algún dispositivo periférico como el ratón, teclado,

monitor, entre otros tantos que existen. Es preciso destacar que para iniciar este mantenimiento se debe tomar en cuenta lo siguiente: ámbito operativo, reconfiguración de la computadora y los principales programas que utiliza; revisión de los recursos del sistema, memoria, procesador y disco duro; optimización de la velocidad de desempeño de la computadora; revisión de la instalación eléctrica (sólo para especialistas); un completo reporte del mantenimiento realizado a cada equipo y observaciones que puedan mejorar su funcionamiento.

2.2.10 Dispositivos de entrada y salida

Comúnmente a los dispositivos de entrada y salida se les conoce como periféricos; en el caso de los dispositivos de entrada estos garantizan la interacción con la computadora, tienen la función de introducirle datos útiles para obtener el resultado de las operaciones que se ejecuten. Como todo equipo la computadora necesita recibir señales de entrada para generar salidas y este sistema de entrada y salida sucede gracias a los dispositivos. Los periféricos más conocidos se encuentran los siguientes; de entrada: el ratón (mouse), lápiz óptico, módem, teclado, manejador de discos, digitalizador escanner, la webcam, micrófono; y de salida: altavoces, impresora, monitor, el proyector de video entre otros (Brys, 2013).

2.2.11 Ciclo de vida de un sistema informático

El ciclo de vida de un sistema informático tiene siete fases: planificación, análisis, diseño, desarrollo, integración y período de prueba, implementación y mantenimiento. Es preciso destacar que en un sistema informático inicialmente se definen actividades, plazos, roles y responsabilidades, luego se concretan los requisitos que regirán el nuevo sistema o los cambios del antiguo, se elige el software y hardware bajo las especificaciones para las distintas aplicaciones y proceder a la implementación del nuevo sistema previa aprobación de la dirección de la organización beneficiaria (Cáceres, 2021).

Al seguir con la explicación, más adelante se inicia la producción enfocándose en formar y capacitar a los usuarios y el equipo técnico porque son muchos los cambios y de manera sistemática. Al llegar a la fase de integración y período de prueba se corrobora el diseño y se realizan tantas pruebas sean necesarias hasta llegar a la conformidad del usuario. Luego se inicia la implementación y se comienza a trabajar con el nuevo sistema, se realiza el proceso de instalación de software y hardware que se ha elegido para concluir con la etapa de mantenimiento donde se va mejorando el rendimiento del sistema y se corrigen los problemas que puedan surgir.

2.2.12 Seguridad Informática en el uso de los nuevos equipos tecnológicos

En la era digital ha crecido considerablemente el número de dispositivos con la capacidad de conectarse a internet y comunicarse por medio de la red y en este contexto ha ganado reconocimiento la atención a la seguridad en el uso de los equipos tecnológicos. En este sentido la función de la seguridad informática se centra en minimizar los riesgos que en el uso de nuevos equipos tecnológicos provienen de muchas partes. La mayoría de estos riesgos provienen de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, de los mismos usuarios y hasta de los mismos protocolos que se están implementando (Morán et al., 2018).

Partiendo de lo expuesto puede decirse que la principal tarea en la protección de nuevos equipos tecnológicos es minimizar los riesgos para obtener mejor y mayor seguridad. Es preciso destacar que existen tres clasificaciones de seguridad: seguridad de los usuarios, seguridad de la información y seguridad de la infraestructura, estas están estrechamente ligadas, pero en este apartado se destaca la protección de equipos tecnológicos por tanto se refiere a la de infraestructura.

2.2.13 Prácticas de control para equipos informáticos

La protección de equipos informáticos ya sea en hogares u oficinas parte del conocimiento de las buenas prácticas de control para que los usuarios tengan precaución de las acciones que realizan en internet. Lo primero es actualizar el antivirus que viene por defecto o instalar uno nuevo; para los parches de seguridad del sistema se debe tener habilitado la actualización automática, aunque muchas veces cause molestias. Se deben visitar solo las páginas web seguras verificando en los navegadores el candadito de color verde en los URL de la parte superior; si va a realizar alguna transacción en internet debe asegurarse de estar en la página correcta; no responder mensajes electrónicos y enviar información personal (Flores et al., 2019).

En este orden de ideas también se reconoce como una práctica muy significativa en temas de protección la de actualizar las contraseñas y ubicar letras, números, caracteres para que no las descifren fácilmente y nunca informar a otras personas sobre las páginas que más se visitan.

2.2.14 Herramientas para evaluación de vulnerabilidades

Según Uriña y Crespo (2022, pp. 48-67) existen diversas herramientas para la evaluación de vulnerabilidades, a continuación, se mencionan algunas de ellas:

El **Escáner de vulnerabilidad** es una herramienta de software que identifica los problemas y riesgos conocidos en los servicios o aplicaciones que están instaladas en los

dispositivos que se encuentran dentro de la empresa. Estos escáneres tienen en su funcionamiento una comparación de los servicios y sus versiones instaladas con base de datos propias.

Acrylic WI-FI es una herramienta que permite a los usuarios, profesionales y administradores de redes sacra y aprovechar el máximo de su red inalámbrica, analizando el rendimiento de esta, permite identificar quién está conectado, las velocidades de transmisión y optimizar los canales Wi-Fi.

Acrylic Wifi Profesional está diseñada para el sistema operativo Microsoft Windows el cual permite analizar, identificar y resolver los problemas en el funcionamiento de redes 802.11a/b/g/n/ac.

Analizador WIFI es la herramienta que permite obtener información donde se describen las redes Wi-Fi, donde también se incluyen las redes Wi-Fi ocultas. El analizador aprovecha todas las funciones para capturar y analizar el tráfico de la red, ver los equipos de dispositivos, inventarios de dispositivos Wi-Fi dentro del rango de cobertura y la velocidad Wi-Fi.

OpenVAS Open Vulnerability Assessment Scanner, es un software framework que brinda una gran variedad de servicios y herramientas, por medio de la cual se puede tener una buena solución para el análisis y administración de vulnerabilidades; es capaz de analizar muchos protocolos industriales y de Internet, tanto de alto nivel como de bajo nivel. Puede analizar varias plataformas, sistemas y más simultáneamente, implementando pruebas de vulnerabilidad obtenidas de un "feet".

2.2.15 Definiciones conceptuales (contexto teórico)

2.2.15.1 Variable independiente: Auditoría informática

Para cada actividad que se realice en una auditoría se debe ejecutar y cumplir un respectivo informe de activos en este caso de los equipos informáticos sobre la fiabilidad de la información establecida, por la información de comprobación de situaciones concretas que pueda tener efectos frente a terceros, por los conceptos que suelen comprobar por hechos en los procedimientos con alcance más limitados, con el fin de emitir una opinión técnica (Abolacio, 2018).

Las Auditorías más conocidas es las normas ISO, en este caso aplicaremos la metodología Magerit para gestionar los recursos y riesgo que se presentan en los equipos informáticos, con el objetivo de optimizar los procesos que se llevan a cabo en el laboratorio (Baca, 2016).

La auditoría informática aporta un asesoramiento importante dentro de la organización, planificación y justificación de las nuevas estructuras o métodos (Derrien, 2009).

La metodología fue creada por el Comité Técnico de Seguridad de los SI, se encarga de un análisis y gestión de riesgos de los sistemas de información, busca gestionar los riesgos y las necesidades, con la finalidad de ofrecer un método sistemático para evaluar y determinar los riesgos, con el objetivo de disminuir y planificar un control de riesgo bajo control (Solano y Riascos, 2021).

En esta investigación se aplicará la metodología Magerit para analizar los componentes físicos y lógicos que se puedan realizar la Auditoría informática en la institución "Alessandro Volta" para llevar a cabo un buen trabajo y recomendar medidas de prevención en las actividades planificadas.

2.2.15.2 Variable dependiente: equipos informáticos

Un ordenador se caracteriza por su hardware y software, mediante el hardware podemos concretar la parte física de la computadora, por otra parte, el software aplica a los programas del sistema, los dispositivos de entrada permiten el ingreso de información al sistema informático, el cual es el teclado, mouse, micrófono, cámara o escáner, entre otros. Por lo tanto, los dispositivos de salida acceden a la extracción o recuperación de información.

Los dispositivos informáticos más reconocido e importante son, monitor, router, modem, unidad central, disco duro, impresora, teclado, ratón, entre otros. Por lo tanto, es recomendable hacer mantenimiento a los equipos informático, en este caso se aplicará una Auditoría informática a los equipos dentro de la institución, tomando en cuenta el ciclo de vida de un sistema informático (Morán, 2019).

2.2.16 Metodología propuesta

En la presente investigación se pretende utilizar la metodología Magerit por los beneficios que se logran en la planificación de manera adecuada los sistemas informáticos en la cual se gestiona y evalúa con la finalidad que la organización tenga seguridad, privacidad, eficacia, confiabilidad mediante un análisis externa e interna de los riesgos que se encuentran en la institución en donde se incluyen las siguientes fases:

- Planteamiento del problema
- Análisis de riesgos
- Gestión de riesgos

2.2.17 Conclusiones relacionadas al marco teórico en referencia al tema planteado.

En la revisión de la literatura se pudo evidenciar que, la implementación de una auditoría informática es sumamente beneficiosa para las organizaciones, por lo que se recomienda implementarlas en todas sus dimensiones posibles.

La auditoría informática juega un papel muy importante en todas las organizaciones e instituciones donde se busca mejorar la calidad y funcionamiento de la institución y de su personal, en especial para las unidades educativas en beneficio de los estudiantes y sus docentes.

Se constató que, la auditoría informática es uno de los aspectos más importantes en la investigación de los dispositivos informáticos de una institución, ofreciendo herramientas para la seguridad en los sistemas y estableciendo políticas, de modo que determine qué es lo que se está haciendo mal y corregirlo; brindando a la unidad educativa un mejor servicio en los procesos pedagógicos pertinentes.

CAPÍTULO III: MARCO INVESTIGATIVO

3.1 Introducción

El capítulo que se presenta a continuación muestra los principales aspectos del diseño metodológico de la presente investigación. En los contenidos que se abordaron se resaltan los tipos de investigación utilizado como descriptivo, bibliográficos y de campo. En la misma idea se desarrollaron los métodos de investigación y las fuentes de información de datos sean primarias y/o secundarias, también se destacan las estrategias operacionales para la recolección de datos a partir de identificar la población, segmentación, técnica de muestreo y tamaño de la muestra.

Se identificaron el análisis de las herramientas de recolección de datos a utilizar, la estructura de los instrumentos de recolección de datos aplicados. Además, se refiere al análisis y presentación de resultados obtenidos de la tabulación de las entrevistas y encuestas, así como la presentación y descripción de los resultados obtenidos. Por último, se reflejan las conclusiones para el marco investigativo.

3.2 Tipo de investigación

La investigación pertenece al enfoque mixto (cuali-cuantitativo), es del diseño no experimental, de carácter longitudinal y del tipo descriptiva, bibliográfica y de campo coincidiendo con lo planteado por Hernández y Mendoza (2018).

3.2.1 Investigación Descriptiva.

Consiste en caracterizar un fenómeno o situación concreta indicando sus rasgos más peculiares o diferenciadores. El objetivo de la investigación descriptiva se fundamenta en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables.

La investigación descriptiva se emplea para determinar las características de la Unidad Educativa “Alessandro Volta”, las cuales sirven para analizar y llegar a corroborar cuál fue la problemática existente dentro de la institución. Se utiliza para la recopilación de información de los instrumentos aplicados y esto favorece el análisis e interpretación de los resultados obtenidos en el desarrollo de la auditoría informática física y lógica en la unidad educativa.

3.2.2 Investigación Bibliográfica.

La investigación bibliográfica constituye una excelente introducción a todos los otros tipos de investigación, además de que es una necesaria primera etapa de todas ellas, puesto que ésta proporciona el conocimiento de las investigaciones ya existentes (teorías, resultados, instrumentos y técnicas usadas) acerco del tema o problema que el investigador se propuso investigar o resolver.

Se define cuestiones generales como el tema, el problema, proporcionando el conocimiento de las investigaciones ya existentes, dicha investigación fue desarrollada en el marco teórico respaldando la teoría de la auditoría informática física y lógica como parte de una de las disciplinas de la Informática dentro de la carrera Tecnologías de la Información en la unidad educativa.

3.2.3 Investigación de Campo.

Se trata de la investigación aplicada para comprender y resolver alguna situación, necesidad o problema en un contexto determinado. El investigador trabajo en el ambiente natural en que conviven las personas y las fuentes consultadas, de las que se obtuvo los datos más relevantes a ser analizados como son: individuos, grupos y representaciones de las organizaciones científicas no experimentales dirigidas a descubrir relaciones e interacciones entre variables sociológicas, psicológicas y educativas en estructuras sociales reales y cotidianas.

Este tipo de investigación es un proceso sistemático y racional de recolección, análisis y presentación de datos lo que permite recabar toda la información necesaria para el correcto planteamiento y desarrollo de la propuesta, avalando el Capítulo II.

3.3. Métodos de investigación

3.3.1 Analítico – Sintético

En esta investigación se utilizó el método analítico-sintético para operar el análisis y la síntesis: el análisis es un procedimiento lógico que posibilita descomponer mentalmente un todo en sus partes y cualidades, en múltiples relaciones, propiedades y componentes. La síntesis es la operación inversa, que establece mentalmente la unión o combinación de las partes previamente analizadas y posibilita descubrir relaciones y características generadas entre los elementos de la realidad (Rodríguez y Pérez, 2017).

Fue aplicado el método sintético para evidenciar resultados que se obtuvieron al utilizar esta herramienta para examinar el comportamiento de los estudiantes de la institución y de los docentes encargados de los laboratorios.

3.3.2 Inductivo -deductivo

Por otra parte, Rodríguez y Pérez (2017), el método inductivo deductivo está conformado por dos procedimientos inversos: inducción y deducción. La inducción es una forma de razonamiento en la que se pasa del conocimiento de casos particulares a un conocimiento más general, que refleja lo que hay en común en los fenómenos individuales. Mediante la deducción se pasa de un conocimiento general u otro de nivel de generalidad. La generalidad son puntos de partida para realizar inferencias mentales y arribar a nuevas conclusiones lógicas para casos particulares (p. 9).

Se aplicó para abordar el fenómeno estudiando de lo general a lo particular; en el marco teórico por ejemplo con ese método se realizó una sistematización de os fundamentos teóricos más relevantes sobre las variables estudiadas llegando a particularizar en la conceptualización.

En el estudio de campo se empleó este método para indagar las particularidades de la seguridad física y lógica en la Unidad Educativa y en la auditoría se hizo un análisis de riesgo donde se evaluaron parámetros específicos de seguridad lo que permitió proyectar una guía con las generalidades que deben sr tomadas en cuenta para solucionar la problemática de la seguridad informática en la Unidad Educativa.

3.4 Fuentes de información de datos

3.4.1 Fuente primaria: Entrevista

Según Hérnandez y Coello (2008), la entrevista es una técnica que puede ser aplicada a todo tipo de persona que tenga algún tipo de limitación como es el caso de analfabetos, limitados físicos y orgánicos o personas que tengan algún tipo de dificultad que le impida dar respuestas escritas (p. 94).

De acuerdo con Abarca et al. (2013), “es posible entender la técnica de la entrevista como: el procedimiento de recolección de información basado en una interacción entre dos personas o más, a través de la conversación como herramienta principal” (p. 100).

Por otra parte, la encuesta es semejante a la entrevista, pero escrita, donde a través de un conjunto de preguntas se puede pretender obtener una información sobre el mundo interior del encuestado o su percepción del fenómeno que se investiga, por lo que no puede ser obtenida por la información

3.4.2 Fuente secundaria: Encuesta

La encuesta se basa a la técnica cuantitativa que tiene una secuencia de preguntas sobre una determinada investigación o problema, con la finalidad de definir asuntos y

lograr conseguir la información oportuna y relevante con el objetivo que aporte los datos e información que se apetece llegar, herramienta que permite medir los datos estadísticos para logar resultados anhelados (Negrín et al., 2017).

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

Se define la población como un conjunto de personas, animales o cosas de la misma especie en donde se desea conocer algún acontecimiento o hecho que se encuentre en un momento y lugar determinado durante una investigación que se esté realizando a las personas que habitan en cierta área geográfica (Atilio, 2020).

La unidad educativa "Alessandro Volta" en el área de informática cuenta con dos laboratorios donde el responsable es el Msc. Patricio Vaca el cual imparte la materia de informática a los siguientes cursos de bachillerato 1ro, 2do y 3ro, donde solo 2do tiene dos grupos de estudiantes. El laboratorio funciona en la mañana y la tarde con la disposición de 40 máquinas.

Tomando en cuenta lo descrito se tomó como población a los 125 estudiantes de bachillerato y al docente que imparte la materia informática, teniendo un total de 126 personas.

3.5.2 Segmentación

Un sistema segmentado implicaba la presencia de un campo diferenciado por segmentos integrados a una totalidad, con posiciones relativas a actores e instituciones que los tornaban reconocibles (Brito y Stagno, 2010). Para el presente estudio la unidad educativa "Alessandro Volta" constituyó el proceso segmentado a partir de la muestra utilizada en los laboratorios de informática.

3.5.3 Técnica de muestreo

Se utilizó para este tipo de estudio el muestreo aleatorio simple, este se caracteriza porque cada elemento de la población tiene la misma probabilidad de ser escogido para formar parte de la muestra (Otzen y Manterola, 2017). Una vez censado el marco de la población, se asigna un número a cada individuo o elemento y se elige aleatoriamente. Este tipo de muestreo se caracteriza por su simplicidad y fácil comprensión, aunque también posee algunas limitaciones, porque no siempre es posible disponer de un listado de todos los individuos que componen la población, generalmente cuando son poblaciones grandes.

3.5.4 Tamaño de la Muestra

La muestra en cualquier tipo de investigación lo que primero se debe definir la unidad de análisis (personas, organizacionales, periódicos). Una vez que se ha definido la unidad de análisis se procede a delimitar la población que será estudiada y sobre la cual se pretende obtener los resultados esperados. No obstante, la muestra suele ser definida como un subgrupo de la población (Aguilar, 2017).

Para el cálculo de la muestra se empleó la muestra discrecional por ser este método discrecional (o muestreo por juicio) un método de muestreo no probabilístico. Los sujetos se seleccionan a base del conocimiento y juicio del investigador. Para este caso particular la investigadora selecciona a los individuos a través de su criterio profesional. Se basó para ello en su conocimiento sobre la población y el comportamiento de esta frente a las características que se estudian, criterios que coinciden con Hernández y Mendoza (2018).

Para calcular la muestra se tomó a las 127 personas que componen la población y como resultado se obtuvo una muestra de 62 personas que quedaron distribuidas de la siguiente manera: 1 es el Rector de la Unidad Educativa, 1 el docente de la materia de informática que a su vez es responsable del laboratorio, 20 estudiantes de 1ero de bachillerato, 20 de segundo de bachillerato (10 de cada grupo) y 20 de tercer año de bachillerato.

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.5.2.1 Encuesta – Entrevista

Las técnicas que se utilizaron durante la investigación para el desarrollo del proyecto de tesis son la entrevista y la encuesta.

Para la fase de recopilación de información se utilizaron las técnicas de la encuesta tipo cuestionario (encuestas semiestructuradas con preguntas abiertas y cerradas) y entrevista (semiestructuradas), el instrumento que se va a utilizar es el cuestionario. Se aplicaron las encuestas a los estudiantes y la entrevista al responsable de laboratorios, además del rector como fuente fidedigna de la información recogida, en los dos instrumentos se utilizó un guion de preguntas.

3.5.2.2 Entrevista

La entrevista se aplicó al encargado del laboratorio y al Rector de la Unidad Educativa con la finalidad de diagnosticar el estado actual del equipamiento informático de la institución. Las entrevistas fueron aplicadas en los cubículos docentes de manera personalizada con el objetivo de realizar un diagnóstico acerca de la situación actual de

los laboratorios de la Unidad Educativa “Alessandro Volta” cómo de los programas que se usan.

La entrevista semiestructurada se aplicó con un grado mayor de flexibilidad que las estructuradas, debido a que parten de preguntas planeadas, que pueden ajustarse a los entrevistados. En este sentido, se aplicó una entrevista que permita a los opinantes avalar sus respuestas por medio de diversas opciones y pueda argumentar desde su percepción los principales contenidos abordados.

Dirigida a: Directivo y Encargado de laboratorios

Objetivo: Realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad Educativa “Alessandro Volta” cómo de los programas que se usan.

1. ¿Qué orientaciones y / o capacitaciones ha recibido usted como directivo para proyectar con sus trabajadores acciones de seguridad informática en los laboratorios de computación?
2. ¿Existe en la Unidad Educativa alguna estrategia para garantizar la seguridad en el laboratorio de computación? Mencione la estrategia y cuantos actores de la comunidad educativa se ven implicados en su implementación.
3. ¿El responsable del laboratorio de computación es un técnico informático que tiene solo esa función o son los profesores que imparten esta materia?
4. ¿Considera usted que existe en la Unidad Educativa suficiente divulgación sobre las acciones de seguridad informática que se deben desarrollar para el mantenimiento del laboratorio de computación? Mencione estas acciones.
5. ¿Qué capacitaciones se han desarrollado en la Unidad Educativa para que los usuarios (estudiantes, docentes y directivos) garanticen la seguridad en el laboratorio de computación?
6. ¿Con que frecuencia se actualiza en la Unidad Educativa el inventario de equipos informáticos?
7. ¿En la Unidad Educativa se realiza el mantenimiento de los equipos informáticos solo cuando hay roturas o están debidamente planificados en diferentes períodos del año lectivo?
8. ¿Usted cómo directivo siente que su información digital está segura? ¿Tiene respaldo de esta? ¿Conoce los mecanismos para recuperarla?
9. ¿Qué evaluación usted le otorga al sistema de actualización de antivirus que se emplea en el laboratorio?

10. ¿Cree usted importante que se realice en la Unidad Educativa una auditoría informática al laboratorio de cómputo para brindarle a usted un informe de evaluación de riesgos que le permita tomar decisiones en función de proteger los medios informáticos?

3.5.2.3 Encuesta

En esta investigación se aplicó una encuesta a los estudiantes de bachillerato para diagnosticar el estado actual de los laboratorios en la unidad educativa (Anexo 2). Se empleó de manera anónima y personal, en salones de clase.

Luego del estudio realizado con los datos coleccionados a través de la encuesta de preguntas cerradas y la encuesta semiestructurada, estos fueron analizados en la herramienta de Office con el Excel para la elaboración de las figuras y tablas. En el Anexo 3 se muestran las imágenes de evidencias de la aplicación de los instrumentos de entrevista y encuesta a la muestra seleccionadas.

Dirigida a: Estudiantes

Objetivo: Realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad educativa Alessandro Volta cómo de los programas que se usan.

Cuestionario de preguntas de la encuesta

1. Seleccione su categoría.

   ____Profesor

   ____ Estudiante

2. En el laboratorio de computación existen horarios definidos para la atención a usuarios.

   ___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

3. ¿Se realizan con frecuencia mantenimientos a los equipos informáticos del laboratorio de computación?

   ___ Nunca ___ Casi nunca ___ A veces ___ Casi siempre ___ Siempre ___

4. Con frecuencia el responsable del laboratorio comprueba que los equipos procesen la información de forma adecuada.

   ___ Nunca ___ Casi nunca ___ A veces ___ Casi siempre ___ Siempre ___

5. ¿En el laboratorio es obligatorio identificarse con usuario y clave para acceder al sistema?

   ___ Nunca ___ Casi siempre___ A veces ___ Casi siempre ___ Siempre ___

6. ¿Al crear su usuario y contraseña el sistema le informa la longitud mínima y los caracteres que debe contener una contraseña?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

7. ¿Está definido el período de caducidad de la contraseña?

____ Si ___ No

8. ¿Cuándo usted accede al laboratorio el responsable le hace firmar en una lista de control de acceso?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

9. ¿Existen en el laboratorio etiquetas de seguridad que le orientan como debe ser su comportamiento en el laboratorio y el cuidado que debe dar a los equipos informáticos?

___Si ___ No

10. ¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el laboratorio de computación?

___ Si ___ No

11. ¿Se ha definido e informado a usted cuales son las sanciones de los usuarios por infringir las normas?

___ Si ___ No

12. ¿Los equipos de laboratorio están conectados en red?

___ Si ___ No

13. ¿Existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

14. ¿Se ha definido la forma de acceso a recursos compartidos?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

15. ¿En el laboratorio se han instalado antivirus en los servidores?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

16. ¿Se han habilitado las actualizaciones del antivirus?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

17. ¿A usted como usuario se le ha informado el proceso adecuado para realizar el respaldo y recuperación de información?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

18. ¿En el laboratorio se han bloqueado puertos USB y la grabadora de CD/DVD para la protección de los medios informáticos?

___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

3.5.2.2 Estructura de los instrumentos de recolección de datos aplicados

Tal como señalan Hernández y Mendoza (2018) "no se inicia la recolección de los datos con instrumentos preestablecidos, sino que el investigador comienza a aprender por observación y descripciones de los participantes y concibe formas para registrar los datos que se van refinando conforme avanza la investigación" (p. 17).

Se empleó la entrevista la que estuvo estructurada por 10 preguntas con el objetivo de realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad Educativa "Alessandro Volta" cómo de los programas que se usan, la entrevista estuvo dirigida al encargado de laboratorios como parte de la muestra y también fue aplicada al Rector de la Unidad Educativa para reforzar la veracidad de los medios informáticos y contrastar los criterios.

Por su parte la encuesta fue aplicada a los estudiantes de los diferentes años de bachiller, tuvo el mismo objetivo que la entrevista y un total de 18 preguntas de forma estructurada que tenía como opciones una, dos o cinco opciones de respuestas.

3.5.3 Plan de recolección de datos

El presente estudio tuvo como plan de recolección de datos los aspectos siguientes: se realizó con el objetivo realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad Educativa "Alessandro Volta" cómo de los programas que se usan, lo que permitió de forma oportuna el desarrollo una Auditoría informática lógica y física mediante el uso de la metodología Magerit en la Unidad Educativa.

Este fue aplicado por la investigadora y su grupo de investigación durante el periodo 2022. Los instrumentos de recolección de datos que fueron utilizados fue la entrevista y la encuesta los que fueron aplicados una sola vez como parte del estudio trasversal que se desarrolló como parte de la metodología fundamentada. Las preguntas a los estudiantes se realizaron de forma anónima, se contó con los espacios de laboratorios de informática, en una charla amena donde se produjo un intercambio de saberes a partir del objetivo de los instrumentos aplicados.

Se escogió como día para la aplicación de los instrumentos un martes en la mañana para lograr la empatía de los horarios docentes y que el flujo de conocimientos fueran los ideales porque se considera que no están los afectos personales del fin de semana y están más centrados en sus objetivos escolares, logrando así mayor compromiso y claridad en las respuestas.

3.6 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos

3.6.1.1. Entrevista aplicada al Rector y encargado de laboratorios

La entrevista fue dirigida al Rector y al encargado de laboratorios de computación con el objetivo de realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad Educativa Alessandro Volta cómo de los programas que se usan. Se puede observar en la tabla 2 como parte de la tabulación y análisis de los datos que está dividido por el número, la pregunta, respuesta del entrevistado y la interpretación de las misma por parte de la investigadora y el equipo de investigación.

Tabla 2. Resultados de entrevista al Rector y encargado de laboratorios de computación

No.	Pregunta	Respuesta		Interpretación
		Rector	Encargado	
1.	¿Qué orientaciones y / o capacitaciones ha recibido usted como directivo para proyectar con sus trabajadores acciones de seguridad informática en los laboratorios de computación?	En realidad, no se ha recibido ninguna capacitación, sin embargo, los docentes a cargo conocen del tema	Se han recibido cursos dictados por la universidad politécnica de Chimborazo	Queda evidenciado que, existe una contradicción porque el Rector opina que no se realizan capacitaciones y el encargado afirma en sentido contrario, además se destaca que los docentes a cargo conocen del tema

				sobre seguridad informática en los laboratorios de computación
2.	¿Existe en la Unidad Educativa alguna estrategia para garantizar la seguridad en el laboratorio de computación? Mencione la estrategia y cuantos actores de la comunidad educativa se ven implicados en su implementación.	No existe ninguna estrategia	Estrategias existen, pero no se encuentran documentadas. Entre ellas, el manejo del firewall de mikrotik para la restricción de páginas no autorizadas	Se muestra que no existe ninguna estrategia documentada para garantizar la seguridad en el laboratorio de computación. Sin embargo, el encargado plantea que tienen estrategia verbal, pero si es evidente que cuentan con el manejo de las mismas por las restricciones oportunas de páginas no autorizadas
3.	¿El responsable del laboratorio de computación es un técnico informático que tiene solo esa función o son los profesores que	Los responsables son docentes encargados del laboratorio	Solo somos profesores que impartimos las materias, no existe un responsable técnico como tal	Se puede constatar que, se cumple con uno de los requisitos donde el responsable del laboratorio de computación es un profesor que

	imparten esta materia?			imparten esta materia.
4.	¿Considera usted que existe en la Unidad Educativa suficiente divulgación sobre las acciones de seguridad informática que se deben desarrollar para el mantenimiento del laboratorio de computación? Mencione estas acciones.	Cuando se trabajó virtual se brindó el servicio, en la presencialidad ninguna acción	No existen divulgaciones o temas para culturizar a ningún miembro de la comunidad educativa	Se puede plasmar que, no se realizan de forma oportuna la divulgación sobre las acciones de seguridad informática, sin embargo, cuando se trabajó de forma virtual se brindó el servicio.
5.	¿Qué capacitaciones se han desarrollado en la Unidad Educativa para que los usuarios (estudiantes, docentes y directivos) garanticen la seguridad en el	Capacitaciones ningunas	Capacitaciones ningunas, se puede mencionar que constantemente se tiene alertado a los estudiantes de los distintos ataques o métodos que los cibercriminales suelen utilizar	Es evidente que no realizan acciones de capacitación para que los usuarios garanticen la seguridad en el laboratorio, sin embargo, se resalta que, los docentes de estas materias mantienen

	laboratorio de computación?			actualizados a los usuarios que utilizan estos laboratorios sobre los distintos ataques o métodos que los cybercriminales suelen utilizar
6.	¿Con qué frecuencia se actualiza en la Unidad Educativa el inventario de equipos informáticos?	Cada inicio y fin de año lectivo	El inventario se lo actualiza cada año	Se constató que, actualizan el inventario de equipos informáticos dos veces al año.
7.	¿En la Unidad Educativa se realiza el mantenimiento de los equipos informáticos solo cuando hay roturas o están debidamente planificados en diferentes períodos del año lectivo?	Están planificados en diferentes periodos	El mantenimiento se lo realiza anualmente con estudiantes de pasantías	Se puede observar que, los mantenimientos de los equipos informáticos se realizan de acuerdo a los términos planificados en diferentes períodos del año lectivo, como se refleja por parte de los estudiantes de pasantías.
8.	¿Usted cómo directivo siente	No existe seguridad de	No soy directivo	Se puede observar que, la

	que su información digital está segura? ¿Tiene respaldo de esta? ¿Conoce los mecanismos para recuperarla?	100%, por no haber sistema perfecto, la mayor parte de información está respaldado		información digital no está segura al 100% pero cuenta la mayor parte de información con respaldado informático.
9.	¿Qué evaluación usted le otorga al sistema de actualización de antivirus que se emplea en el laboratorio?	Creo que es buena	Creo que es buena porque existe la actualización semanal y además existen varias para cada tipo de antivirus	Se constató que, el sistema de actualización de antivirus que se emplea en el laboratorio esta actualizado
10.	¿Cree usted importante que se realice en la Unidad Educativa una auditoría informática al laboratorio de cómputo para brindarle a usted un informe de evaluación de riesgos que le permita tomar decisiones en función de proteger los	Sería muy importante, porque en los últimos cinco años no se han realizado una auditoría informática	Sí, es importante que este tipo de actividades se las realice periódicamente	Es evidente que, necesitan del desarrollo de una auditoría informática al laboratorio de cómputo porque no la realizan hace más de cinco años.

	medios informáticos?			

Fuente: Elaboración propia

3.6.1.2. Encuestas aplicadas a los estudiantes de bachillerato de la Unidad Educativa

Las encuestas fueron aplicadas a los estudiantes de bachiller con el objetivo de realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad educativa Alessandro Volta cómo de los programas que se usan.

Los resultados fueron divididos en bloques para conocer la percepción de cada grupo, respecto a sus expectativas, intereses y los ítems que aparecen reflejados en cada una de las cuatro figuras. Este instrumento fue aplicado a 60 estudiantes del 1^{ero}, 2do y 3ro de bachillerato de la unidad educativa. Con lo cual se obtienen cuatro figuras. Para una mejor comprensión de los resultados se ubicaron cuatro figuras para las 17 respuestas y los ítems, con lo cual se observan los criterios que a continuación se presentan.

En la figura 2, se hace referencia a los criterios sobre si en el laboratorio de computación existen horarios definidos para la atención a usuarios, donde se observa en la mayoría de los criterios de los estudiantes de 1ero y 2do año de forma positiva en la respuesta de siempre, sin embargo, los estudiantes de 3er año se inclinan por la respuesta de a veces. Otro elemento a tener en cuenta es que cerca de la mitad de los estudiantes de 2do y 3ro consideran que casi siempre existen horarios definidos para la atención a usuarios, no obstante, la minoría de 1er año plantea que a veces.

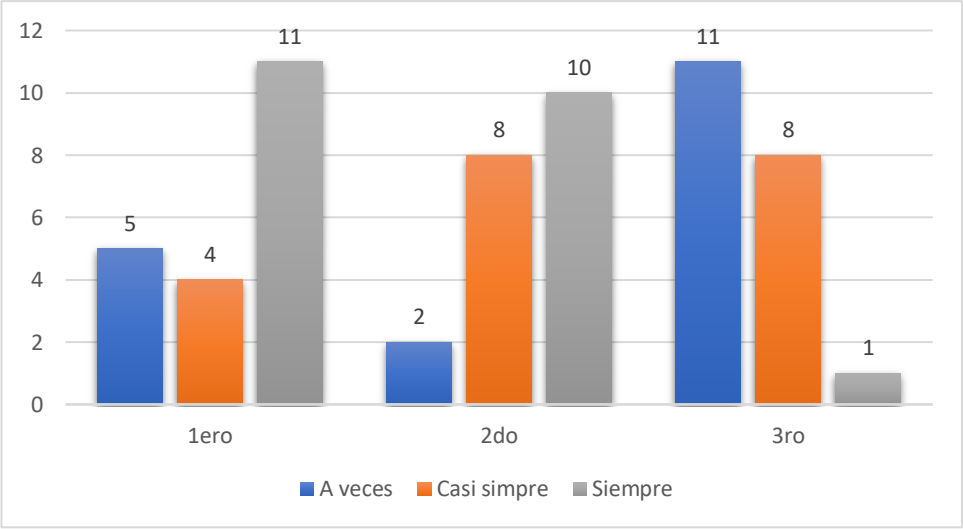


Figura 2. En el laboratorio de computación existen horarios definidos para la atención a usuarios.

Fuente: Elaboración propia

Cuando se observa la figura 3 se realiza un análisis sobre si realizan con frecuencia mantenimientos a los equipos informáticos se evidencian en los resultados, donde los

estudiantes de 1ro y 2do en su mayoría consideran que siempre, por otro lado, los de 3er año no tienen igual criterio donde siete plantean que a veces, y cinco consideran que casi nunca y de igual cifra se proyectan de forma positiva al responder que siempre.

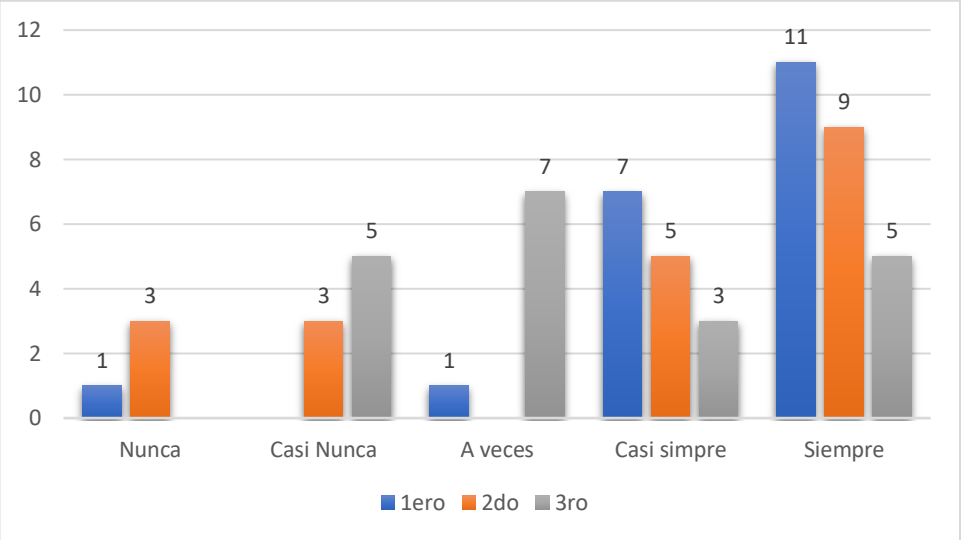


Figura 3. Realizan con frecuencia mantenimientos a los equipos informáticos.

Fuente: Elaboración propia

Se puede constatar que en figura 4 se muestran los resultados si se comprueban que los equipos procesen la información, donde la mayoría de los estudiantes en los tres cursos plantean que siempre, otro pequeño grupo considera que casi siempre. Por lo que se interpreta que ocurre de forma sistemática que los equipos procesen la información.

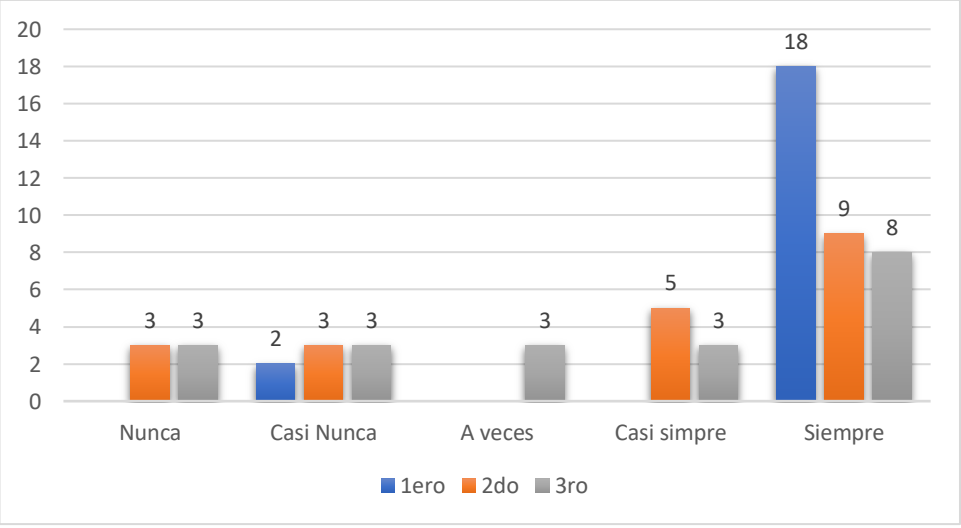


Figura 4. Comprueban que los equipos procesen la información.

Fuente: Elaboración propia

Al evaluar los resultados de la figura 5, en el caso del criterio sobre si, es obligatorio identificarse con usuario y clave, la mayoría, 14 estudiantes del 1^{ero}, refiere que Nunca, con lo que se podría inferir que la seguridad no es adecuada, sin embargo, en

el caso de 2do y 3ro, hacen referencia que casi siempre y a veces, en ese orden, convirtiéndose el registro de los estudiantes en un proceso formal y espontáneo, a medida que avanza en su año académico.

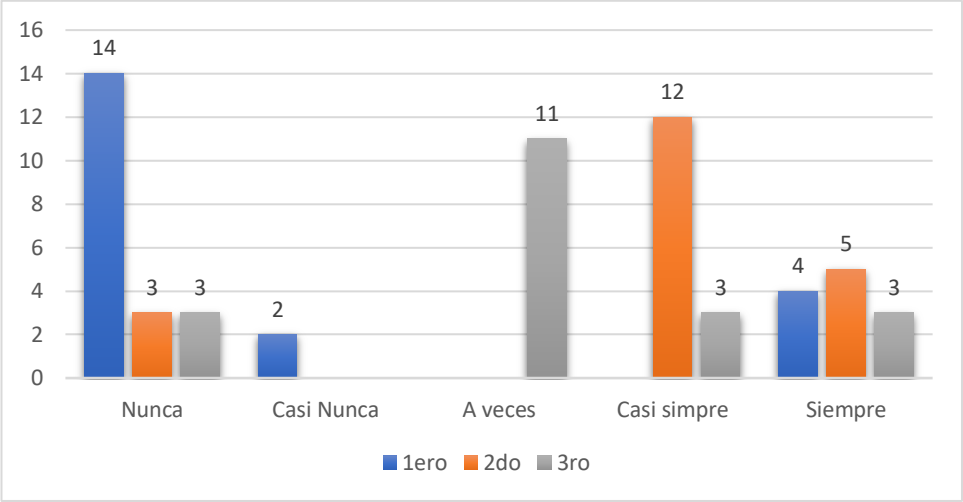


Figura 5. Es obligatorio identificarse con usuario y clave.

Fuente: Elaboración propia

Lo que representa un tema a considerar, tomando en consideración que la identificación con usuario y clave es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema, lo que debe generar exclusividad en el sistema.

En la figura 6 referida a; la longitud mínima y los caracteres que debe contener una contraseña, según se constata, la mayoría de los estudiantes de 1er año se inclina como respuesta por el Nunca, y los demás años académicos de 2do y 3ro afirman en su mayoría que casi siempre.

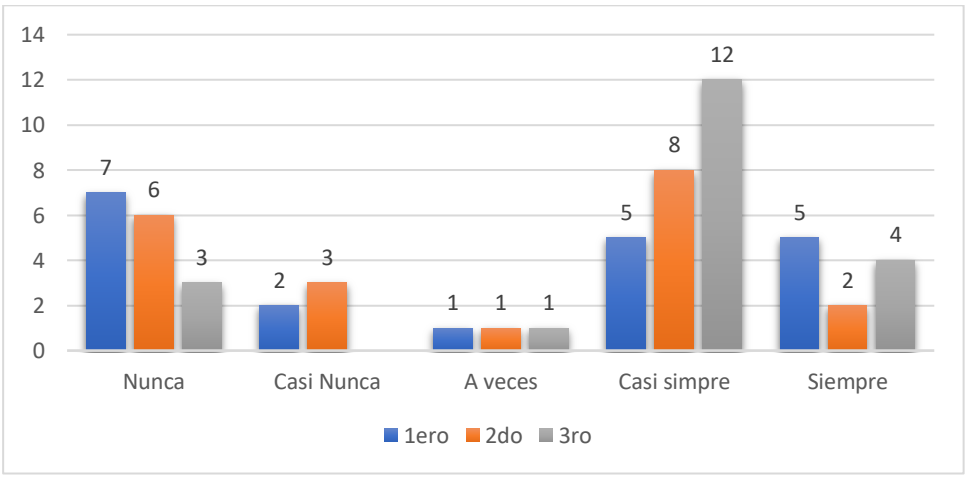


Figura 6. Se informa la longitud mínima y los caracteres que debe contener una contraseña.

Fuente: Elaboración propia

Vale destacar que, en el criterio, longitud mínima y los caracteres que debe contener una contraseña, para el tercer año académico no representa del todo un problema, la mayoría (12) refiere que, Casi siempre, lo que puede estar dado por niveles de conocimiento y capacitación respecto a este aspecto en el último año, lo que no poseen los años precedentes.

Se muestra en la figura 7 que, la pregunta cuándo acceden al laboratorio el responsable le hace firmar en una lista de control de acceso la gran mayoría responde que nunca, lo que evidencia una falencia en la seguridad informática de la información porque al no tener control de los usuarios que utilizan las computadoras los riesgos a la seguridad son mayores.

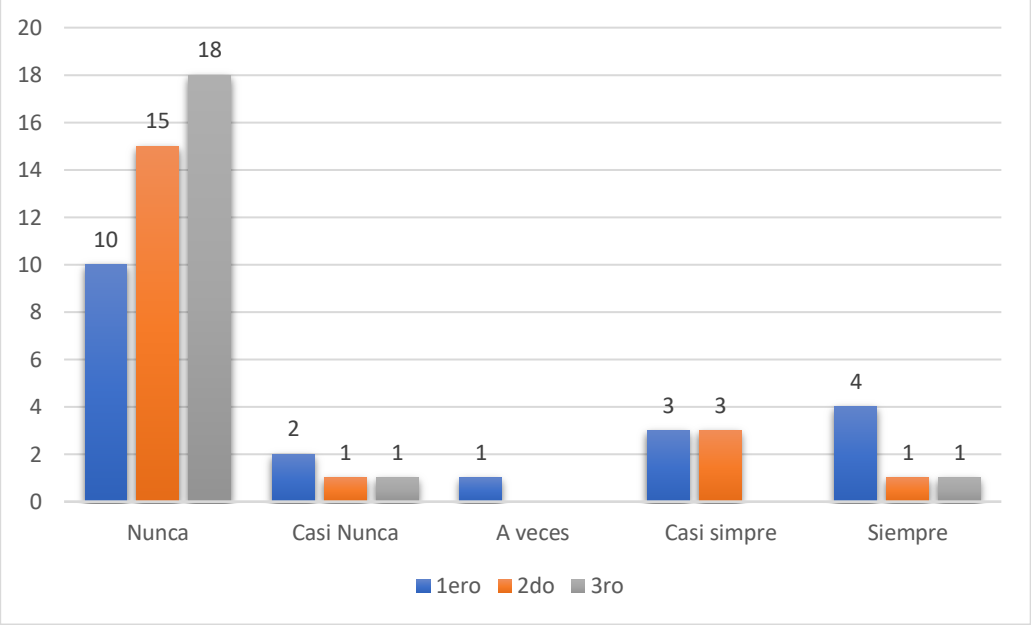


Figura 7. Le hace firmar en una lista de control de acceso.

Fuente: Elaboración propia

Al indagar sobre si existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica la figura 8 muestra la mayoría de los estudiantes de 1er y 2do curso tienen la opinión que nunca, más sin embargo los de 3er año tienen criterios divididos donde cinco de ellos plantean que nunca y otros cinco casi nunca, por lo que se interpreta que no existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica

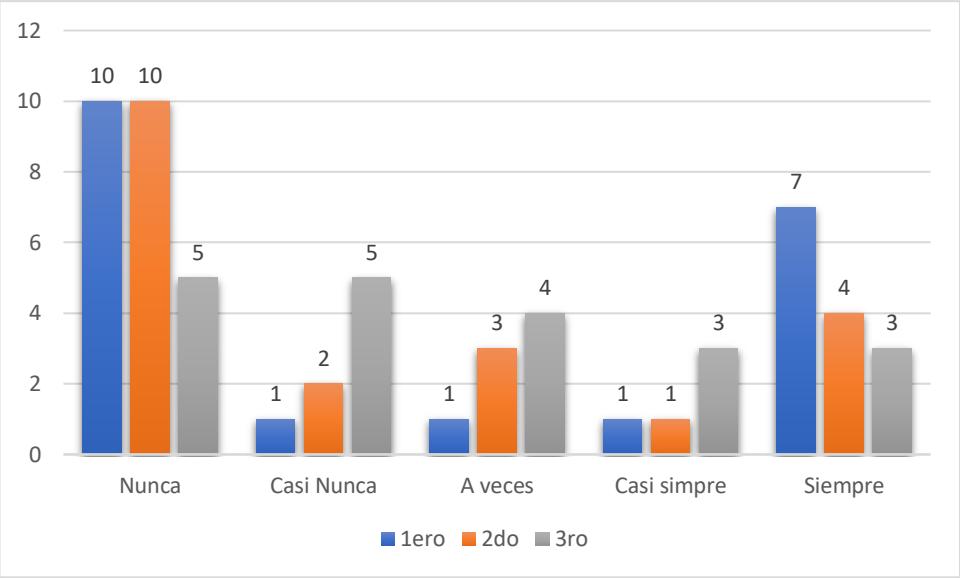


Figura 8. Evitar el acceso a páginas que no tienen finalidad académica.

Fuente: Elaboración propia

La figura 9 muestra los resultados de si se ha definido la forma de acceso a recursos compartidos, se observa que, los criterios son divididos en todos los ítems, al no existir consenso en cuanto a su utilización, aunque se reconoce que están las respuestas en a veces y siempre.

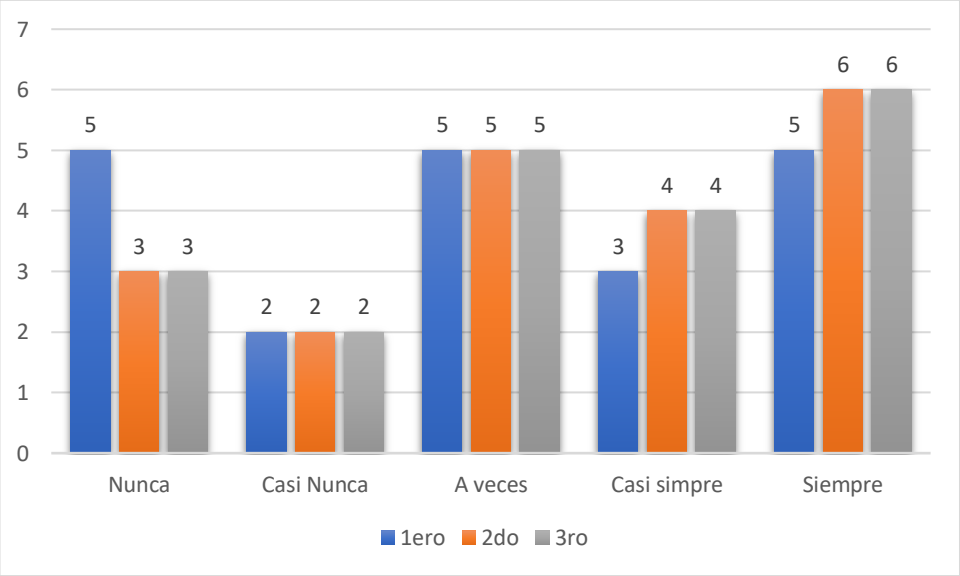


Figura 9. Forma de acceso a recursos compartidos.

Fuente: Elaboración propia

Al evaluar si en el laboratorio se han instalado antivirus en los servidores, los resultados se muestran en la figura 10 donde los estudiantes de 1er año muestran criterios divididos en su mayoría en respuestas de nunca y siempre, en el mismo orden de idea los estudiantes de 2do año la mayoría con 15 plantean que nunca y los de 3er año las mayores agrupaciones de criterios están en casi siempre y siempre.

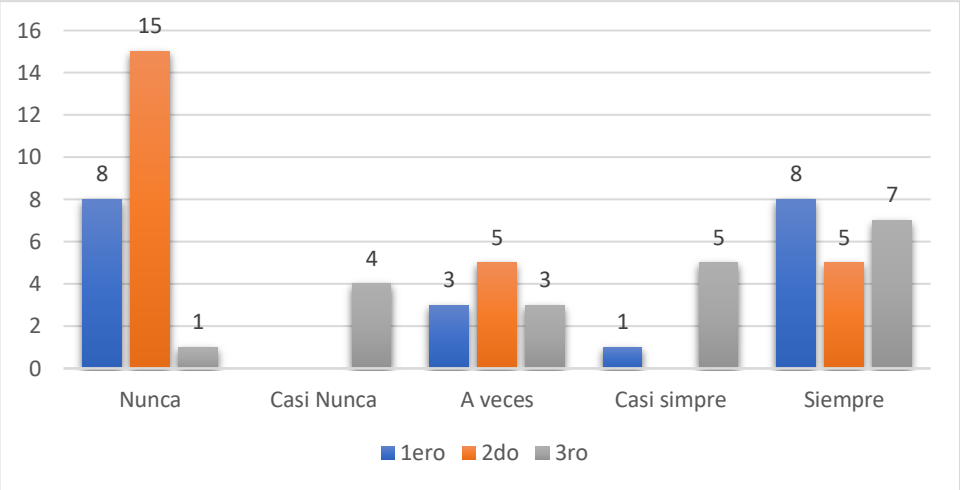


Figura 10. Instalado antivirus en los servidores.

Fuente: Elaboración propia

En la figura anterior está asociada a la Protección de la información, donde en el criterio si existe instalado antivirus en los servidores, el 2do año en su mayoría hace referencia que Nunca, 15 estudiantes, otros ocho educandos de 1er año refieren el mismo criterio. En este grupo de criterios, otro elemento importante a tener en cuenta, es que la mayoría no perciba que están habilitadas las actualizaciones de antivirus, constituyendo un riesgo informático importante en la seguridad de los equipos y de la propia información.

Cuando se evalúa las respuestas de si se han habilitado las actualizaciones del antivirus se puede observar en la figura 11 que, los estudiantes de 1er año mantienen grupos divididos en 10 plantean que siempre y ocho que nunca, los de 2do año consideran en su mayoría que nunca y a veces, y no existe un consenso claro en los de 3er año donde están sus criterios en nunca, a veces y siempre.

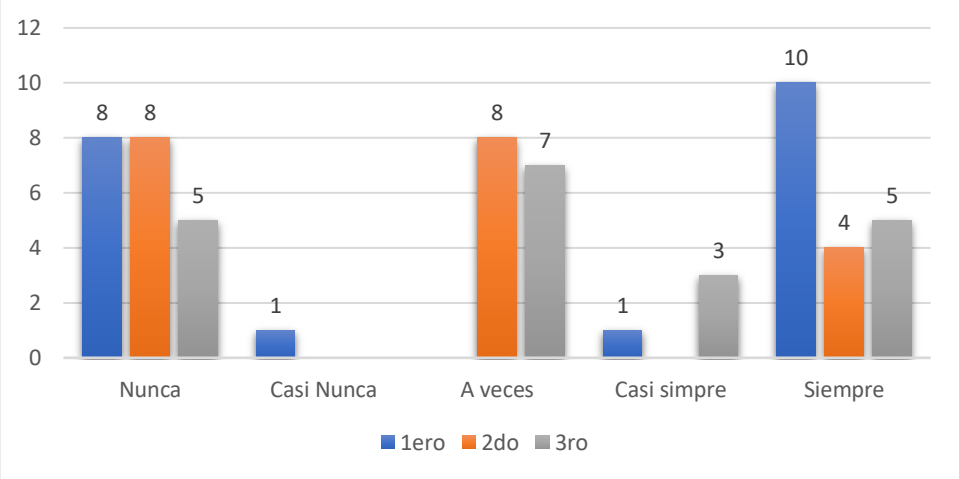


Figura 11. Habilitado las actualizaciones del antivirus.

Fuente: Elaboración propia

Se indaga sobre si a usted como usuario se le ha informado el proceso adecuado para realizar el respaldo y recuperación de información, se muestra en la figura 12 los resultados donde la mayoría de los estudiantes de 1er año plantea que siempre, por otro lado, la mayoría de 2do y 3er año consideran que nunca.

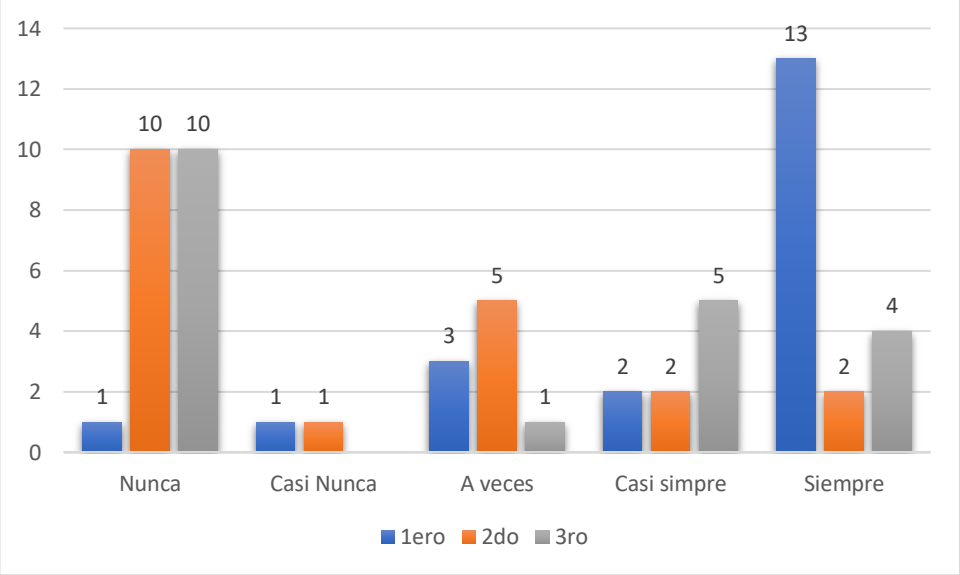


Figura 12. Realizar el respaldo y recuperación de información

Fuente: Elaboración propia

En la figura 13 se muestran los datos de la pregunta si en el laboratorio se han bloqueado puertos USB y la grabadora de CD/DVD para la protección de los medios informáticos, existe consenso en los tres años que nunca se realiza este proceso, por lo que se infiere que existen factores de riesgos de la seguridad de la información.

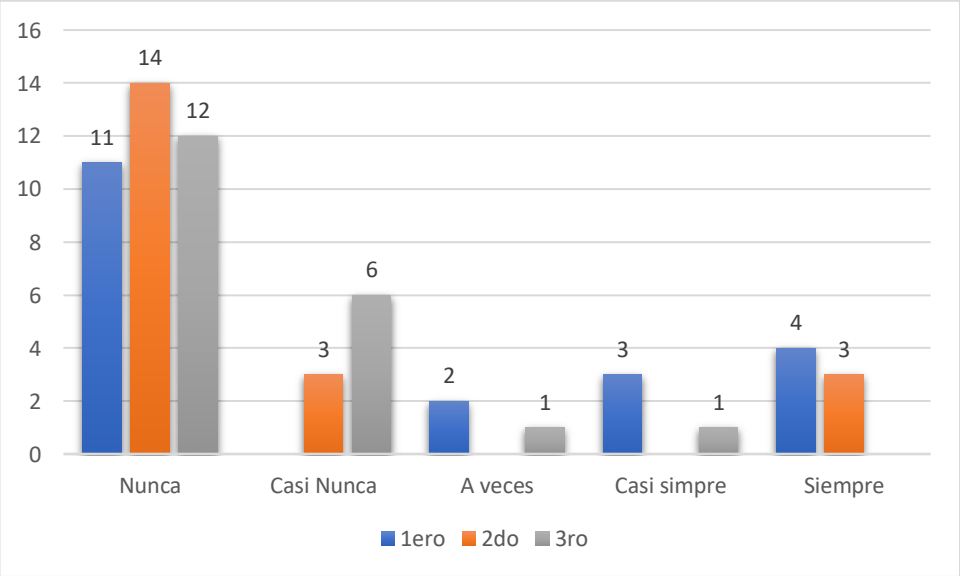


Figura 13. Bloqueado puertos USB y la grabadora de CD/DVD.

Fuente: Elaboración propia

En la figura 14 se hace referencia a Accesos y hábitos de conducta, la mayor cantidad de criterios aparece dividido en los años académicos, por lo que se realizará un análisis de los que más están representados en el ítem No, para comprender su dinámica.

En el caso del período de caducidad de la contraseña, la gran mayoría en los tres años académicos refiere no conocerla, lo que podría representar un problema serio en la seguridad informática, tomando en consideración que, el uso de contraseñas es un recurso valioso para preservar la seguridad de la información que tiene en su PC, uno de los recursos que brinda para que la misma se mantenga es un periodo de validez de su clave, que una vez cumplido deberá cambiarla.

Otro criterio representado en el Ítem No, es el sí conocen que están conectados en red. Para la mayoría de los estudiantes de 1^{ero} y 2do año, representa un problema, no así en el 3er año académico, a lo que se pueden asociar elementos de conocimiento y habilidades informática, que igualmente representa una brecha en la seguridad informática.

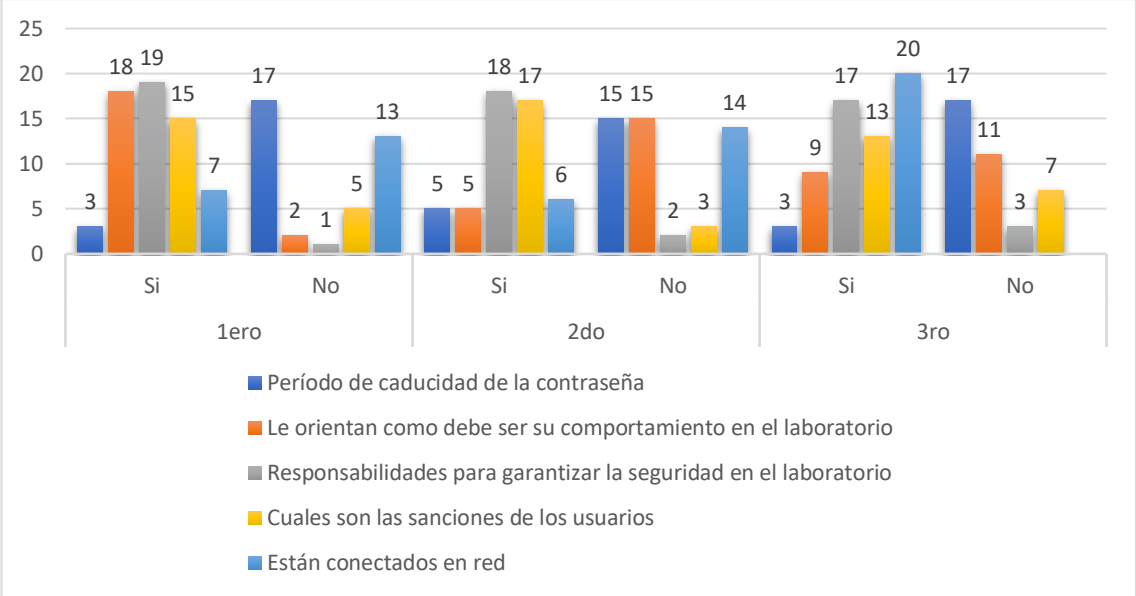


Figura 14. Accesos y hábitos de conducta.

Fuente: Elaboración propia

Un elemento interesante sobre los hábitos de conducta es que, en el año inicial, la mayoría de los estudiantes del 1er año, refiere que se les orienta como debe ser su comportamiento en el laboratorio, en el caso de los años continuantes, deja de ser una práctica cotidiana y se convierte por lo general en una formalidad, dejando a la espontaneidad de los educandos. Este último elemento también representa un riesgo en la seguridad informática, sobre todo en el resguardo de los datos y privacidad en el laboratorio.

En resumen, del instrumento de encuestas aplicado a los estudiantes de bachiller de la Unidad Educativa, en el caso de los años académicos, se percibe, insuficiente conocimiento por parte de los estudiantes sobre las regularidades en el trabajo del laboratorio, la salvaguarda de la información y de los hábitos de conducta, asociado a problemas de incumplimiento de los normado para la seguridad informática y el trabajo precedente que debe existir en este tipo de instalaciones. Los criterios divididos en los diferentes años académicos puede estar asociado a cuestiones de hábitos de formalidad, conformidad y confiabilidad que se ha creado entre los estudiantes, lo que puede constituir riesgos importantes en la seguridad informática.

3.6.2 Presentación y descripción de los resultados obtenidos

La triangulación de los resultados de investigación es una técnica y herramienta potente que facilita el uso de múltiples métodos para la articulación y validación de datos a través del cruce de dos o más fuentes (Charres et al., 2018). Además, se plantea que, la triangulación se establece como la combinación y de articulación de dos o más métodos para la obtención y recolección de datos. Como consecuencia, los datos observados y los datos de entrevista se codifican y se analizan separadamente, y luego se comparan, sustentados por los fundamentos teóricos, como una manera de validar los hallazgos.

En este sentido se puede observar en la tabla 3 la triangulación de los resultados de investigación de los instrumentos de la entrevista y la encuesta.

Se puede observar en la pregunta 1 de la entrevista realizada al encargado de laboratorio que, se cumple con el principio de una orientación y / o capacitación sobre seguridad informática en los laboratorios de computación porque han recibido cursos dictados por la universidad politécnica de Chimborazo, sin embargo, el Rector plantea que no se realizan capacitaciones, no obstante, se destaca que, los docentes a cargo conocen del tema. Mientras que la encuesta a los estudiantes en su pregunta 10 la mayoría refiere que si se les ha informado cuales son las sanciones de los usuarios por infringir las normas. Con base a estos criterios se considera que existe contradicción de los resultados porque el encargado y estudiantes refieren de forma positiva sobre el aspecto evaluado, no siendo así las respuestas del rector.

La pregunta 2 de la entrevista dice que, si existe alguna estrategia para garantizar la seguridad en el laboratorio de computación, se evidencia en las respuestas que el encargado de laboratorios dice que sí y pone ejemplos como el manejo del firewall de mikrotik para la restricción de páginas no autorizadas, por su parte el Rector plantea de forma negativa, donde los estudiantes sin embargo tienen criterios separados, los de

primer y segundo año plantea en su mayoría que no, respecto a la pregunta 9 de su encuesta y algo parecido ocurre con la pregunta 18 donde la mayoría refiere que nunca o a veces, no obstante, los estudiantes del tercer año de bachillerato en su mayoría lo realiza de forma positiva donde concuerdan con el encargado. Se puede ver que, tienen estrategia verbal, pero al no tenerlas registradas no se pueden comprobar.

En relación a la pregunta 4 de la entrevista sobre la divulgación sobre las acciones de seguridad informática que se deben desarrollar para el mantenimiento del laboratorio de computación el encargado refiere que no, por su lado el Rector plantea que cuando se trabajó virtual se brindó el servicio, en la presencialidad ninguna acción. Sobre el tema los estudiantes en su mayoría en la pregunta 3 de su encuesta responden en el mayor porcentaje que lo realizan a veces, casi siempre y siempre. Es criterio que existe contradicción de las opiniones porque el Rector y encargado plantean de forma negativa y los estudiantes tienen una percepción positiva.

Al evaluar las respuestas de la pregunta 9 de la entrevista sobre la evaluación al sistema de actualización de antivirus que se emplea en el laboratorio, el Rector y encargado refieren que es buena, no obstante, en los criterios de los estudiantes referente a tema en su pregunta 16 el mayor porcentaje de respuestas consideran que nunca o a veces tienen el servicio. Se constató que, el sistema de actualización de antivirus que se emplea en el laboratorio esta actualizado pero los estudiantes tienen criterios negativos del tema.

Tabla 3. Triangulación de los resultados de la entrevista y la encuesta.

Pregunta de la entrevista	**Respuesta**		**Pregunta de la encuesta**	**Respuesta de los estudiantes**	**Interpretación**
	Rector	**Encargado**			
1. ¿Qué orientaciones y / o capacitaciones ha recibido usted como directivo para proyectar con sus	No se realizan capacitaciones, aunque se destaca que los docentes a cargo	Han recibido cursos dictados por la universidad politécnica de Chimborazo	10. ¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el	La mayoría refiere que si se les han informado cuales son las sanciones de los usuarios	Se considera que existe contradicción de los resultados porque los encargados y estudiantes refieren de

trabajadores acciones de seguridad informática en los laboratorios de computación?	conocen del tema		laboratorio de computación?	por infringir las normas seguridad en el laboratorio	forma positiva sobre el aspecto evaluado, no siendo así las respuestas del rector
2. ¿Existe en la Unidad Educativa alguna estrategia para garantizar la seguridad en el laboratorio de computación? Mencione la estrategia y cuantos actores de la comunidad educativa se ven implicados en su implementación.	Plantea de forma negativa ya que no existen estrategias	Su respuesta es que sí y pone ejemplos como el manejo del firewall de mikrotik para la restricción de páginas no autorizadas	18. ¿En el laboratorio se han bloqueado puertos USB y la grabadora de CD/DVD para la protección de los medios informáticos?	Los de primer y segundo año plantea en su mayoría refiere que nunca o a veces, no obstante, los estudiantes del tercer año en su mayoría lo realizan de forma positiva donde concuerdan con el encargado	Se puede ver que, tienen estrategia verbal, pero al no tenerlas registradas no se pueden comprobar
4. ¿Considera usted que existe en la Unidad	Cuando se trabajó virtual se brindó el	No se realizan divulgaciones	3. ¿Se realizan con frecuencia mantenimiento	En su mayoría que lo realizan a	Se constató que, el Rector y encargado plantean de

Educativa suficiente divulgación sobre las acciones de seguridad informática que se deben desarrollar para el mantenimiento del laboratorio de computación? Mencione estas acciones.	servicio, en la presencialidad ninguna acción		s a los equipos informáticos del laboratorio de computación?	veces, casi siempre y siempre	forma negativa y los estudiantes tienen una percepción positiva
9. ¿Qué evaluación usted le otorga al sistema de actualización de antivirus que se emplea en el laboratorio?	Es buena	Es buena	16. ¿Se han habilitado las actualizaciones del antivirus?	Consideran que nunca o a veces tienen el servicio	Se plantea que, el sistema de actualización de antivirus que se emplea en el laboratorio esta actualizado pero los estudiantes tienen criterios negativos del tema.

Fuente: Elaboración propia

3.6.3 Informe final del análisis de los datos

Se reconoce que, como parte de los resultados de los instrumentos aplicados se revela la realidad sobre la gestión de riesgos y los datos en la unidad educativa objeto de análisis, puesto que no tiene implementada un plan de control de riesgos sobre todo en la

seguridad informática. Además, un gran porcentaje de sus miembros desconocen de estas prácticas; adicionalmente, se rescata el impacto que tiene la implementación de la auditoría informática como herramienta para mejorar gestión de control de riesgo.

Los hallazgos de la auditoría informática desarrollada en la unidad educativa, a partir de los resultados de los instrumentos han sido herramientas apropiadas para la obtención de resultados que muestran las falencias en seguridad informática y con ello exponen el análisis y gestión de riesgo del equipamiento tecnológico en los laboratorios de la institución objeto de análisis.

CAPÍTULO IV: MARCO PROPOSITIVO

4.1 Introducción

Para elaborar una propuesta, es necesario definir el tema establecido por una institución reglamentaria, con el propósito de llevar a cabo los procesos de titulación y egreso. Normalmente, se establece el tema del proyecto para registrar la temática de la tesis y se propone un índice tentativo para trabajar en dicho proyecto, el cual está relacionado con el tema elegido (Juárez, 2016).

En la investigación se desarrolla una Auditoría informática física y lógica para reducir o controlar los riesgos que se manifiesten durante la investigación relacionados con la seguridad informática. Para su desarrollo se empleó la metodología Magerit que permite el análisis y gestión de riesgo del equipamiento tecnológico de la Unidad Educativa “Alessandro Volta”.

La ejecución de la auditoría se llevó a cabo cumpliendo con la planificación que se presenta en este capítulo, ajustada a los criterios de evaluación y orientaciones de la metodología Magerit.

Para mayor comprensión del escenario donde se desarrolló la auditoría se presenta en este apartado una pequeña síntesis histórica de la Unidad Educativa “Alessandro Volta” está ubicada en la Cooperativa Santa Martha vivienda No 2, parroquia Verde, sector 3 en la Av. Jacinto Cortez y los Quinches, del cantón de Santo Domingo de los Tsáchilas.

La institución inicia sus labores en la Escuela Héroes de Paquisha en el año 1983, con 89 estudiantes y como Colegio particular sin nombre, mediante Acuerdo Ministerial 1734 del 25 de octubre de 1983. El año siguiente se consigue el Acuerdo Ministerial No. 3879 del 01 de junio de 1984 emanado por el Ministerio de Educación y Cultura con el nombre de Colegio Nacional Santa Martha. Para 1988, el MEC autoriza el funcionamiento definitivo de la especialidad de Electricidad. El 10 de diciembre de 1991 mediante Acuerdo Ministerial Nro. 099 se cambia la Razón Social de Colegio Nacional Santa Martha por Alejandro Volta.

Para el año 1993 se gestiona e incrementa a la Especialidad de Electrónica. En 1996 el Colegio alcanza el reconocimiento de Técnico Industrial. Y para el 2005 incrementa su tercera especialidad Electromecánica Automotriz. En el año 2013 ante la nueva distribución pasa a denominare Unidad Educativa Alejandro Volta, perteneciente a la Zona 4 Distrito 1.

En el año 2017, pasó a constituirse en la Unidad Educativa Siglo XXI, bajo el mismo nombre “Alejandro Volta”, producto de la fusión con las instituciones Aurelio Falconí, Carlos Tapia y 6 de noviembre. Con esta fusión se implementaron las especialidades de Comercialización y Ventas, Aplicaciones Informáticas y Bachillerato en Ciencias Generales. Por primera ocasión se amplió la oferta a la educación inicial y la Educación General Básica.

4.2 Descripción de la propuesta

En sentido general la propuesta persigue el desarrollo de una auditoría informática lógica y física mediante el uso de la metodología Magerit en la Unidad Educativa “Alessandro Volta” durante el periodo 2022. En el estudio se revela la realidad sobre la gestión de riesgos y los datos en la unidad educativa, puesto que no tiene implementada un plan de control de riesgos sobre todo en la seguridad informática en los laboratorios de computación.

Calcular la estimación del riesgo modelando impacto, probabilidad y riesgo por medio de escalas cualitativas. La utilización de la metodología Magerit se aplicó cumpliendo todas las etapas de una auditoría informática. La planificación de la auditoría tuvo como objetivo general realizar un análisis de riesgos de los equipos informáticos que se encuentran dentro de los laboratorios de computación de la Unidad Educativa “Alessandro Volta” mediante la auditoría informática con el empleo de la metodología Magerit. El objetivo específico está fundamentado en calcular la estimación del riesgo modelando impacto, probabilidad y riesgo por medio de escalas cualitativas en la unidad de análisis.

Para el desarrollo de la auditoría informática en la etapa de planificación se cuenta con cinco pasos fundamentales desde la conceptualización, los instrumentos, los criterios de evaluación según la metodología Magerit, la aplicación y tabulación de datos, por último, el informe de auditoría que culmina en los resultados y las conclusiones. Como instrumento principal se manejó para el desarrollo de la auditoría el cálculo de riesgo, donde tiene como criterios el impacto y probabilidad, cuenta con cuatro parámetros generales y los 22 ítems o preguntas.

4.3 Determinación de recursos

4.3.1 Humanos

Forman parte de los recursos humanos de esta investigación, el encargado de laboratorio de computación, el Rector, 60 estudiantes de bachillerato y la investigadora quien conduce la auditoría en la unidad educativa objeto de estudio.

4.3.2 Tecnológicos

Los principales recursos tecnológicos que se encuentran disponibles para desarrollar la auditoría informática son: dos laboratorios de computación donde existen 15 computadoras en cada uno para un total de 30 equipos los que tienen la descripción de ser capaz de recibir un conjunto de órdenes y ejecutarlas realizando cálculos complejos, o también agrupando y correlacionando otros tipos de información. La entrada o el ingreso es el acto por medio del cual se suministran los datos e instrucciones a la computadora.

Además, se encuentran dos impresoras multifuncionales, una en cada laboratorio estos son un equipo de impresión que es capaz de realizar varias funciones en un solo dispositivo: actúa como fotocopiadora, como escáner, como impresora y también puede actuar como fax.

Se logra tener como equipos disponibles los celulares del encargado de laboratorio, el Rector y la investigadora, los equipos celulares tienen como funciones de tener capacidad de procesamiento, abiertos a conexión permanente o intermitente a una red, cuenta con memoria (RAM, tarjetas MicroSD, flash, etc.) y realizan él envió y recibo de mensajes y llamadas, consultar la hora, utilizar la alarma entre otras funciones.

Herramientas a utilizar en el desarrollo de la investigación:

Las herramientas que se utilizó de manera principal es la computadora obteniendo el manejo y control de las actividades, a través de la aplicación de Excel y Word, para registrar todos los activos de los equipos informáticos, por medio de Word se realizaran los respectivos informes y recopilación de la información, desarrollo de la documentación requerida mediante la investigación a través de los docentes encargados en el área computación, de igual manera el uso de Internet, impresoras entre otros.

4.3.3 Económicos

El principal presupuesto que está disponible en el desarrollo de la Auditoría están las computadoras valoradas entre 624 ± 837 USD cada una, los celulares tienen un costo aproximado de 123 ± 252 USD y las impresoras 426 ± 621 USD, además de 380 horas de la investigadora teniendo en cuenta que los salarios mensuales están en la siguiente clasificación: Categoría A: $1.676. USD Categoría B: $1.412. USD Categoría C: $1.212 USD, en este sentido la investigadora está en la categoría B por ello percibe $1.412. USD de forma mensual.

4.4 Etapas de acción para el desarrollo de la propuesta

4.4.1 Fase I Planificación

Se puede observar en la tabla 4 la planificación de la auditoría informática la cual se encuentra ajustada a la metodología Magerit. Es evidente que está estructurada en el objetivo general, objetivo específico, los procedimientos o pasos de la metodología y los códigos para cada uno de los procedimientos.

Tabla 4. Planificación de la auditoría

Planificación de la auditoría informática ajustada a la metodología Magerit	
Objetivo general Realizar un análisis de riesgos de los equipos informáticos que se encuentran dentro de la Unidad Educativa "Alessandro Volta" mediante la auditoría informática con el empleo de la metodología Magerit. **Objetivo específico** Calcular la estimación del riesgo modelando impacto, probabilidad y riesgo por medio de escalas cualitativas.	
Procedimientos	**Códigos**
1. Conceptualización de la metodología Magerit	CMM 1
2. Instrumento aplicado para el levantamiento de la información. -Ficha de verificación elaborada de acuerdo con la metodología Magerit para el análisis de riesgos de los equipos informáticos que se encuentran dentro de la Unidad Educativa "Alessandro Volta"	ILInf 2 (FVer)
3. Criterios de evaluación aplicados según la metodología Magerit. - Criterio para estimación del riesgo por medio de escalas cualitativas.	CrEvMag 3
4. Aplicación de instrumentos y Tabulación de datos.	AInsTabD 4

5. Informe de auditoría (Capítulo V) 5.1. Resultados de la auditoría 5.2.Conclusiones del informe	InAud 5

Fuente: Elaboración propia.

4.4.1.1 Conceptualización de la metodología Magerit

De la búsqueda de la literatura científica sobre la conceptualización de la metodología Magerit la autora asume los supuestos teóricos de la definición De Santiago (2019), cuando plantea que; consiste en un método sistemático para el análisis y gestión de los riesgos que derivan del uso de la información. Su fin es informar de los riesgos y de la necesidad de gestionarlos a los responsables de la actividad, así como ayudar a encontrar y planificar un plan adecuado para tratarlos.

Por los elementos antes descritos se determinó oportuno para la unidad educativa "Alessandro Volta" el empleo de la metodología Magerit porque se busca realizar un análisis de riesgos de los equipos informáticos mediante la auditoría informática física y lógica, con ello se busca trazar un protocolo que permita el uso más eficiente y seguro de esta los medios informáticos en los laboratorios de computación dentro de la unidad educativa en esta se implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los directivos tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

4.4.1.2 Instrumento aplicado para el levantamiento de la información

Se empleó de la ficha de verificación elaborada de acuerdo con la metodología Magerit para el análisis de riesgos de los equipos informáticos que se encuentran dentro de la Unidad Educativa "Alessandro Volta". Se utilizó para el desarrollo de la auditoría el cálculo de riesgo con combinación de impacto y probabilidad por cada uno de los cuatro parámetros generales y los 22 ítems que son posibles riesgos detectados en el proceso de análisis. Están las instrucciones que existen por la importancia de los riesgos, dado que se tiene para el impacto de riesgo y probabilidad de ocurrencia los indicadores de evaluación en correspondencia con los parámetros generales que serán evaluados (Anexo 4).

4.4.1.3 Criterios de evaluación aplicados según la metodología Magerit

Como se pude observar en la tabla 5, el criterio aplicado fue el que la metodología Magerit presenta para la estimación del riesgo por medio de escalas cualitativas; con este se modelan impacto, probabilidad y riesgo.

Tabla 5. Escala de estimación del riesgo

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012)

Para calcular riesgo de manera cualitativa se combinan impacto y probabilidad como muestra la tabla 6 en un ejemplo.

Tabla 6. Cálculo de riesgo con combinación de impacto y probabilidad

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012)

La metodología Magerit se destaca en analizar el impacto que puede provocar a una empresa la violación de seguridad; identificando las amenazas y vulnerabilidades para crear medidas preventivas y correctivas más apropiadas; presentando una guía completa paso a paso de cómo llevar a cabo el análisis de riesgos.

En este sentido la tabla 7 muestra la matriz del cálculo de riesgo con combinación de impacto y probabilidad en la Unidad Educativa “Alessandro Volta”. Se evidencia que el color rojo correspondiente a riesgo crítico tiene mayor predominio con 10 preguntas respecto a las realizadas, a su vez el segundo color predominante es el gris con siete preguntas correspondiente a riesgo despreciable, por otro lado, de igual forma con dos preguntas está representado el color amarillo y blanco (sin color), por último, con una solo pregunta se encuentra en color carmelita respecto al riesgo importante.

Tabla 7. Matriz del cálculo de riesgo con combinación de impacto y probabilidad en la Unidad Educativa “Alessandro Volta”.

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**		SMI4	CSO1	SMI1, CSO2, CSO3, CSO4, CSO5, CSO6, CSO7	
	A				SMI2	
	M			GCET2, GCET5	GCET1	
	B	PRDO2, PRDO4	SMI3	GCET3		
	MB	GCET4, PRDO1, PRDO3, PRDO5, SMI5				

Fuente: Elaboración propia.

Se puede observar en la tabla 8 el resultado de la matriz de los parámetros generales respecto a las preguntas de acuerdo con el tipo de riesgo. Cuando se realiza el análisis al parámetro general de Gestión y control del equipamiento tecnológico (GCET) se puede observar que uno de los riesgos es clasificado como importante corresponde a la pregunta (para un 20% del total de preguntas del parámetro): En los laboratorios algunas computadoras ya no son funcionales y no han sido remplazadas, tiene además dos evaluados de apreciable con color amarillo lo que tienen relación a las preguntas (para un 40% del total de preguntas del parámetro): los periféricos de las computadoras existentes en la unidad educativa no funcionan en su totalidad y el inventario del equipamiento tecnológico de la Unidad Educativa está desactualizado, además tiene una pregunta correspondiente a riesgo bajo y otra a riesgo despreciable, donde son: Es inadecuada la ubicación de las computadoras con relación al espacio físico de los

laboratorios (para un 20% del total de preguntas del parámetro) y la pregunta El número de computadoras en los laboratorios no es suficiente para la cantidad de usuarios (para un 20% del total de preguntas del parámetro), respectivamente.

Tabla 8. Matriz de los parámetros generales respecto a las preguntas de acuerdo con el tipo de riesgo

Parámetros generales	**Preguntas**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
GCET	A	M	B	MB	M		
PRDO	MB	MB	MB	MB	MB		
SMI	MA	MA	B	MA	MB		
CSO	MA	MA	MA	MA	MA	MA	MA

Fuente: Elaboración propia.

Siguiendo la misma idea al analizar el parámetro general de Procedimientos y responsabilidades de operación (PRDO) se puede observar que el 100% de sus preguntas están relacionadas con riesgo despreciable representados con el color gris.

Por su parte el parámetro general de Seguridad en la utilización de medios informáticos (SMI) tiene el 60% de sus preguntas evaluadas de riesgo crítico visto en las preguntas de: los medios informáticos están desprotegidos pues no se han bloqueado puertos USB y la grabadora de CD/DVD, las sanciones que pueden recibir los usuarios por infringir las normas de seguridad de los equipos informáticos no se encuentran publicadas y en los laboratorios de computación no existe un registro para el control de entrada y salida de los usuarios, representados con el color rojo. Otro de sus preguntas corresponde al riesgo bajo para un 20% del total de preguntas del parámetro y el otro 20% responde a otra pregunta que esta evaluada de riesgo despreciable de acuerdo con que los horarios para la atención a usuarios en los laboratorios no están publicados.

Cuando se evaluado el parámetro general de Control de acceso al sistema operativo (CSO) se puede observar que el 100% de sus preguntas se encuentra en análisis crítico vistos por el color rojo, lo que evidencia que la alta dirección debe tomar decisiones con todos los parámetros evaluados pero en este último se debe prestar mayor prioridad de sus resultados, porque es el más comprometido en lograr la satisfacción de los usuarios respecto a la seguridad informática en los laboratorios de computación.

En síntesis, cuando se realiza la clasificación según el cálculo de riesgo de manera cualitativa se combinan impacto y probabilidad como resultados se obtuvo que 11 (50%) de los indicadores son críticos, uno (4.5%) son importante, uno (4.5%) es apreciable, dos

(9%) son de riesgo bajo y siete (32%) son despreciables, se puede evidenciar que los mayores riesgos en la unidad educativa son de categoría críticos.

4.4.1.4 Aplicación de instrumento y tabulación de datos

Los instrumentos se aplicaron en la Unidad Educativa "Alessandro Volta", a todos los equipos tecnológicos de esta institución, pero con mayor peso en los laboratorios.

Los datos obtenidos se tabularon asignando códigos a cada uno de los riesgos (Anexo 5). Se tabularon primeramente los impactos y luego la probabilidad, para cada caso se analizó por riesgo y por parámetro general.

Los resultados de esta auditoría se presentan en el siguiente capítulo donde se completa el cumplimiento de la planificación de la propuesta.

4.4.2. Informe final del análisis de los datos

Como conclusiones de este apartado se pudo constatar los pasos principales para el desarrollo de la Auditoría informática en los laboratorios de la Unidad Educativa "Alessandro Volta", aspectos que son conducentes de la metodología de Magerit. Se puede evidenciar la estructura de la ficha de verificación que fue utilizada en el desarrollo de la Auditoría, donde se muestran los resultados de sus componentes, parte de ella son los resultados del instrumento los cuales se muestran en el capítulo siguiente a partir de la implementación de la ficha en la unidad educativa.

CAPÍTULO V: EVALUACIÓN DE RESULTADOS

5.1 Introducción

En el capítulo de evaluación de resultados se muestran los principales hallazgos obtenidos con la implementación de la ficha de verificación de la Auditoría informática aplicada a los laboratorios de computación de la Unidad Educativa "Alessandro Volta". Se tomó como aspectos fundamentales los propuestos por la metodología de Magerit donde se tienen cinco contenidos fundamentales.

En este apartado de forma concreta se evidencian los resultados de la ficha donde tiene cuatro parámetros generales los que son: Gestión y control del equipamiento tecnológico, Procedimientos y responsabilidades de operación, Seguridad en la utilización de medios informáticos, y Control de acceso al sistema operativo, cada uno de los parámetros cuenta con preguntas o ítems los cuales son comprendidos como principales riesgos en el proceso de Auditoría llegando a sumar un total de 22 riesgos.

Estos resultados son importantes para los directivos de la unidad educativa por lograr una toma de decisiones más factibles para el control o minimizar los riesgos presentes en la seguridad informática y con ello lograr un mayor nivel de satisfacción de los servicios informáticos de la comunidad educativa.

5.2 Informe detallado

El informe que se presenta muestra los hallazgos encontrados en la auditoría informática física y lógica desarrollada en la Unidad Educativa Alessandro Volta, en el período académico 2022.

5.2.1. Dirigido a Directivos de la Unidad Educativa y profesor de computación que funciona también como responsable de informática en el centro.

5.2.2. Motivo Concluir con los requerimientos académicos que la titulación exige aplicado al área de auditoría informática y seguridad de la información.

5.2.3. Objetivos

Realizar un análisis de riesgos de los equipos informáticos que se encuentran dentro de la Unidad Educativa "Alessandro Volta" mediante la auditoría informática con el empleo de la metodología Magerit.

Calcular la estimación del riesgo modelando impacto, probabilidad y riesgo por medio de escalas cualitativas.

5.2.4. Alcance

La auditoría desarrollada, abarcó toda la infraestructura tecnológica de la Unidad Educativa, se realizó en un período académico 2022 y fue aplicada una ficha de verificación ajustada a la metodología Magerit que permitió analizar cualitativo de los riesgos asociados a la seguridad física y lógica de la infraestructura informática de la Unidad Educativa. Para el cálculo de la estimación de riesgos informáticos antes de realizó en análisis de los riesgos de manera independiente y por parámetro general. A continuación, se presenta un preámbulo de los hallazgos encontrados en el desarrollo de la auditoría.

5.2.5. Hallazgos

El Anexo 6 presenta los resultados de la ficha de verificación los cuales sirve para realizar las figuras por parámetro general y los riesgos incluidos en cada uno de estos. Se muestra en la figura 15 el Parámetro gestión y control del equipamiento tecnológico donde se constata que, los parámetros más afectados son: el hecho que en los laboratorios algunas computadoras ya no son funcionales y no han sido remplazadas, otro elemento de impacto de evaluación media, son que los periféricos de las computadoras existentes en la unidad educativa no funcionan en su totalidad y el inventario del equipamiento tecnológico de la Unidad Educativa está desactualizado. Estos elementos sin embargo tienen una probabilidad de ocurrencia de probable en el primero y de posible en los otros dos criterios, respectivamente. Por lo que la gestión y control del equipamiento puede estar afectada al tener la mayor cantidad de sus criterios en riesgo de impacto y probabilidad.

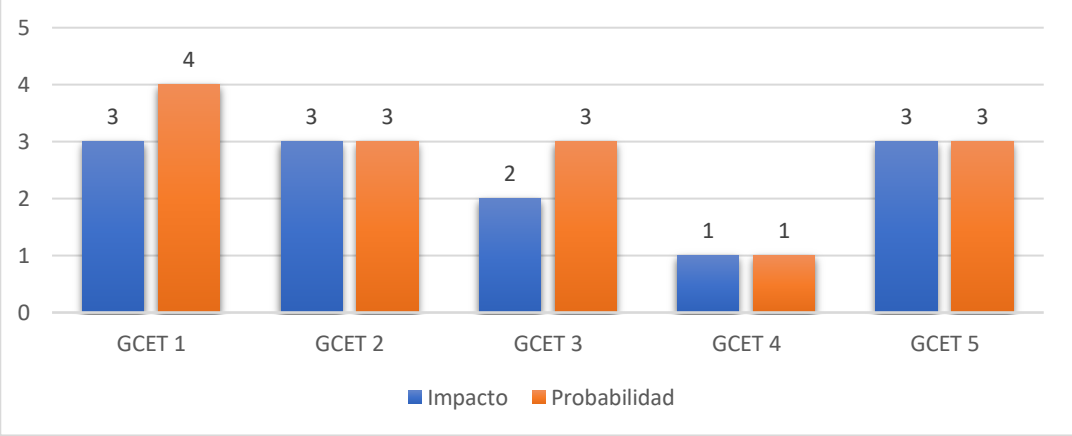


Figura 15. Parámetro gestión y control del equipamiento tecnológico.

Fuente: Elaboración propia

En la figura 16 se realiza un análisis similar, donde se encontró que los procedimientos y responsabilidades de operación, no obstante, se revela que son bajos los impactos y muy raras las probabilidades de ocurrencia de estos criterios.

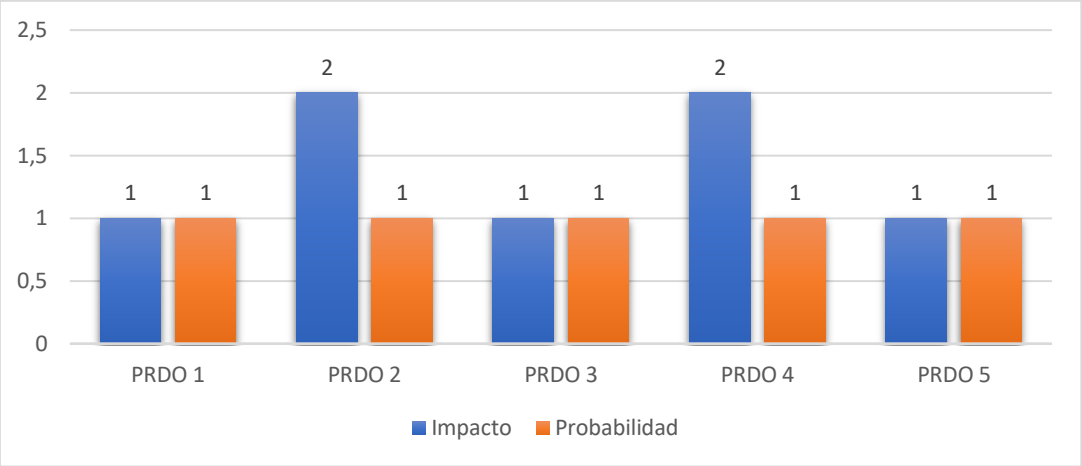


Figura 16. Parámetro procedimientos y responsabilidades de operación.

Fuente: Elaboración propia

La figura 17 refleja un contexto diferente en cuanto a los criterios de la Seguridad en la utilización de medios informáticos, se pueden encontrar afectados con un impacto muy alto: que los medios informáticos están desprotegidos pues no se han bloqueado puertos USB y la grabadora de CD/DVD, con una alta probabilidad de ocurrencia, otro elemento es que las sanciones que pueden recibir los usuarios por infringir las normas de seguridad de los equipos informáticos no se encuentran publicadas, elemento que es probable que ocurra y que en los laboratorios de computación no existe un registro para el control de entrada y salida de los usuarios, este último elemento viola toda normativa de la seguridad informática, desde la gestión de auditoría.

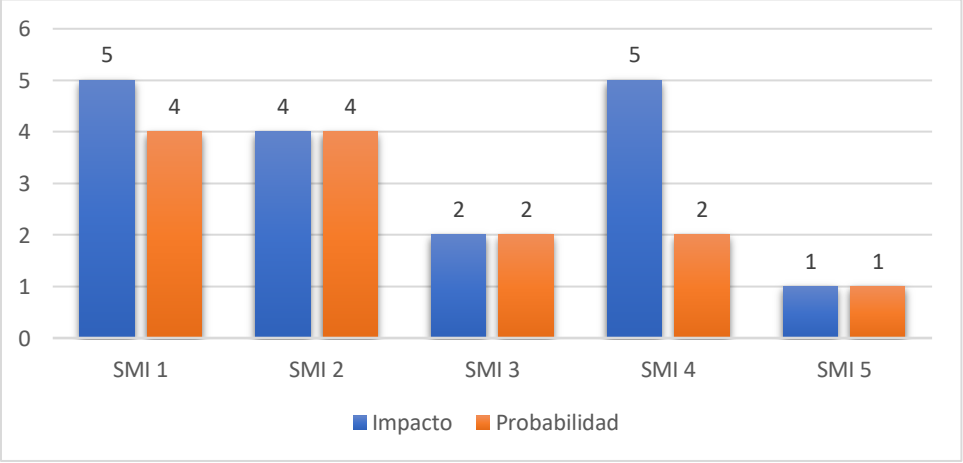


Figura 17. Parámetro seguridad en la utilización de medios informáticos.

Fuente: Elaboración propia

La figura 18, en cuanto a al control de acceso al sistema operativo tiene marcado todos sus criterios con un alto impacto, así como la mayoría de ellos posee una alta probabilidad de ocurrencia. En la ficha de verificación se puede observar además su compartimento, que en la figura se grafica de manera clara. Casi todos los criterios alcanzan un valor de 5, Muy alto. Se destaca en las cuestiones de la seguridad informática para el control de la auditoría, el hecho que, nunca se inhabilita a los usuarios por superar el número de intentos de acceso fallidos, lo que puede contribuir al robo de secciones y que en el laboratorio se han instalado antivirus pero no se han habilitado las actualizaciones, entre otros elementos.

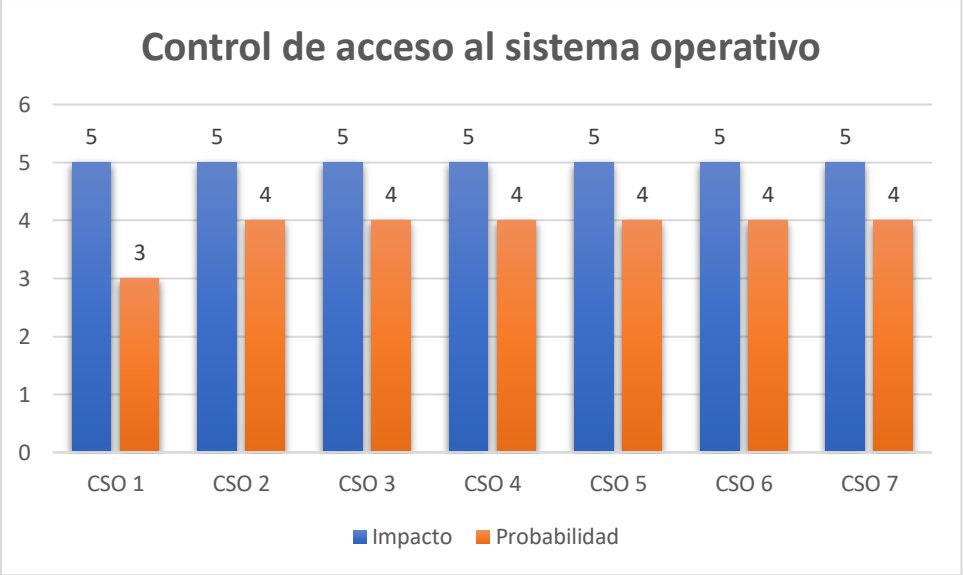


Figura 18. Parámetro control de acceso al sistema operativo.

Fuente: Elaboración propia

En resumen, los elementos antes planteados como parte de la evaluación de la ficha de verificación, permitió reconocer que pueden existir probablemente riesgos de la seguridad informática en los laboratorios, al constatar criterios en su mayoría son evaluados de medio al muy alto impacto de ocurrencia.

5.3 Interpretación objetiva: conclusiones y recomendaciones

Los resultados de la ficha de verificación de los cuales a partir de la interpretación de sus resultados por para parámetro general y los riesgos incluidos en cada uno de estos se pudo constatar que el parámetro más afectado en la ocurrencia de riesgos fue Control de acceso al sistema operativo por lo que se debe mostrar mayor interés a minimizar y control los riesgos asociados en el parámetro.

Como parte del desarrollo una Auditoría informática lógica y física mediante el uso de la metodología Magerit se presentan en la unidad educativa una probabilidad de

ocurrencia de riesgo de media a alta y un impacto de media a muy alto en la mayoría de los criterios evaluados.

Los resultados de la clasificación según el cálculo de riesgo de manera cualitativa más del 50 % de los indicadores son críticos lo que evidencia un impacto y probabilidad de ocurrencia alto por ello se deben tomar todas las decisiones posibles en corto periodo de tiempo para minimizar y controlar los riesgos.

Se recomienda realizar anualmente una Auditoría para ver el estado actual de los equipos y su funcionamiento para que brinden un correcto servicio y que no estén vulnerables a los daños físicos como lógicos y lograr tener un control de la seguridad de su base de datos de la red informática en los laboratorios informáticos de la unidad educativa.

Se debe elaborar un calendario de mantenimiento correctivo y preventivo de rutina periódico. Además, se debe crear nuevas políticas de seguridad para el correcto uso de sistemas informáticos y se debe actualizar la documentación y el manual de políticas de seguridad.

Revisar los perfiles de los usuarios en cada uno de los recursos, buscar inconsistencia en los perfiles, cuentas con privilegios elevados, cuentas huérfanas, etc.

Se recomienda realizar mantenimiento permanente a los diferentes equipos físicos como lógicos, porque las vulnerabilidades son constantes y cambiantes al pasar el tiempo teniendo en cuenta que las salvaguardas no son iguales para todos los activos, además la creación de backup con nuevas políticas de seguridad y un sistema en caso de desastres naturales o robo.

Como complemento importante del informe de auditoría se propone una guía de buenas prácticas informáticas para la seguridad lógica y física en la Unidad Educativa “Alessandro Volta”. Esta guía fue redactada a partir de los hallazgos encontrados en la auditoría y puede encontrarse en el Anexo 7 de este trabajo de investigación.

5.4.Guía de buenas prácticas informáticas para la seguridad física y lógica

Introducción

La rápida evolución tecnológica de los últimos años ha traído consigo una dependencia creciente de los equipos informáticos en todos los ámbitos de la sociedad, incluyendo el sector educativo. La Unidad Educativa, como institución que promueve la formación y el desarrollo integral de sus estudiantes, debe asegurar el uso adecuado y seguro de los recursos informáticos a su disposición.

En este sentido, se ha detectado durante la auditoría informática realizada en la Unidad Educativa la ausencia de un plan de control de riesgos en seguridad informática, lo que se traduce en una vulnerabilidad de los equipos informáticos y la información que en ellos se maneja. Además, se han identificado otros problemas como la falta de actualización del inventario del equipamiento tecnológico, la ausencia de registro de entrada y salida de usuarios en los laboratorios de computación, y la falta de implementación de sanciones por infringir las normas de seguridad informática.

Para abordar estos problemas, se propone en este trabajo la elaboración de una guía de buenas prácticas informáticas para la Unidad Educativa, la cual busca establecer los lineamientos para el uso seguro y responsable de los recursos informáticos en la institución. Con esta guía se pretende garantizar la protección de la información y los equipos informáticos, establecer las políticas y prácticas de seguridad informática, y fomentar el uso responsable y ético de los recursos informáticos en la Unidad Educativa.

Objetivo general: Establecer los lineamientos para el uso seguro y responsable de los recursos informáticos en la Unidad Educativa para la protección de la información y los equipos informáticos.

Objetivos específicos:

- Sugerir procedimientos para la gestión de riesgos informáticos, incluyendo la identificación, evaluación y tratamiento de los riesgos asociados con el uso de los equipos informáticos en la Unidad Educativa.
- Plantear los lineamientos para la gestión de los equipos informáticos, incluyendo la identificación, adquisición, mantenimiento y renovación de los mismos.
- Proponer políticas y prácticas de seguridad informática, incluyendo el bloqueo de puertos USB y grabadoras de CD/DVD, la gestión de contraseñas, el registro de entradas y salidas de usuarios y la implementación de sanciones por infracciones a las normas de seguridad.
- Fomentar el uso responsable y ético de los recursos informáticos, incluyendo el respeto de los derechos de autor, la privacidad y la propiedad intelectual.
- Sugerir la capacitación de los usuarios en el uso seguro y responsable de los equipos informáticos, incluyendo la formación en la gestión de riesgos, seguridad informática y ética en el uso de los recursos informáticos.

Justificación de la presentación de la guía de buenas prácticas informáticas

La guía de buenas prácticas informáticas en la Unidad Educativa es crucial para garantizar la seguridad y protección de los equipos y datos, así como también para fomentar un uso responsable de la tecnología en el entorno educativo.

Los hallazgos encontrados en la auditoría física y lógica desarrollada son el punto de partida para la elaboración de la guía de buenas prácticas informáticas que se propone en este apartado y en la contribución que esta ofrece se concreta su importancia.

Al resaltar las consecuencias que podría traer consigo cada hallazgo detectado se muestra la relevancia que tiene la guía como propuesta de solución:

-Como primer aspecto a considerar está la ausencia de un plan de control de riesgos en la seguridad informática de la Unidad Educativa que la deja vulnerable a posibles amenazas informáticas, como virus, malware y ataques cibernéticos. Una guía de buenas prácticas informáticas puede ayudar a establecer políticas y medidas preventivas para proteger los equipos y datos de posibles riesgos.

-El hecho de que algunas computadoras no funcionen y que los periféricos no estén en pleno funcionamiento puede tener un impacto negativo en el aprendizaje y productividad de los estudiantes y el personal docente. Una guía de buenas prácticas informáticas puede incluir recomendaciones sobre el mantenimiento y actualización regular de los equipos para asegurar su correcto funcionamiento.

-La falta de un registro para el control de entrada y salida de los usuarios puede hacer que sea difícil identificar posibles infracciones o actos de vandalismo en los equipos informáticos, lo que puede llevar a la pérdida de datos y tiempo de inactividad. Una guía de buenas prácticas informáticas puede establecer políticas de registro y control de acceso para garantizar la seguridad y el uso responsable de los equipos.

-La falta de sanciones claras para los usuarios que infrinjan las normas de seguridad de los equipos informáticos puede fomentar un comportamiento irresponsable y negligente en el uso de la tecnología, lo que puede poner en riesgo la seguridad de los equipos y datos. Una guía de buenas prácticas informáticas puede establecer políticas claras sobre las sanciones que se aplicarán en caso de infracciones.

-La falta de bloqueo de puertos USB y la grabadora de CD/DVD puede permitir la copia no autorizada de datos y la introducción de virus y malware en los equipos informáticos. Una guía de buenas prácticas informáticas puede incluir recomendaciones sobre cómo bloquear estos puertos y establecer políticas para el uso responsable de los medios informáticos.

-Por último, la falta de habilitación de las actualizaciones de los antivirus puede dejar a la Unidad Educativa vulnerable a posibles amenazas informáticas, porque los antivirus no estarán actualizados para detectar las últimas amenazas. Una guía de buenas prácticas informáticas puede incluir recomendaciones sobre cómo habilitar las actualizaciones de los antivirus y establecer políticas para su uso adecuado.

En consecuencia, con lo expuesto se sugieren a continuación las buenas prácticas y las acciones que para cada una de ellas se recomiendan en la guía propuesta:

Buena Práctica	**Acciones recomendadas**
Implementa un plan de control de riesgos sobre todo en la seguridad informática	1. Realiza una evaluación de riesgos al menos anualmente y define medidas de seguridad en consecuencia. 2. Establece una política de seguridad que incluya la definición de contraseñas seguras, la prohibición de compartir contraseñas, y la autenticación de los usuarios. 3. Mantén actualizado el software de seguridad y antivirus en todas las computadoras y dispositivos.
Reemplazo de las computadoras que ya no funcionan en la Unidad Educativa	1. Mantén un registro de inventario actualizado y evalúa el estado de los equipos regularmente. 2. Establece un presupuesto y plan de reemplazo para los equipos obsoletos o dañados.
Verificación del estado de los periféricos existentes y actualización del inventario de equipamiento tecnológico en la Unidad Educativa.	1. Mantén un registro actualizado de los periféricos y dispositivos. 2. Reemplaza o repara los periféricos y dispositivos que no funcionen correctamente.

Protección de los medios informáticos	1. Bloquea los puertos USB y la grabadora de CD/DVD para evitar la instalación de software malintencionado. 2. Establece permisos y controles de acceso a los medios informáticos.
Establecimiento y Publicación de las sanciones para los usuarios que infrinjan las normas de seguridad	1. Crea un documento que establezca las sanciones por infracciones de seguridad. 2. Asegúrese de que los usuarios estén al tanto de las sanciones.
Establecimiento de un registro de control de entrada y salida de los usuarios	1. Crea un registro para controlar el acceso y la salida de los usuarios en el laboratorio. 2. Verifica la identidad de los usuarios y limita el acceso a las computadoras según el tipo de usuario.
Inhabilita a los usuarios por superar el número de intentos fallidos de acceso	1. Configura la política de seguridad para inhabilitar a los usuarios después de un número determinado de intentos fallidos. 2. Asegure que los usuarios estén al tanto de esta política.
Habilita las actualizaciones del software de seguridad y antivirus	1. Configura los softwares de seguridad y antivirus para habilitar actualizaciones automáticas. 2. Verifica que las actualizaciones se estén instalando correctamente y en tiempo y forma.
Capacitación a los responsables de informática de la Unidad Educativa.	1. Capacitar a los usuarios del laboratorio sobre buenas prácticas informáticas y seguridad, de manera que estén conscientes de los riesgos y sepan cómo prevenirlos.

Propuesta de Política de sanciones por infracciones de seguridad informática en la Unidad Educativa

La Unidad Educativa, en su compromiso por garantizar el uso seguro y responsable de los recursos informáticos, establece la presente política de sanciones por infracciones de seguridad informática. El objetivo de esta política es establecer las sanciones correspondientes a los usuarios que, de manera negligente o malintencionada, incumplen las normas de seguridad informática establecidas en la institución.

Infracciones y sanciones

A continuación, se detallan las infracciones de seguridad informática que serán objeto de sanción, así como las sanciones correspondientes:

Acceso no autorizado*:* Se considera acceso no autorizado al ingreso a sistemas o información sin contar con los permisos necesarios.

Sanciones:

Primera infracción: Amonestación verbal.

Segunda infracción: Amonestación escrita.

Tercera infracción: Suspensión del acceso a los sistemas informáticos por un período determinado de tiempo.

Cuarta infracción: Revocación definitiva del acceso a los sistemas informáticos.

Mal uso de los recursos informáticos: Se considera mal uso de los recursos informáticos a la utilización de los mismos con fines distintos a los académicos o administrativos de la Unidad Educativa.

Sanciones:

Primera infracción: Amonestación verbal.

Segunda infracción: Amonestación escrita.

Tercera infracción: Suspensión del acceso a los sistemas informáticos por un período determinado de tiempo.

Cuarta infracción: Revocación definitiva del acceso a los sistemas informáticos.

Instalación de software no autorizado: Se considera instalación de software no autorizado a la instalación de programas o aplicaciones en los equipos informáticos de la Unidad Educativa sin contar con los permisos correspondientes.

Sanciones:

Primera infracción: Amonestación verbal.

Segunda infracción: Amonestación escrita.

Tercera infracción: Suspensión del acceso a los sistemas informáticos por un período determinado de tiempo.

Cuarta infracción: Revocación definitiva del acceso a los sistemas informáticos.

Copia o distribución de información confidencial: Se considera copia o distribución de información confidencial a la reproducción o divulgación de información o datos que tengan carácter confidencial o privado.

Sanciones:

Primera infracción: Amonestación escrita.

Segunda infracción: Suspensión del acceso a los sistemas informáticos por un período determinado de tiempo.

Tercera infracción: Revocación definitiva del acceso a los sistemas informáticos.

Ataques informáticos: Se considera ataque informático a la realización de acciones que puedan dañar o comprometer la integridad de los sistemas informáticos de la Unidad Educativa.

Sanciones:

Primera infracción: Suspensión inmediata del acceso a los sistemas informáticos y denuncia a las autoridades competentes.

Elaborado por: _____

Aprobado por: _____

Propuestas de temas de capacitación para los usuarios del laboratorio sobre buenas prácticas informáticas y seguridad

Tema	Objetivo
Seguridad de contraseñas.	Enseñar a los usuarios cómo crear contraseñas seguras y fáciles de recordar, cómo cambiarlas regularmente y cómo no compartirlas con nadie.
Phishing y correo electrónico fraudulento	Identificar y evitar correos electrónicos sospechosos, cómo verificar la autenticidad de los correos electrónicos y cómo no hacer clic en enlaces desconocidos.
Seguridad de la red	Asegurar la conexión inalámbrica de los dispositivos, la importancia de no compartir la red y cómo utilizar conexiones seguras y privadas, como VPN.
Actualización de software y antivirus	Enseñar la importancia de tener software actualizado y programas antivirus activos en todas las computadoras.
Protección de datos y privacidad	Explicar cómo proteger los datos personales y confidenciales, cómo evitar la pérdida de datos y cómo mantener la privacidad en línea.
Uso adecuado de dispositivos extraíbles	Explicar cómo utilizar de manera segura los dispositivos de almacenamiento extraíbles, como USB o discos duros externos, y cómo evitar la propagación de virus.
Accesos y permisos	Instruir sobre cómo se concede y revocan los permisos de acceso a los dispositivos y a los archivos.
Uso adecuado de redes sociales	Enseñar a los usuarios cómo configurar adecuadamente la privacidad en las redes sociales y cómo evitar compartir información personal que pueda comprometer la seguridad.
Respaldo y restauración de datos	Enseñar cómo respaldar regularmente los datos y cómo restaurarlos en caso de un fallo en el sistema.

Normas de seguridad y políticas de uso	Asegurar que los usuarios estén familiarizados con las políticas y normas de seguridad de la organización y su importancia en la prevención de riesgos.

Conclusiones de la guía de buenas prácticas informáticas

Es importante destacar que la implementación de estas prácticas no solo beneficia a la Unidad Educativa, sino también a los usuarios finales, porque reduce los riesgos de fraude, robo de identidad y otros delitos informáticos.

La guía de buenas prácticas informáticas presentada en este trabajo puede ser utilizada como una herramienta valiosa para mejorar la seguridad y privacidad de la información, y contribuir así a reducir los riesgos y aumentar la confianza de los usuarios en el uso de la tecnología.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Se logró desarrollar una auditoría informática lógica y física mediante el uso de la metodología Magerit en la Unidad Educativa "Alessandro Volta" durante el periodo 2022, con lo cual se realizaron los análisis pertinentes, la interpretación de los resultados y su graficación para comprender a dinámica de su evolución. Con lo cual se reconocen los siguientes elementos conclusivos.

- La sistematización de los fundamentos teóricos referidos a las variables de estudio: auditoría informática y equipos informáticos, permitió constatar que en la literatura esta actividad tiene un papel importante y de gran impacto social, con lo cual se realiza una revisión práctica sobre la utilización de los recursos informáticos con que cuenta una entidad y así emitir un informe sobre la situación en la que se gestionan esos recursos, con un análisis crítico por parte de los auditores, se logra analizar las condiciones de una instalación informática, para el caso proporcionar un análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.
- Se diagnosticó la situación actual de los laboratorios de la Unidad educativa Alessandro Volta y de los programas que se usan a partir de la aplicación de un grupo de instrumentos, con lo que se obtuvo que, se percibe insuficiente conocimiento por parte de los estudiantes sobre las regularidades en el trabajo del laboratorio, la salvaguarda de la información y de los hábitos de conducta, asociado a problemas de incumplimiento de los normado para la seguridad informática y el trabajo precedente que debe existir en este tipo de instalaciones. Los criterios divididos en los diferentes años académicos puede estar asociado a cuestiones de hábitos de formalidad, conformidad y confiabilidad que se ha creado entre los estudiantes, lo que puede constituir riesgos importantes en la seguridad informática.
- Al realizar un análisis de riesgos de los equipos informáticos que se encuentran dentro de la "Unidad Educativa Alessandro Volta" mediante la auditoría informática con el empleo de la metodología Magerit, permitió reconocer que pueden existir probablemente riesgos de la seguridad informática en los laboratorios, al constatar criterios en su mayoría son evaluados de medio al muy alto impacto de ocurrencia.
- El informe de la auditoría elaborado tuvo como fin la búsqueda de las debilidades existentes y las brechas en la seguridad, con lo cual se mejoran las actividades

planificadas por los encargados de los laboratorios. Con estos elementos y con la guía de buenas prácticas propuesta a posterior se pueden reducir o controlar los riesgos relacionados con la seguridad informática de la Unidad Educativa "Alessandro Volta" ubicada en Santo Domingo de los Tsáchilas.

6.2 Recomendaciones

- Resulta oportuno que los directivos de la Unidad Educativa "Alessandro Volta" tomen en cuenta los criterios de la presente auditoría informática a los laboratorios de computación que los ayude a tomar decisiones en disminuir y controlar los riesgos de seguridad informática de los laboratorios de computación lo que redundará en beneficios para toda la comunidad educativa.
- Sugerir a los directivos de la Unidad Educativa "Alessandro Volta" puedan incorporar en su plantilla a tiempo completo como parte de su estructura un encargado de los laboratorios de computación el cual pueda dedicarse en sus funciones a disminuir y solucionar los riesgos de seguridad informática presentes en los locales de la comunidad educativa con énfasis los laboratorios de computación.
- El informe de auditoría debe ser usado como línea base para generar una línea base de proyectos, mismos que están orientados a mitigar los riesgos identificados, la prioridad la puede dar la organización o el jefe del área de tecnología de la unidad educativa.
- Se recomienda que los directivos tomen en cuenta estándares como: ISO/IEC 27002:2015 Código de buenas prácticas para la Gestión de la Seguridad de la Información, COBIT e ITIL (mejores prácticas de prestación de servicios TI y auditoría) y CISCO (estándares internacionales de redes y telecomunicaciones)
- Implementar un sistema de administración de incidencias que cuente con un inventario, de modo que, sea capaz de tener el control de las incidencias atendidas por soporte, conocer los equipos que más incidencias han presentados, así como otros filtros que se considere por los directivos de la unidad educativa.
- Fortalecer la política de comunicación de la cultura de riesgo, realizar ejercicios, evaluaciones y motivar el aprendizaje con recompensas y reconocimientos a las personas que los conozcan.
- Crear los ambientes de pruebas y control de calidad, estos ambientes serán usados para evaluar las aplicaciones antes de su pase a producción, también contendrán los datos necesarios para su evaluación, corrección y mejora.

- Generar una política de transferencia de conocimiento entre los técnicos. Hacerla cumplir y evaluarla periódicamente para tener un mejoramiento continuo
- Preparar planes de simulacro de fallos de sistemas, evaluar la calidad de los respaldos, definir procedimientos para responder en caso de un evento de desastre.
- Para minimizar las vulnerabilidades y amenazas de los activos del departamento de sistemas es de alta prioridad que se elabore el plan de contingencia, dentro del cual debe incluir un sitio alterno para proteger toda la información contenida en los laboratorios de computación de la unidad educativa.

Bibliografía

Abarca, A., Alpízar, F., Sibaja, G. & Rojas, C. (2013). Técnicas cualitativas de investigación. Universidad de Costa Rica, 1-344. Recuperado de: http://www.editorial.ucr.ac.cr/ciencias-sociales/item/2268-tecnicas-cualitativas-de-investigacion.html

Abolacio Bosch, M. (2018). *Planificación de la auditoría. ADGD0108.* IC. Editorial.

Aguilar, M. (2017). *site*. Obtenido de Metodología de la investigación-Muestra: Recuperado de: https://sites.google.com/site/metodologiadeinvestigaciontese/mestra

Alvarado Zabala, J., Pacheco Guzmán, J., & Martillo Alchundia, I. (2018). El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT. *Revista Contribuciones a las Ciencias Sociales*. Recuperado de: https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html

Alvira, J. O. (2021). *Estrategias complementarias para mejorar la seguridad informática y de la información en la compañía qwerty s.a. utilizando la norma iso 27001.* Universidad Nacional Abierta y A Distancia UNAD, La Plata Huila. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/47673/jotrujilloa.pdf?sequence=3&isAllowed=y

Aponte Cisneros, G., & Cuenca Tapia, J. P. (2021). Modelo de gestión de TI para el Gobierno Autónomo Descentralizado Municipal del Cantón Huaquillas. *Dominios de las Ciencias, 7*(6), 1078-1098. doi: http://dx.doi.org/10.23857/dc.v7i6.2382

Arcentales Fernández, D. & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias*, 3, 157-173.

Atilio de la Orden, E. (2020). Conceptos de ecología y población. *Editorial Científica Universitaria*, 4-5. Recuperado de: https://www.ine.cl/ine-ciudadano/definiciones-estadisticas/poblacion/que-es-poblacion

Avila Torres, R. A., & Cuenca Tapia, J. P. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. *Dominio de las Ciencias, 7*(4), 363-376. doi: http://dx.doi.org/10.23857/dc.v7i4.2425

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Grupo Editorial Patria.

Bravo, D. M., & Giler, J. F. (2021). *Auditoría informática interna de los módulos de matriculación y notas del sistema de gestión académica de la ESPAM MFL.* Escuela Superior Politécnica Agropecuaria de Manabí, Ecuador. Recuperado de https://repositorio.espam.edu.ec/bitstream/42000/1566/1/TTC13D.pdf

Brito, J. & Stagno, G. (2010). *La (des) igualdad social y cultural en la escuela: reflexiones en torno a una compleja tensión*. Clase 17 perteneciente a la Diplomatura Superior en Currículum y Prácticas escolares en Contexto. Buenos. Aires. FLACSO virtual, Argentina.

Brys, C. (2013). *Introducción a la informática* (edición 2013 ed.). Misiones. Argentina. . Recuperado de http://190.57.147.202:90/jspui/bitstream/123456789/432/1/Introduccion-a-la-Informatica.pdf

Cáceres, A. B. (2021). *Implementación de un sistema informático para el restaurante turístico "Los Claveles" Pariacoto – Huaraz.* Universidad Católica los Ángeles Chimbote. Recuperado de http://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/22980/INFORMATICA_PROCESOS_ESPINOZA_CACERES_ANGIE_BERTH.pdf?sequence=1&isAllowed=y

Charres, H., Villalaz, J. & Martínez, J. A. (2018). Triangulación: Una herramienta adecuada para las investigaciones en las ciencias administrativas y contables. *FAECO sapiens*, 1(1), 1-9. Recuperado de: http://portal.amelica.org/ameli/jatsRepo/221/2211026002/index.html

Chuquín, D. J. (2020). *Implementación de la normativa internacional pci-dss, para la seguridad de cajeros automáticos de la cartera de clientes de la empresa greenetics soluciones S.A.* (Trabajo de Ingeniero en Sistemas Computacionales), Universidad Técnica del Norte, Ibarra.

De Santiago Bartolomé, I. (2019). *Análisis de magerit y pilar*. (Tesis de Ingeniería de Organización Industrial). Universidad de Valladolid, España.

Derrien, Y. (2009). *Técnicas de la auditoría informática.* Marcombo.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.Libro III - Guía de Técnicas.* Madrid: ed. Ministerio de Hacienda y Administraciones Públicas. Recuperado de: http://administracionelectronica.gob.es/

Fernández, D. A., & Casas, X. C. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias, III*(3), 157-173. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Ferro Veiga, J. M. (2020). Bullying o acoso escolar. La respuesta juridico-legal-2 EDI. Alcala Grupo Editorial. Recuperado de: https://www.lavanguardia.com/libros/libro/bullying-o-acoso-escolar-la-respuesta-juridico-legal-2-edi-9788413239408

Flores, J., Guarda, T., & Molina, L. (2019). Seguridad informática en el uso de los nuevos equipos tecnológicos. *Ibérica de Sistemas e Tecnologias de Informação*, (E17), 32–38. Recuperado de: https://www.proquest.com/openview/77d7d0f4e35e4177e0ca7913fa8f2300/1?pq-origsite=gscholar&cbl=1006393

González Retamozo, J. E. (2017). *Auditoría de seguridad informática para la institución educativa departamental Luis Carlos Galán - municipio de Yacopí Cundinamarca*. (Tesis de Especialista en Seguridad Informática). Universidad Nacional Abierta y A Distancia. Colombia.

Hérnandez León, R., & Coello Gonzalez, S. (2008). *El paradigma cuantitativo de la investigacion cientifica.* Universitaria.

Hernández, R. & Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana Editores, S.A. de C. V.

ISOTools Excellence. (2015). *Seguridad de la Información* . Obtenido de ISO 27001: El método MAGERIT: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Iturralde Heredia, A. Y. (2018). *Auditoría informática de la seguridad física y lógica de la biblioteca de la Universidad Técnica de Machala*. (Tesis de Mestria). Universidad Técnica de Machala. Ecuador.

Jiménez Ortega, M., & Benavides Rojas, M. (2012). *Auditoría de control interno I*. Universidad Técnica Particular de Loja. Ecuador.

Juárez Martínez, G. (2016). La propuesta de investigación. *Atlante*, 3.

Martínez, Y. A., Alfonso, B. B., & Marichal, L. L. (2012). Auditoría con Informática a Sistemas Contables. *Arquitectura e Ingeniería, VI*, 1-14. Recuperado de http://www.redalyc.org/articulo.oa?id=193924743004

Morales Gortárez, F. J. (octubre 2019). Tecnología de la información como herramienta de la auditoría. *Contaduría pública*, 1-7. Recuperado de: https://contaduriapublica.org.mx/2019/10/01/tecnologia-de-la-informacion-como-herramienta-de-la-Auditoría/

Morán Flores, C. (2019). *Mantenimiento de equipos informáticos.* Morán Flores, C. (2019). Mantenimiento de equipos informáticos. Ministerio de Educación y Formación Profesional de España.

Morán, L. F., Navarrete, D. S., Cruzatty, J. E., Anzúles, G. R., Mero, C. J., Quimiz, Á. L., & Merino, M. A. (Octubre 2018). *Introducción a la seguridad informática y el análisis a las vulnerabilidades* (Primera edición ed.). Manabí, Ecuador: 3 Ciencias. Recuperado de https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=Herramientas+para+evaluaci%C3%B3n+de+vulnerabilidades+en+equipos+inform%C3%A1ticos&ots=ymvUwYe1Nq&sig=N6yy5GRpiiTjX-vqKiFNs30vST8#v=onepage&q=Herramientas%20para%20evaluaci%C3%B3n%2

Negrín Sosa, E., López García, L., Rodriguez Cabrera, K., & Martinez Guerra, D. (2017). Propuesta de un programa de auditoría a los sistemas de información. *ECA Sinergia*, 135.

NORMA ISO 27001. (2020). Obtenido de NORMA ISO 27001: https://normaiso27001.es/a9-control-de-acceso/#

Ortiz, D. A., & Ayala, J. C. (2019). *Estado del Arte de la Auditoría Informática y su importancia para las empresas.* Universidad Nacional de Piura. Perú. Recuperado de https://repositorio.unp.edu.pe/bitstream/handle/UNP/1971/FCC-JIM-ORT-2019.pdf?sequence=1&isAllowed=y

Otero Escobar, A. D. (2020). El desarrollo de competencias profesionales en el área de Auditoría Informática a través del aprendizaje móvil. *Interconectando Saberes*, 5(10), 19-29. Recuperado de: https://doi.org/10.25009/is.v0i10.2658

Otzen, T. & Manterola, C. (2017). Técnicas de muestreo sobre una población a estudio. *International Journal of Morphology*, 35(1), 227-232. https://dx.doi.org/10.4067/S0717-95022017000100037

Palacios, L. A., Tineo, D. A., Pozo, J. C., & Jimenez, B. A. (2022). *Sistema web utilizando la metodología scrum para mejorar la gestión de los equipos informáticos en la institución educativa 14053-Cucungara de Cura Mori.* Universidad Nacional de

Piura. Perú. Recuperado de https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/3500/INFO-COR-GUE-MER-SIR-2022.pdf?sequence=1&isAllowed=y

Párraga, A. C., & Castillo, V. A. (2014). *Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la ESPAM MFL.* Escuela Superior Politécnica Agropecuaria de Manabí. Ecuador. Recuperado de http://190.15.136.145/bitstream/42000/72/1/TESIS%20AMARILIS%20CAROLINA%20LOOR%20P%c3%81RRAGA%20-%20VER%c3%93NICA%20ALEXANDRA%20ESPINOZA%20CASTILLO.pdf

Piattini, M., Del Peso, E. & Del Peso, M. (2008). *Auditoría de tecnologías y sistemas de información*. 4ed. Madrid, ES. RA-MAl. 1378. 1-67.

Pincay, J. M. (2021). *Diseño de un plan informático para mejorar la gestión operativa de los equipos informáticos en el laboratorio móvil de la carrera de ingeniería en computación y redes.* Universidad Estatal del Sur de Manabí, Ecuador. Recuperado de http://repositorio.unesum.edu.ec/bitstream/53000/3038/1/MARCILLO%20PINCAY%20JUAN%20MARTIN%20.pdf

Rodriguez Jimenez, A., & Pérez Jacinto, A. (2017). Métodos científicos de indagación y de contruccion de conocimiento. R*evista EAN*, 10.

Rodriguez, L. A. (2018). *Diseño de un plan de soporte técnico para el mantenimiento preventivo y correctivo de los equipos computacionales de la sala de cómputo #14 de la carrera de ingeniería en computación y redes.* Universidad Estatal del Sur de Manabí, Ecuador. Recuperado de http://repositorio.unesum.edu.ec/bitstream/53000/1489/1/UNESUM-ECU-REDES-2017-21.pdf

Rodríguez, V. K. (2012). *Auditoría informatica a la superintendencia de telecomunicaciones.* Universidad de Cuenca. Recuperado de http://dspace.ucuenca.edu.ec/bitstream/123456789/652/1/ts205.pdf

Salgado Soto, M. O. (2017). La auditoría informática en las organizaciones. *Electrónica sobre cuerpos académicos y grupos de investigación en iberoamérica, IV*(8). Recuperado de: http://www.cagi.org.mx/index.php/CAGI/article/view/165/324

Sandoval Morales, H. (2012). *Introducción a la auditoría*. México: RED TERCER MILENIO S.C.

Santana, J. K. (2018). La importancia de los desarrollos informáticos en los procesos administrativos. *Polo del Conocimiento, III*(1), 24-35. Recuperado de https://polodelconocimiento.com/ojs/index.php/es/article/viewFile/378/450

Solano Javier, O., & Riascos Erazo, S. C. (2021). *Sistema de información contable en la era digital: Marco de referencia para su administración y control.* Universidad del Valle.

Solarte, F. N., & Rosero, E. R. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE, 28* (5), 492-507. Recuperado de http://200.10.147.88/index.php/tecnologica/article/view/456

Sunkel, G., Trucco, D. & Espejo, A. (2016). *La integración de las tecnologías digitales en las escuelas de América Latina y el Caribe. Una mirada multidimensional*. Red de Desarrollo Social de América Latina y el Caribe. CEPAL, Chile. Recuperdo de: https://dds.cepal.org/redesoc/publicacion?id=2759

Tobar, R. A., & Ordoñez, A. F. (2015). *Estudio para la implementacion del sistema de gestion de seguridad de la informacion para la secretaria de educacion departamental de nariño basado en la NORMA ISO/IEC 27001.* (Trabajo de Especialista en Seguridad Informática), Universidad Nacional Abierta y A Distancia – UNAD.

Trujillo, S. E., Merlos, J. C., Gallegos, M. S., & Conzuelo, L. L. (2020). Las metodologías de la auditoría informática y su relación con buenas prácticas y estándares. *Ideas en Ciencias de la Ingeniería, 1*(1). Recuperado de https://ideasencienciasingenieria.uaemex.mx/article/view/14591/10992

Uriña, S. M., & Crespo, J. R. (2022). *Auditoría informática de las vulnerabilidades de seguridad en la red inalámbrica de la empresa punto de vista con las herramientas Acrylic Wi-Fi y Openvas utilizando la metodología de evaluación de seguridad wireless abierta (OWISAM).".* Universidad de Guayaquil,. Obtenido de http://repositorio.ug.edu.ec/handle/redug/59764

Valencia, G. & Orozco, K. (2017). Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. *Ibérica de Sistemas e Tecnologias de Informação,* (22), 73-88. Recuperado

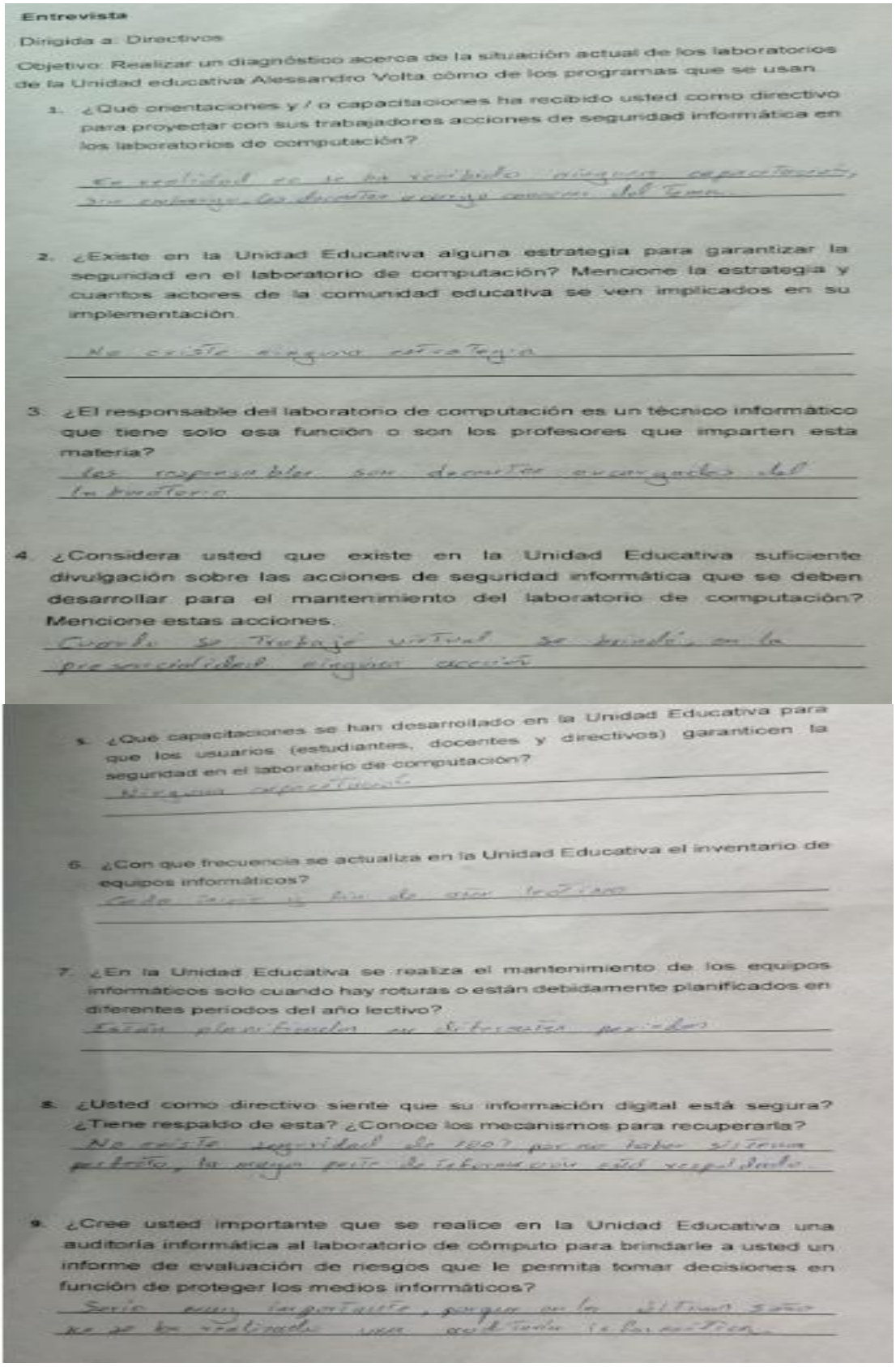
de: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006

Yangua, B. (2014). *Auditoría informática y su incidencia en los riesgos para el manejo de la información en la cooperativa de ahorro y crédito educadores de Tungurahua. Ambato*. (Tesis de Maestría en Contabilidad). Universidad Técnica de Ambato.

Zambrano, R. C. (2020). *Plan de implementación de la normativa PCI-DSS en la cooperativa de ahorros y crédito La Benéfica.* Master Universitario en Seguridad Informática, Universidad Internacional de la Rioja (UNIR), El Carmen. Ecuador.

Anexos

Anexo 1. Entrevista



Entrevista

Dirigida a: Directivos

Objetivo: Realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad educativa Alessandro Volta cómo de los programas que se usan

1. ¿Qué orientaciones y / o capacitaciones ha recibido usted como directivo para proyectar con sus trabajadores acciones de seguridad informática en los laboratorios de computación?

   En realidad no se ha recibido ninguna capacitación, sin embargo los docentes encargados del tema.

2. ¿Existe en la Unidad Educativa alguna estrategia para garantizar la seguridad en el laboratorio de computación? Mencione la estrategia y cuantos actores de la comunidad educativa se ven implicados en su implementación.

   No existe ninguna estrategia

3. ¿El responsable del laboratorio de computación es un técnico informático que tiene solo esa función o son los profesores que imparten esta materia?

   los responsables son docentes encargados del laboratorio

4. ¿Considera usted que existe en la Unidad Educativa suficiente divulgación sobre las acciones de seguridad informática que se deben desarrollar para el mantenimiento del laboratorio de computación? Mencione estas acciones.

   Cuando se trabaja virtual se brinda en la presencialidad ninguna acción

5. ¿Qué capacitaciones se han desarrollado en la Unidad Educativa para que los usuarios (estudiantes, docentes y directivos) garanticen la seguridad en el laboratorio de computación?

   Ninguna capacitación

6. ¿Con que frecuencia se actualiza en la Unidad Educativa el inventario de equipos informáticos?

   Cada cierto tiempo de acuerdo a los daños

7. ¿En la Unidad Educativa se realiza el mantenimiento de los equipos informáticos solo cuando hay roturas o están debidamente planificados en diferentes periodos del año lectivo?

   Están planificados en diferentes periodos

8. ¿Usted como directivo siente que su información digital está segura? ¿Tiene respaldo de esta? ¿Conoce los mecanismos para recuperarla?

   No existe seguridad del 100% por no tener sistema perfecto, la mayor parte de información esta respaldada.

9. ¿Cree usted importante que se realice en la Unidad Educativa una auditoría informática al laboratorio de cómputo para brindarle a usted un informe de evaluación de riesgos que le permita tomar decisiones en función de proteger los medios informáticos?

   Sería muy importante, porque en la actualidad todo se debe realizar una auditoría informática.

Anexo 2. Encuesta

Encuesta

Dirigida a: Estudiantes y profesores

Objetivo: Realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad educativa Alessandro Volta cómo de los programas que se usan.

Cuestionario de preguntas de la encuesta

1. Seleccione su categoría.
   ____Profesor
   ___/ Estudiante
2. En el laboratorio de computación existen horarios definidos para la atención a usuarios.
   ___ Nunca ___ Casi Nunca ___ A veces ___/ Casi siempre ___ Siempre ___
3. ¿Se realizan con frecuencia mantenimientos a los equipos informáticos del laboratorio de computación?
   ___ Nunca ___ Casi nunca ___/ A veces ___ Casi siempre ___ Siempre ___
4. Con frecuencia el responsable del laboratorio comprueba que los equipos procesen la información de forma adecuada.
   ___ Nunca ___/ Casi nunca ___ A veces ___ Casi siempre ___ Siempre ___
5. ¿En el laboratorio es obligatorio identificarse con usuario y clave para acceder al sistema?
   ___ Nunca ___ Casi siempre___ A veces ___ Casi siempre ___ Siempre ___/
6. ¿Al crear su usuario y contraseña el sistema le informa la longitud mínima y los caracteres que debe contener una contraseña?
   ___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___/ Siempre ___
7. ¿Está definido el período de caducidad de la contraseña?
   ___/ Si ___ (No)
8. ¿Cuándo usted accede al laboratorio el responsable le hace firmar en una lista de control de acceso?
   ___/ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

9. ¿Existen en el laboratorio etiquetas de seguridad que le orientan como debe ser su comportamiento en el laboratorio y el cuidado que debe dar a los equipos informáticos?
   ___Si ___/ No
10. ¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el laboratorio de computación?
    ___ Si ___/ No
11. ¿Se ha definido e informado a usted cuales son las sanciones de los usuarios por infringir las normas?
    ___/ Si ___ No
12. ¿Los equipos de laboratorio están conectados en red?
    ___/ Si ___ No
13. ¿Existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica?
    ___/ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___
14. ¿Se ha definido la forma de acceso a recursos compartidos?
    ___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___/ Siempre ___
15. ¿En el laboratorio se han instalado antivirus en los servidores?
    ___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___/
16. ¿Se han habilitado las actualizaciones del antivirus?
    ___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___/
17. ¿A usted como usuario se le ha informado el proceso adecuado para realizar el respaldo y recuperación de información?
    ___ Nunca ___ Casi Nunca ___ A veces___/ Casi siempre ___ Siempre ___
18. ¿En el laboratorio se han bloqueado puertos USD y la grabadora de CD/DVD para la protección de los medios informáticos?
    ___ Nunca ___ Casi Nunca ___ A veces___ Casi siempre ___ Siempre ___

Organización de las preguntas por aspectos evaluados para la tabulación de los datos.

Categoría de los encuestados

____Profesor ____ Estudiante

No. Preg	Aspectos Evaluados	Pregunta	Escala para evaluación
2	Control de acceso a las aplicaciones y la información	¿En el laboratorio de computación existen horarios definidos para la atención a usuarios?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
3	Procedimientos y responsabilidades de operación	¿Se realizan con frecuencia mantenimientos a los equipos informáticos del laboratorio de computación?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
4	Procedimientos y responsabilidades de operación	Con frecuencia el responsable del laboratorio comprueba que los equipos procesen la información de forma adecuada.	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
5	Control de acceso a las aplicaciones y la información	¿En el laboratorio es obligatorio identificarse con usuario y clave para acceder al sistema?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
6	Control de acceso al sistema operativo	¿Al crear su usuario y contraseña el sistema le informa la longitud mínima y los caracteres que debe contener una contraseña?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
7	Control de acceso al sistema operativo	¿Está definido el período de caducidad de la contraseña?	____ Si ___ No
8	Control de acceso al sistema operativo	¿Cuándo usted accede al laboratorio el responsable le hace firmar en una lista de control de acceso?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
9	Control de acceso al sistema operativo	¿Existen en el laboratorio etiquetas de seguridad que le orientan como debe ser su comportamiento en el laboratorio y el cuidado que debe dar a los equipos informáticos?	___ Si ___ No
10	Responsabilidades de usuarios con la seguridad	¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el laboratorio de computación?	___ Si ___ No

11	Responsabilidades de usuarios con la seguridad	¿Se ha definido e informado a usted cuales son las sanciones de los usuarios por infringir las normas?	___ Si ___ No
12	Control de acceso a la red	¿Los equipos de laboratorio están conectados en red?	___ Si ___ No
13	Control de acceso a la red	¿Existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
14	Control de acceso a la red	¿Se ha definido la forma de acceso a recursos compartidos?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
15	Protección contra software malicioso	¿En el laboratorio se han instalado antivirus en los servidores?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
16	Protección contra software malicioso	¿Se han habilitado las actualizaciones del antivirus?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
17	Gestión del respaldo y recuperación	¿A usted como usuario se le ha informado el proceso adecuado para realizar el respaldo y recuperación de información?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre
18	Seguridad en la utilización de medios informáticos	¿En el laboratorio se han bloqueado puertos USD y la grabadora de CD/DVD para la protección de los medios informáticos?	___ Nunca ___ Casi Nunca ___ A veces ___ Casi siempre ___ Siempre

Fuente: Elaboración propia

Anexo 3. Imágenes de evidencias de la aplicación de los instrumentos de entrevista y encuesta a la muestra seleccionadas

Imágenes 1. Aplicación de instrumento al Rector

Imágenes 2. Instrumentos a muestra seleccionada

Anexo 4. Ficha de verificación

Ficha de verificación

Objetivo: Recolectar información mediante la observación para el análisis de riesgos de los equipos informáticos que se encuentran dentro de la "Unidad Educativa Alessandro Volta".

Instrucciones: Marcar para cada caso solo una opción de impacto y una de probabilidad.

Importancia del riesgo: 1,2,3,4. Probabilidad de ocurrencia: 1,2,3.

El parámetro estabilidad de la red se evalúa tomando la información observada con la herramienta en línea **Speddtest.net.**

Escala de evaluación:

Impacto del riesgo: Muy bajo (MB, 1); Bajo (B, 2); Medio (M, 3); Alto (A, 4); Muy Alto (MA, 5)

Probabilidad de ocurrencia: Muy raro (MB,1); Poco probable (B,2) Posible (M,3); Probable(A,4); Prácticamente seguro (MA,5).

			Impacto					Probabilidad				
			1 Muy bajo	2 Bajo	3 Medio	4 Alto	5 Muy Alto	1 Muy raro	2 Poco probable	3 Posible	4 Probable	5 Prácticamente seguro
Nº	Parámetros generales	Preguntas										
1	Gestión y control del equipamiento tecnológico	En los laboratorios algunas computadoras ya no son funcionales y no han sido remplazadas.										
2		Los periféricos de las computadoras existentes en la unidad educativa no funcionan en su totalidad.										
		Es inadecuada la ubicación de las computadoras con relación al espacio físico de los laboratorios.										
		El número de computadoras en los laboratorios no es suficiente para la cantidad de usuarios.										
		El inventario del equipamiento tecnológico de la Unidad Educativa está desactualizado.										
Estimación de riesgo general												
6	Procedimientos y responsabilidades de operación	Los mantenimientos a los equipos informáticos no son frecuentes.										
7		El responsable de los equipos informáticos no comprueba con frecuencia que los equipos procesen la información de forma adecuada. .										
8		Los equipos tecnológicos de la Unidad educativa permanecen sucios lo que denota falta de mantenimiento.										

8		Los equipos tecnológicos de la Unidad educativa permanecen sucios lo que denota falta de mantenimiento.												
		Existen computadoras con fallas sencillas y por falta de mantenimiento por lo que pueden quedar en desuso.												
9		Las fallas y roturas del equipamiento tecnológica de la Unidad Educativa no se registran por tanto no se les da seguimiento.												
Estimación de riesgo general														
9	Seguridad en la utilización de medios informáticos	Los medios informáticos están desprotegidos pues no se han bloqueado puertos USD y la grabadora de CD/DVD.												
10		Las sanciones que pueden recibir los usuarios por infringir las normas de seguridad de los equipos informáticos no se encuentran publicadas.												
		Los usuarios desconocen cuáles son sus responsabilidades para garantizar la seguridad en los laboratorios de computación.												
11		En los laboratorios de computación no existe un registro para el control de entrada y salida de los usuarios.												
		Los horarios para la atención a usuarios en los laboratorios no están publicados.												
Estimación de riesgo general														
	Control de acceso al sistema operativo	La identificación previa no es necesaria para acceder al sistema operativo.												
		Nunca se inhabilita a los usuarios por superar el número de intentos de acceso fallidos.												
15		La caducidad de la contraseña no tiene un período definido.												
16		En los laboratorios no existe una lista de control para que el usuario firme antes de acceder al sistema operativo.												
17		Los programas y equipos personales se introducen sin inconveniente pues no existe una política de prohibición.												
18		No se observan etiquetas de seguridad que informen a los usuarios el comportamiento que se exige en el laboratorio y el cuidado que debe dar a los equipos informáticos.												
		En el laboratorio se han instalado antivirus pero no se han habilitado las actualizaciones.												
Estimación de riesgo general														

Fuente: Elaboración propia

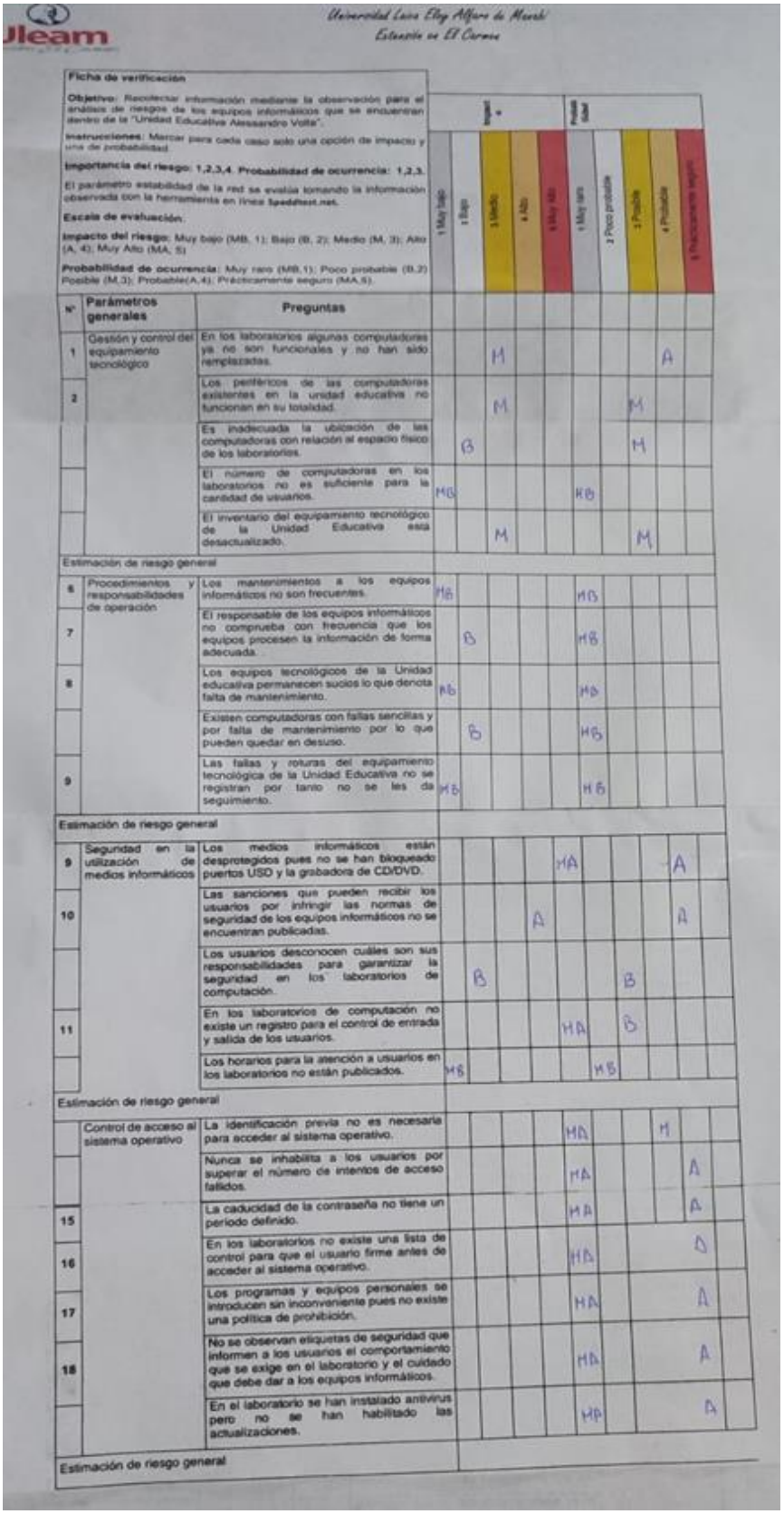
Anexo 5. Códigos de la ficha de verificación

Nº	Parámetros generales	Preguntas	Código
1	Gestión y control del equipamiento tecnológico.	En los laboratorios algunas computadoras ya no son funcionales y no han sido remplazadas.	GCET 1
2	**GCET**	Los periféricos de las computadoras existentes en la unidad educativa no funcionan en su totalidad.	GCET 2
3		Es inadecuada la ubicación de las computadoras con relación al espacio físico de los laboratorios.	GCET 3
4		El número de computadoras en los laboratorios no es suficiente para la cantidad de usuarios.	GCET 4
5		El inventario del equipamiento tecnológico de la Unidad Educativa está desactualizado.	GCET 5
6	Procedimientos y responsabilidades de operación. PRDO	Los mantenimientos a los equipos informáticos no son frecuentes.	PRDO 1
7		El responsable de los equipos informáticos no comprueba con frecuencia que los equipos procesen la información de forma adecuada. .	PRDO 2
8		Los equipos tecnológicos de la Unidad educativa permanecen sucios lo que denota falta de mantenimiento.	PRDO 3
9		Existen computadoras con fallas sencillas y por falta de mantenimiento por lo que pueden quedar en desuso.	PRDO 4
10		Las fallas y roturas del equipamiento tecnológica de la Unidad Educativa no se registran por tanto no se les da seguimiento.	PRDO 5

11	Seguridad en la utilización de medios informáticos SMI	Los medios informáticos están desprotegidos pues no se han bloqueado puertos USD y la grabadora de CD/DVD.	SMI 1
12		Las sanciones que pueden recibir los usuarios por infringir las normas de seguridad de los equipos informáticos no se encuentran publicadas.	SMI 2
13		Los usuarios desconocen cuáles son sus responsabilidades para garantizar la seguridad en los laboratorios de computación.	SMI 3
14		En los laboratorios de computación no existe un registro para el control de entrada y salida de los usuarios.	SMI 4
15		Los horarios para la atención a usuarios en los laboratorios no están publicados.	SMI 5
16	Control de acceso al sistema operativo CSO	La identificación previa no es necesaria para acceder al sistema operativo.	CSO 1
17		Nunca se inhabilita a los usuarios por superar el número de intentos de acceso fallidos.	CSO 2
18		La caducidad de la contraseña no tiene un período definido.	CSO 3
19		En los laboratorios no existe una lista de control para que el usuario firme antes de acceder al sistema operativo.	CSO 4
20		Los programas y equipos personales se introducen sin inconveniente pues no existe una política de prohibición.	CSO 5
21		No se observan etiquetas de seguridad que informen a los usuarios el comportamiento que se exige en el laboratorio y el cuidado que debe dar a los equipos informáticos.	CSO 6
22		En el laboratorio se han instalado antivirus pero no se han habilitado las actualizaciones.	CSO 7

Fuente: Elaboración propia

Anexo 6. Resultados de la ficha de verificación



Universidad Laica Eloy Alfaro de Manabí
Extensión en El Carmen

Ficha de verificación

Objetivo: Recolectar información mediante la observación para el análisis de riesgos de los equipos informáticos que se encuentran dentro de la "Unidad Educativa Alessandro Volta".

Instrucciones: Marcar para cada caso solo una opción de impacto y una de probabilidad.

Importancia del riesgo: 1,2,3,4. Probabilidad de ocurrencia: 1,2,3.

El parámetro estabilidad de la red se evalúa tomando la información observada con la herramienta en línea **Speedtest.net.**

Escala de evaluación:

Impacto del riesgo: Muy bajo (MB, 1); Bajo (B, 2); Medio (M, 3); Alto (A, 4); Muy Alto (MA, 5)

Probabilidad de ocurrencia: Muy raro (MB,1); Poco probable (B,2) Posible (M,3); Probable(A,4); Prácticamente seguro (MA,5).

Impacto: 1 Muy bajo | 2 Bajo | 3 Medio | 4 Alto | 5 Muy Alto

Probabilidad: 1 Muy raro | 2 Poco probable | 3 Posible | 4 Probable | 5 Prácticamente seguro

Nº	Parámetros generales	Preguntas	Impacto	Probabilidad
1	Gestión y control del equipamiento tecnológico	En los laboratorios algunas computadoras ya no son funcionales y no han sido remplazadas.	M	A
2		Los periféricos de las computadoras existentes en la unidad educativa no funcionan en su totalidad.	M	M
		Es inadecuada la ubicación de las computadoras con relación al espacio físico de los laboratorios.	B	M
		El número de computadoras en los laboratorios no es suficiente para la cantidad de usuarios.	MB	MB
		El inventario del equipamiento tecnológico de la Unidad Educativa esta desactualizado.	M	M
Estimación de riesgo general				
6	Procedimientos y responsabilidades de operación	Los mantenimientos a los equipos informáticos no son frecuentes.	MB	MB
7		El responsable de los equipos informáticos no comprueba con frecuencia que los equipos procesen la información de forma adecuada.	B	MB
8		Los equipos tecnológicos de la Unidad educativa permanecen sucios lo que denota falta de mantenimiento.	MB	MB
		Existen computadoras con fallas sencillas y por falta de mantenimiento por lo que pueden quedar en desuso.	B	MB
9		Las fallas y roturas del equipamiento tecnológica de la Unidad Educativa no se registran por tanto no se les da seguimiento.	MB	MB
Estimación de riesgo general				
9	Seguridad en la utilización de medios informáticos	Los medios informáticos están desprotegidos pues no se han bloqueado puertos USD y la grabadora de CD/DVD.	MA	A
10		Las sanciones que pueden recibir los usuarios por infringir las normas de seguridad de los equipos informáticos no se encuentran publicadas.	A	A
		Los usuarios desconocen cuáles son sus responsabilidades para garantizar la seguridad en los laboratorios de computación.	B	B
11		En los laboratorios de computación no existe un registro para el control de entrada y salida de los usuarios.	MA	B
		Los horarios para la atención a usuarios en los laboratorios no están publicados.	MB	MB
Estimación de riesgo general				
	Control de acceso al sistema operativo	La identificación previa no es necesaria para acceder al sistema operativo.	MA	M
		Nunca se inhabilita a los usuarios por superar el número de intentos de acceso fallidos.	MA	A
15		La caducidad de la contraseña no tiene un periodo definido.	MA	A
16		En los laboratorios no existe una lista de control para que el usuario firme antes de acceder al sistema operativo.	MA	A
17		Los programas y equipos personales se introducen sin inconveniente pues no existe una política de prohibición.	MA	A
18		No se observan etiquetas de seguridad que informen a los usuarios el comportamiento que se exige en el laboratorio y el cuidado que debe dar a los equipos informáticos.	MA	A
		En el laboratorio se han instalado antivirus pero no se han habilitado las actualizaciones.	MA	A
Estimación de riesgo general				

Glosario de términos

IP: La dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

MAGERIT: El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos).

WiFi: es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Los dispositivos habilitados con wifi, pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica.

Activo: Cualquier cosa que tenga valor para la organización.

Ataque: Cualquier acción deliberada con el objetivo de violar los mecanismos de seguridad de un sistema de información.

Auditoría de Seguridad: Estudio y examen independiente de registros históricos y actividades de un sistema de información con el objetivo de comprobar la solidez de los controles del sistema, alinear los controles con la estructura de seguridad y procedimientos operativos establecidos a fin de detectar brechas en la seguridad y recomendar modificaciones en los procedimientos, controles y estructuras de seguridad.

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a sus activos asociados.

Estado de riesgo: Caracterización de activos por riesgo residual. “Lo que puede pasar tomando en consideración que las salvaguardas han sido desplegadas”.

Evento de seguridad: Momento en que la amenaza existe y pone en riesgo activos, procedimientos o información. Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

Política. Toda intención y directriz expresada formalmente por la Dirección.

Riesgo. Combinación de la probabilidad de un evento y sus consecuencias.

Análisis de riesgos. Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Evaluación de riesgos. Todo proceso de análisis y valoración del riesgo.

Valoración del riesgo. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza.

Tratamiento del riesgo. Proceso de selección e implementación de medidas a para modificar el riesgo.

Vulnerabilidad: Cálculo o estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.