UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO DE INVESTIGACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA

AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA INFRAESTRUCTURA TECNOLÓGICA EN LA UNIDAD EDUCATIVA ANTONIO JOSÉ DE SUCRE EN EL PERIODO 2022.

AUTOR:

PALADINES CHUEZ LEONELA MICHELLE

TUTOR:

ING. CLARA GUADALUPE POZO HERNÁNDEZ MGS.

EL CARMEN, MARZO DEL 2023

CERTIFICACIÓN DEL TUTOR

CERTIFICACIÓN DEL TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 2
		Página 2 de 98

En calidad de docente tutor(a) 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 de la estudiante **PALADINES CHUEZ LEONELA MICHELLE**, legalmente matriculado/a en la carrera de Ingeniería en Sistemas, período académico 2022-2023, cumpliendo el total de 400 horas, bajo la opción de titulación de Proyecto Integrador, cuyo tema del es **"AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA INFRAESTRUCTURA TECNOLÓGICA EN LA UNIDAD EDUCATIVA ANTONIO JOSÉ DE SUCRE EN EL 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, 23 de enero de 2023.

Lo certifico.

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

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: "**Auditoría de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre en el Periodo 2022.**", corresponde exclusivamente a: Paladines Chuez Leonela Michelle con cédula de ciudadanía número 1313957324 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Leonela Michelle Paladines Chuez
C.C:1313957324

DEDICATORIA

Dedico mi tesis principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre, Alexandra Chuez Mendoza por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar cualquier obstáculo. A mi padre, Tomas Paladines Cevillano por siempre brindarme su amor y buenos consejos para que siga adelante por compartir momentos significativos conmigo y por siempre estar dispuesto a escucharme y apoyarme en cualquier momento. A mi hija Daenerys Rodríguez porque con ella siento que todo es más fácil y por ella eh salido adelante cuando eh tenido adversidades ella siempre ha estado ahí ha sido mi motor para culminar mis estudios. A mis hermanos por darme esas fuerzas para salir adelante. A mi esposo por haberme apoyado en cada momento de mi carrera con su amor y por siempre confiar en mí que si podía

AGRADECIMIENTO

A Dios, por acompañarme todos los días. A mi Mamá Alexandra Chuez quien más que una madre ha sido mi mejor amiga, me ha consentido y apoyado en lo que he propuesto y sobre todo ha sabido corregir mis errores. Agradezco también a mi padre Tomas Paladines Cevillano por ser mi apoyo en mi carrera profesional, en mis logros, en todo siendo mí pilar para salir adelante.

Expresar mi agradecimiento a mi Asesora de tesis Ing. Clarita Pozo por la dedicación y apoyo que ha brindado la oportunidad de recurrir a su capacidad y conocimiento en este trabajo, por el respeto de mis sugerencias e ideas y por la dirección y rigor que ha facilitado a las mismas. Así como también haberte tenido toda la paciencia del mundo para guiarme durante todo el desarrollo de la tesis. Gracias por la confianza ofrecida desde que llegue a esta universidad. Pero un trabajo de investigación es también fruto del reconocimiento y del apoyo vital que nos ofrecen las personas que nos estiman, sin el cual no tendríamos la fuerza y energía que nos anima a crecer como personas y como profesionales.

Gracias a mi familia, a mis padres, abuelos, a mis dos hermanos Dylan y Adael, en especial a mi hermano Jipson Paladines que me cuida desde el cielo y siempre será mi ángel guardián, porque con el compartí una infancia feliz, que guardo en el recuerdo y es un aliento para seguir escribiendo sobre la infancia.

Pero, sobre todo, gracias a mi esposo y a mi hija, por su paciencia, comprensión y solidaridad con este proyecto, por el tiempo que me han concedido, un tiempo robado a la historia familiar. Sin su apoyo este trabajo nunca se habría escrito y, por eso, este trabajo es también el suyo.

La Autora

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto de investigación es una auditoría de Seguridad informática para la infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre. El objetivo principal fue elaborar un informe de auditoría donde se evaluó y verifico el cumplimiento de normas de seguridad de la infraestructura tecnológica que posee la institución. Se realizó un diagnóstico en la institución para identificar el problema, las técnicas empleadas para la investigación fueron la encuesta y la entrevista siendo herramientas fundamentales para la recopilación de información, para esto se contó con la participación de 18 docentes que laboran en la institución y la máxima autoridad del plantel educativo el rector Ing. Luis Arteaga e Inspectora general la Lic. Mónica Andrea Mejía Guerrero. Mgs. La propuesta consistió en una auditoría de seguridad física al laboratorio de cómputo, la metodología que se usó fue MAGERIT, por medio de esta se pudieron realizar ciertos pasos con más facilidad como definir activos y amenazas, diseño de instrumentos, tabulación, análisis de riesgo y matriz de riesgos. Como resultados relevantes se obtuvo que el nivel de seguridad es de 43%, encontrando que las principales vulnerabilidades fueron exposición a: riesgo 1 de robo de información con un 95% de nivel de riesgo, riesgo 2 de virus con un 83% nivel altos, los demás riesgos fueron robo, incendio, daños de equipos, inundación sus resultados fueron muy bajos. Finalmente, se elaboró el informe de auditoría y una guía de recomendación que posee pasos a tomar en cuenta para prevenir dichos riesgos de seguridad informática.

SUMMARY

This research project is an audit of Computer Security for the technological infrastructure in the Antonio José de Sucre Educational Unit. The main objective was to prepare an audit report where compliance with security standards of the technological infrastructure owned by the institution was evaluated and verified. A diagnosis was made in the institution to identify the problem, the techniques used for the investigation were the survey and the interview, being fundamental tools for the collection of information, for this, 18 teachers who work in the institution and the highest authority of the educational establishment the rector Ing. Luis Arteaga and General Inspector Lic. Mónica Andrea Mejía Guerrero. Mgs. The proposal consisted of a physical security audit of the computer laboratory, the methodology used was MAGERIT, through which certain steps could be carried out more easily, such as defining assets and threats, instrument design, tabulation, analysis of risk and risk matrix. As relevant results, it was obtained that the security level is 43%, finding that the main vulnerabilities were exposure to: risk 1 of information theft with a 95% risk level, risk 2 of viruses with 83% high level, The other risks were theft, fire, equipment damage, and flooding. Their results were low. Finally, the audit report and a recommendation guide that has steps to take into account to prevent said computer security risks were prepared.

INTRODUCCIÓN

A través de la presente investigación se aborda temas de suma importancia en la auditoría de seguridad informática para la infraestructura tecnológica, actualmente el riesgo principal de la informática son los virus, donde tiende a propagarse por medio de los equipos de cómputo, la seguridad nos brindan las directrices y guía para manejar la información, que se manipula a nivel académico, a través de la auditoría informática se utilizan algunos factores que garantizan el desempeño y la utilización de seguridad en los equipos educativos, la gestión de riesgo esta nos permite analizar e identificar las posibles vulnerabilidades e inconvenientes, que se puedan producir al no adoptar un adecuado mantenimiento y cuidado de dichos dispositivos en la institución educativa.

En la actualidad podemos encontrar libros afines de la auditoría informática y seguridad informática como lo detalla Fernández (2016) que la auditoría informática son procesos que se realizan mediante técnicas que se debería llevar a cabo para mejorar los controles como políticas, procedimiento entre otros, en las empresas, organizaciones y establecimiento educativos, para poder identificar vulnerabilidades, amenazas y riesgos que se encuentran expuestos los dispositivos tecnológicos, a los posibles daños que se puedan suscitar. Por otra parte Chaos García et al. (2017) enfatiza sobre la infraestructura tecnológica y esto ha permitido grandes avances en todos los campos, las nuevas tecnologías están avanzando en actualidad y uno de los mayores retos que enfrentan en la inseguridad de la información que se manipulan mediante los dispositivos informáticos.

La auditoría de seguridad informática efectúa las tareas con eficacia y eficiencia, hace referencia sobre la seguridad informática fraccionando por parte diferente de la investigación, se enfoca en la mejora de la infraestructura y sus riesgos, el deterioro y comprobación de daños en la información, hace énfasis de los elementos que dispone el sistema con el pasar de los años la tecnología ha adquirido una gran importancia pues no tiene un límite en cuanto a crecimiento

y a las nuevas oportunidades que ofrecerá en diferentes campos, mientras se inventan herramientas de hardware y software que ayudan a mejorar y automatizar procesos en empresas e instituciones públicas y privadas se descuida un poco la inspección de estas, con el tiempo la tecnología se expone a riesgos causando fallas en los equipos que ocasionan reparaciones costosas o perdida de datos importantes para las instituciones, para ello es necesario evaluar para evitarlos y prevenirlos. El problema es que la unidad educativa no cuenta con un plan de riesgo para proteger sus activos que se encuentra en la infraestructura tecnológica como son los equipos informáticos.

En el capítulo uno resalta las definiciones acerca de todos los términos que se van a utilizar en la auditoria para tener una idea más clara de todo lo que conlleva a realizar una auditoria informática, de la misma manera el conocer información sobre infraestructura tecnológica se pudo despejar dudas acerca de cuáles son los equipos que conforman un centro informático.

En el capítulo dos profundiza el estudio de campo**,** el diseño y métodos de investigación en la cual se describe inductivo-deductivo y para fundamentar la información teórica se aplicó el método bibliográfico, las técnicas e instrumentos nos brindaron la recopilación de datos en una zona determinada para evaluar, esta se puede realizar por varios instrumentos como es la encuesta-cuestionario y entrevista-guía de entrevista en las cuales están involucrados la autoridad principal de la institución como es el Rector, inspectora y docentes de la Unidad Educativa Antonio José de Sucre.

En el tercer capítulo del trabajo de investigación presenta la propuesta de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre se empleó la metodología Magerit en donde nos brindan recursos informáticos, en la auditoría que se implementó dentro de una institución en cada uno de los activos definiendo las vulnerabilidades y amenazas en cada uno de los equipo tecnológicos para así poder concluir con los resultados obtenidos y detectados mediante la investigación propuesta en la organización como tal en la Unidad Educativa Antonio José de Sucre. Al final se

obtuvo que dentro de la infraestructura tecnológica los equipos se encontraban expuestos a virus, incendio, daños de equipos, inundación, robo de inundación, siendo su porcentaje total de seguridad del 43% y nivel de riesgo 57% y se elaboró un informe de auditoría por ende en la guía de recomendación se colocaron varios pasos a seguir para prevenir dichas vulnerabilidades.

CAPÍTULO I

MARCO TEÓRICO

2.1 Auditoría de seguridad Informática:

2.1.1 Definición de auditoría

Fernández (2016) define a la auditoría como un proceso necesario que siguen las organizaciones que utilizan para velar por sus intereses, esto a través de un documento que tenga recomendaciones que se deberían llevar acabo para mejorar los controles como políticas, procedimientos y controles que permiten una mejor operatividad dentro de una empresa, este se logra a través de un examen llevado a detalle por una o varias personas que verifiquen la realidad de la organización y así enfocar de manera eficiente el objetivo.

La auditoría es realizada por un auditor, una persona capacitada para dar una opinión independiente de una organización.

2.1.2 Tipos de auditoría:

Según Chicano tejada (2016) la clasificación de la auditoría es:

- **Auditoría de estados financieros:** El auditor en este campo observa estados financieros e informa si han sido realizados correctamente, además se asegura de que la empresa tenga una seguridad razonable para librarse de errores materiales debido a fraudes.
- **Auditoría fiscal:** En esta rama se verifica si el pago de impuestos a diferentes instituciones es correcto.
- **Auditoría interna:** Este tipo de auditoría ayuda a la organización al evaluar los procesos de gestión de riesgos, control y gobierno.
- **Auditoría externa:** Ayuda por medio de un examen de verificación a evaluar la conformidad o comportamiento de disposiciones legales o internas del control interno vigente.

- **Auditoría operacional:** Realiza un análisis de todas las operaciones de una entidad de forma analítica objetiva y sistemática de una empresa.
- **Auditoría administrativa:** Esta realiza un examen más completo y constructivo de una organización, departamento o entidad, así mismo monitorean sus métodos de control y operación.
- **Auditoría gubernamental:** En esta la autoridad vigila los recursos públicos de carácter económico, humano y material para su correcta administración.
- **Auditoría de calidad:** Esta es una de las más importantes pues forma parte de un elemento fundamental de las normas ISO 9001.
- **Auditoría de marketing:** Se enfoca en un análisis de entorno al mercadeo, así como estrategias y actividades de un negocio.
- **Auditoría ambiental:** Esta la realiza un auditor independiente y busca conocer el grado de satisfacción de la comunidad con su hábitat.
- **Auditoría de legalidad:** Este tipo de auditoría revisa que el desarrollo de las actividades se haya cumplido con las leyes, reglamentos o decretos que sean aplicables.
- **Auditoría forense:** Se enfoca en la revisión, prevención y detección de fraudes de tipo financiero

2.1.3 Auditoría informática

Es un proceso que a través de recoger, agrupar y evaluar evidencia para permitir asegurar los activos de una institución, algunas de las tareas que se ejecutan en una auditoría informática son la revisión de los sistemas a través de planes para implementar sistemas e implementarles mejoras, así como revisión de las instalaciones informáticas para revisar políticas y estándares de seguridad, así como creación de copias de seguridad y por último la revisión de aplicaciones al verificar si están en uso o si están actualizadas para evitar las vulnerabilidades. (Loor Venegas & Esparza Bernal, 2018)

Algunas de las áreas en que se ejecuta una auditoría son:

- Velar por la eficiencia de un sistema informático al corroborar la calidad para así proponer mejoras.
- Mantener las instalaciones en donde se almacenan los equipos informáticos.
- Vigilar accesos lógicos y gestión de privilegios.
- Controlar la seguridad física ante desastres naturales y físicos.

2.1.4 Tipos de auditoría en los sistemas de información:

Dentro de una auditoría informática se pueden encontrar diferentes tipos de sistemas de información, estos son:

- **Explotación:** Se encarga de revisar todos los resultados de listados informáticos.
- **Sistemas:** Este analiza toda actividad que tenga relación con los sistemas informáticos.
- **Comunicaciones y redes:** Este tipo de auditoría se encarga del análisis de las redes que se encuentran dentro de una organización.
- **Desarrollo de proyectos:** Por medio de esta auditoría se estudian las metodologías que se utilizan para el desarrollo de los proyectos que llevan la organización.

2.1.5 Seguridad Informática

La seguridad es aquella acción que siempre busca el prevenir riesgos a través de gestiones que permitan evitar situaciones de peligro, esto a través de métodos como el mitigar, transferir o aceptar un riesgo que se presente para un proyecto u organización, al elevar el nivel de seguridad en las áreas de trabajo se pueden prevenir desastres que comprometan a personas u objetos que están en ejecutando funciones dentro de las mismas. (Romero, et al. 2018)

Vale aclarar que muchas personas confunden seguridad de información con seguridad informática, para aclarar la primera solo busca la seguridad del bien informático, es decir se preocupa por su contenido, mientras que la seguridad

informática es el uso de los procesos o técnicas que se usan para poder transmitir o almacenar dicha información.

La seguridad informática se puede definir como el proceso que tiene por objetivo el diseñar, plantear y procesar normas o procedimientos que ayuden a proteger la información de la manipulación de datos ejecutada por personas que no estén autorizadas a ellos.

2.1.6 Importancia de la seguridad informática

En los últimos años se podido observar un gran crecimiento de las plataformas digitales, tanto para transacciones bancarias, como para almacenar información de uno o varios usuarios, aunque se crea que los archivos en dispositivos informáticos están seguros no siempre es así, ahí el porqué de la importancia de la seguridad informática en la actualidad, siempre que estas operaciones se efectúen hay cosas que pueden salir mal y esto puede causar perdida de información parcial o total, por medio de la seguridad informática se pueden recuperar estos archivos a través de planes de contingencia que involucran varios métodos efectivos que respalden esa pérdida de información, las empresas más grandes son las que tienen más cuidado con la seguridad informática por la enorme cantidad de datos que poseen a su disposición. (Urbina Baca, 2017)

2.1.7 Principios de seguridad

Para asegurar la protección de los activos se debe tener como prioridad el conocimiento de que el atacante explota las debilidades asociadas a todos los dispositivos que se tiene al alcance, la protección especial de la infraestructura requiere de medidas en base a recursos como instalaciones o equipos, con ellos se puede evaluar la importancia y probabilidad del impacto y las amenazas (Arroyo Guardeño et.al, 2020).

Para ello se tienen tres pilares fundamentales que detallan a continuación como funciona actualmente la seguridad.

2.1.7.1 *Los tres pilares de la seguridad:*

Estos pilares de seguridad son una parte fundamental en cuanto a la seguridad de la información, se basan en tener una prioridad máxima con los datos de las personas, para eso se sugieren tres principios que siempre se deben aplicar a un sistema informático, los cuales son la confidencialidad, integridad y disponibilidad.

Ilustración 1 LA TRIADA CID

2.1.7.2 *Confidencialidad:*

En este paso se debe asegurar que solo aquellas personas con las credenciales apropiadas pueden acceder a la información, esto puede funcionar según su rol en una organización, esta información puede ser de vital importancia y por ello es por lo que no debe caer en manos de cibercriminales (Urbina Baca, 2017).

Con esto se implementan diferentes recursos como:

- **Autenticación de usuarios:** Esto para verificar quien es la persona que accede a los datos.
- **Gestión de privilegios:** Los usuarios de un sistema solo ven la información que se autoriza, esto por su rol en la empresa.
- **Cifrado de la información:** Se transforma la información para que sea ilegible para usuarios ajenos a la misma, a través de un sistema de contraseña se puede extraer esa información para que pueda ser transmitida con total seguridad.

2.1.7.3 *Integridad:*

Aquí es cuando se debe cuidar que toda la información que se posea no sea comprometida de ninguna manera, en caso de que llegara a ocurrir que se está trabajando con información errónea puede alterar gravemente las operaciones de una empresa, para mantener la información que se tenga siempre integra es necesario seguir algunos pasos para que eso no ocurra. (Palacios Postigo, 2020)

Algunos de estos pasos son:

a) Monitorear el tráfico de red por si existen intrusiones
b) Auditar los sistemas para registrar cual es la función de esa información, quien la manipula, cuándo y cómo?
c) Implementar sistemas de control de cambios para verificar si algunos de los archivos han cambiado o no.
d) Crear copias de seguridad que permitan restablecer la información en caso de que esta se haya modificado o corrompido.

2.1.7.4 *Disponibilidad:*

En esta etapa se declara que toda la información que sea necesaria para realizar cualquier operación debe estar en perfecto estado para poder acceder a ella sin ningún problema, pues no serviría de nada contar con un ingreso seguro a través de confidencialidad y tener los datos sin ninguna corrupción si al final el acceso a la misma es tediosa o imposible, para ello toda la información debe estar disponible para quien la necesita, por lo general es una de las partes más afectadas en la seguridad, puesto a que muchas veces los ataques cibernéticos van enfocados a dejar a las personas sin acceso a los programas o páginas que quieran visitar (Lederkremer, 2020).

Por esta razón existen algunas políticas de control que se deben considerar al momento de dar disponibilidad a los datos:

- El acuerdo de nivel de servicio.

- Balanceadores de carga que ayuden a controlar el tráfico
- Copias de seguridad en caso de restauración

2.1.8 Autenticación

Se puede definir a la autenticación como el proceso que tiene por finalidad el verificar que algo es correcto o verdadero, esto al visualizar si un dato es correcto, esto puede ser aplicado a muchos campos como los sistemas, así como a dispositivos e inclusive a las personas. Dentro del mundo de la informática este proceso es algo recurrente pues la mayoría de personas suele guardar datos personales dentro de cuentas alojadas en nubes como correos electrónicos o redes sociales, mediante este método se pueden proteger aún más por el motivo en que no siempre las contraseñas de seguridad son 100% seguras, se pueden usar varios medios como características físicas para autenticar estos datos, como ejemplo tenemos voz, huellas dactilares, los ojos por medio del escáner de retina o inclusive la misma escritura gracias a patrones de dibujo. (Romero et al., 2018)

Aunque es verdad que autenticar los datos es necesario actualmente, es verdad que los costos para llegar a esto son algo elevados, pues se utilizan más en sistemas complejos, es importante pensar en el usuario, sin embargo, hay que analizar el costo vs beneficio que este servicio representa. En la actualidad existen dos tipos de autenticación a considerar:

- **Origen de datos:** Garantiza que los datos sean procedentes del sitio real, a través de categorías como contraseñas, tarjetas inteligentes, características físicas, conductas e inclusive por ubicación.
- **Autenticación por entidad par:** Garantiza que los datos que se intercambian sean directamente con la entidad adecuada, es decir que se demuestra que la persona es quien dice ser por medio de datos difíciles de obtener que solo la persona en si puede conocer.

2.1.9 Riesgos de seguridad informática

Según Arroyo Guardeño et.al (2020), los riegos y amenazas puedes aparecer a lo largo de todos los procesos que conlleven el almacenamiento y gestión de la información, por esa razón existe una lista en donde se pueden identificar cuáles son los riesgos más comunes y estos son:

- Comprometer la seguridad en las comunicaciones y gestión de datos
- Comprometer la seguridad de la provisión de servicio
- Falta de integración de políticas y técnicas de seguridad
- Defectos de autenticación y autorización mutuas
- Defectos en la auditoría de seguridad

2.1.10 Los virus informáticos

Se puede definir como virus informático a un programa de computadora que tiene como objetivo causar daño en un ordenador, teléfono o Tablet corrompiendo o borrando los archivos que están dentro de un disco solido o mecánico. Debido a que se crean y operan de manera clandestina es difícil encontrar el origen del primer virus creado, sin embargo, se conoce que las motivaciones no eran con el fin de dañar, sino más bien eran bromas para entretener, con el tiempo fueron evolucionando hasta convertirse en código malicioso para hurtar información. (Pardo Clemente, 2017)

Algunos de los antecedentes más comunes de virus informáticos son:

- **Programas conejo:** Estos son aquellos que se infiltran por medio de una red informática, se autocopian hasta llenar la memoria del equipo hasta bloquear el sistema.

- **Programas gusano:** Estos fueron creados por piratas informáticos, burlan la seguridad del sistema al descubrir las palabras clave por medio del intento y error hasta dar con las correctas para poder espiar archivos o alterar el sistema.

- **Bombas lógicas:** Estos programas son un poco más completos, además de infiltrarse en el sistema esperan un cierto tiempo, al activarse causaría fallos dentro del sistema, se usan más para extorsión del pirata con la finalidad de cobrar más por desactivar la bomba y así asegurar su pago.
- **Caballos de Troya:** Este es de los virus más comunes, pues con cada ejecución o tras un cierto tiempo borra información del equipo, aunque carece de formas para reproducirse a sí mismos para ser un verdadero peligro.

2.1.11 Riesgos de seguridad física

Como lo hace notar Urbina Baca (2017) Los equipos de cómputo necesitan de un constante mantenimiento y supervisión pues se encuentran expuestos a todo tipo de riesgos, dependiendo del entorno se pueden presentar diferentes problemas, destaca aquellos que se presentan con más frecuencia:

- Desastres naturales que pueden provocar daños como terremotos, lluvias intensas o incendios accidentales.

- Violación física al espacio donde se encuentran las computadoras, pues le da acceso al atacante a toda la información de la organización.

- Obsolescencia de los equipos que con el pasar el tiempo y la evolución de la tecnología deja que la información grabada sea irrecuperable.

2.1.12 Ingeniería social

2.1.12.1 *Los principios del ataque por ingeniería social*

El primero se basa en la conservación de la libertad de acción, para aquel que se dedica a la ingeniería social es de vital importancia el aprender a recuperar información que será usada posteriormente sin ser detectado, así es que debe aprender a permanecer invisible y usar sus tácticas para borrar u ocultar sus huellas. Luego tenemos el principio de unidad de mando, sin duda un elemento clave dentro de las operaciones pues se centra en las operaciones de equipo por medio de procesos de decisión claros, para eso existe una jerarquía sobre quien decide y quien da las órdenes. (ACISSI, 2018)

También está la economía de medios que tiene por objetivo el ahorrar la mayor cantidad de recursos al reutilizar formas de acción, para ellos se basa en factores de éxito y riesgos cambiantes, el siguiente es la investigación del efecto palanca y es la respuesta a los fallos humanos, al recopilar datos que no están tan ligados a la investigación pero que pueden ayudar a obtener una visión más clara del objetivo a futuro, por ultimo tenemos la adaptación al entorno, para esto los encargados de la ingeniería social usan diferentes métodos de comunicación como cartas, teléfonos, correos con el fin de sacar provecho de sus acciones y así ahorrar energía, además de ayudarlos a permanecer ocultos a la vista de los demás. (Lederkremer, 2020)

2.1.12.2 *Concepto de ingeniería social*

El arte de un ingeniero consiste en utilizar modelos y métodos a través de herramientas que le permita obtener resultados concretos dentro del mundo real, con ello se puede ver que al ingeniero social se lo llama comúnmente como estafador que se aprovecha de los usuarios al engañarlos para que entreguen datos confidenciales o infectar sus computadoras. Estas técnicas tienen un alto grado de efectividad y como herramienta principal se usa la comunicación con la persona para tratar de persuadirlo a entregar información valiosa como nombres, usuarios y contraseña. (Maillo Fernández, 2022)

2.1.12.3 *Ataque de ingeniería social*

A través de muchos estudios, empresas como Gartner establecieron un ciclo que determina los pasos que se siguen al momento de realizar un ataque de ingeniería social, estos son:

- **Recopilación de información:** Este paso es de vital importancia pues es aquí donde se debe buscar toda la información relacionada al objetivo para armar un pretexto que le permita al atacante acercarse al mismo.
- **Desarrollo de relaciones:** Después de haber analizado toda la información obtenida se debe planear el primer contacto con el objetivo, para esto se debe causar una muy buena primera impresión para facilitar las acciones futuras que se llevaran a cabo.
- **Explotación de las relaciones:** Esta fase por lo general lleva bastante tiempo porque se busca construir una relación de mayor confianza con la víctima, de esa forma al llegar el momento de obtener información clave no tenga motivos para sospechar del atacante.
- **Ejecución para lograr el objetivo:** Si se han cumplido los pasos anteriores con éxito se lograría el ataque perfecto, en el que la víctima nunca será consciente de que hizo algo malo, lo que deja una puerta abierta para nuevos ataques futuros en caso de necesitarlos.

2.1.13 Gestión de riesgos de seguridad informática

2.1.13.1 *Riesgos*

A través de la innovación de las tecnologías las empresas se han dedicado a mejorar todos sus servicios y procesos, por esa razón se han percatado que un medio para el éxito es controlar los riesgos a los que sus empleados u objetos están expuestos, por ello es que se implementan medidas de seguridad que ayuden a prevenir dichos riesgos potenciales, por ende se puede definir a la evaluación de riesgos como la función de desarrollar funciones que permitan proteger los recursos económicos, humanos y materiales porque estos le

permiten a la organización cumplir sus metas y objetivos. (Loor Venegas & Esparza Bernal, 2018).

2.1.13.2 *Vulnerabilidades y amenazas*

Las amenazas son aquellas funciones cuyo objetivo es dañar cualquier recurso o procedimiento de la institución, mientras que las vulnerabilidades son los propios fallos de seguridad que posee el sistema. Para el encargado de controlar las vulnerabilidades y amenazas del sistema de una organización es muy importante que tome en cuenta estos tres conceptos, puesto a que se debe considerar el riesgo, la probabilidad de la amenaza y cuál puede ser una vulnerabilidad que deba ser reforzada para aplicar las diferentes medidas correctivas y así prevenir que cualquier desastre como daño de los equipos a nivel de hardware como de software resulten catastróficos al nivel de perder la información. (Romero et al., 2018)

2.1.14 Metodologías de análisis de riesgo

Hasta la actualidad se han desarrollado una serie de normas ISO que están enfocadas en la administración de los riesgos, algunas de las más relevantes y conocidas a nivel mundial son:

ISO/IEC 27001: Con este se pueden especificar los requisitos necesarios para implantar o establecer un sistema de gestión de la seguridad de la información.

CRAMM: También conocida como metodología de manejo y evaluación de riesgos fue desarrollada por el Reino Unido, con ella se puede obtener una mejor visión de los riesgos a los que se enfrenta una organización al identificar los principales riesgos a los que se expone una entidad como desastres naturales, fallos de infraestructura o que vengan de parte del personal.

MAGERIT: Esta es la metodología de análisis y gestión de riesgos de los sistemas de información, se basa en la ISO 27001 y está muy relacionada con

los medios electrónicos e informáticos para minimizar riesgos con medidas de seguridad.

2.1.15 Fases de la metodología MAGERIT:

Para lograr un correcto desempeño de la metodología MAGERIT es necesario el seguimiento de ciertos pasos que permitan evaluar correctamente una empresa, tiene cinco pasos principales a seguir, Amutio Gómez (2017) menciona en su manual que estos son:

- Determinación de los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Estimar el impacto potencial, definido como el daño sobre el activo derivado.
- Determinación del riesgo potencial al derivar el riesgo dependiendo de la probabilidad de ocurrencia.
- Se miden los impactos a través de salvaguardias o procedimientos que reducen el riesgo.
- Obtener el impacto residual, que puede calcularse acumulado sobre los activos inferiores o repercutido con activos superiores.
- Lograr un riesgo residual al modificar el riesgo desde un valor potencial a un valor residual.

2.1.16 Vulnerabilidades físicas

Al hablar de vulnerabilidades físicas lo primero que debemos pensar es en la palabra infraestructura, pues aquí podemos pensar en objetos como computadores, oficinas, conexiones que podrían ser afectados por desastres naturales, como ejemplo podríamos decir una escuela que este ubicada en una zona de alto riesgo en cuanto a sismos o erupciones volcánicas, así como existen riesgos de alta prioridad como sismos e inundaciones también se tienen riesgos físicos que no son tan catastróficos, pero que si pueden causar daño

como una puerta sin cerrojo porque al ingresar a un área con material confidencial un usuario podría infectar equipos informáticos y así dañarlos. (Urbina Baca, 2017)

2.1.17 Vulnerabilidades lógicas

Aquí es donde exploramos aquellas amenazas que están en forma de un programa, con la finalidad de dañar un sistema, existen aquellos que fueron construidos con intenciones de hacer daño como aquellos softwares maliciosos y los errores que no son depurados como bugs o agujeros. (Lederkremer, 2020)

2.1.18 Hallazgos

Chicano Tejada (2016) menciona que, un hallazgo es el conjunto de información recopilada de una tarea o actividad que sea de interés para una organización, estos surgen ante la necesidad de averiguar debilidades en el sistema que se va a auditar, por lo general estos surgen durante el examen de auditoría que ejecuta el auditor para así presentar sus conclusiones y recomendaciones finales.

2.1.18.1 *Medidas físicas*

Estas son aquellas que protegen el hardware por medio de prevención a los desastres físicos, para ello se estudian bien la ubicación correcta entre los dispositivos de hardware para que no sean afectados por inundaciones o incendios para evitar pérdida de información de los sistemas de almacenamiento. (Lederkremer, 2020)

2.1.18.2 *Medidas Lógicas*

Por medio de estas medidas se puede proteger el software del sistema, con la finalidad de evitar manipulación o pérdida de información como contraseñas, permisos de usuarios o copias de seguridad, todo esto a través de software especializado como los antivirus. (Urbina Baca, 2017)

2.2 Infraestructura Tecnológica:

2.2.1 Introducción a la informática

En la actualidad la informática puede considerarse como una de las disciplinas más importantes jamás creadas, esto ha permitido grandes avances en todos los campos existentes, al automatizar procesos en diferentes industrias o al crear nuevos empleos gracias a los ordenadores esta se ha posicionado como una de las tecnologías más revolucionarias que existen, y lo mejor es que esta no para, sino que evoluciona constantemente, no existen límites para lo que pueda venir después. (Chaos García et al., 2017)

2.2.2 Historia de la informática

2.2.2.1 *Primera Generación:*

Este ordenador no fue muy tomado en cuenta en ese momento por lo que no se pusieron esfuerzos en mejorarlo, el evento detonante para ver el potencial de estas máquinas fue la segunda guerra mundial que dio paso a los ordenador electrónicos capaces de descifrar mensajes codificados, después de ello saltamos a los primeros ordenadores modernos, la ENIAC se presentó el 15 de febrero de 1946 y era de un tamaño bastante grande por todos los componentes que utilizaba, las válvulas al vacío no era duraderas, por lo que no le daban mucho tiempo de vida útil a ese equipo, entre sus funciones están que podía realizar 5000 sumas y 300 multiplicaciones por segundo, algo peculiar es que carece de sistema operativo y solo almacenaba números (Molero Prieto, 2016).

Después de aquellos ordenadores continuo la evolución hasta llegar a un dispositivo electrónico que sea más compacto que presentan ventajas como rapidez al procesar miles de datos por segundo, confiabilidad al mantener alta precisión a través de sus componentes, creatividad al desarrollar cualquier proyecto y seguridad para ayudar a prevenir errores en los sistemas. (Pereyra, 2020)

2.2.2.2 *Segunda generación:*

En esta generación se empezaron a construir los circuitos de transistores y empiezan a aparecer aquellos lenguajes de programación conocidos de nivel alto, aquí se reduce su tamaño con el fin de enfocarlo a un público diferente, a través de diseños más ergonómicos con pantallas antirreflejos y teclados que permitan descansar las muñecas para una mayor comodidad. (Weber, 2020)

2.2.2.3 *Tercera generación:*

Para esta generación los ordenadores se centran en los circuitos integrados, por ello se reduce más el tamaño a uno mediano pero que sin sacrificar el rendimiento al seguir disponiendo de una gran cantidad de procesamiento, los lenguajes de control de los sistemas operativos toman una gran importancia para las computadoras personales de IBM. (Molero Prieto, 2016)

2.2.2.4 *Cuarta generación:*

La invención más relevante en esta generación son los circuitos integrados de alta densidad, al reducirlos sus costos se abarataron y aquí es cuando empieza la verdadera revolución industrial, los pioneros de aquella revolución son Steve Wozniak y Steve Jobs con la creación de la primera computadora Apple, el avance no solo se produce a nivel de hardware, el software toma una gran importancia con la invención de los procesadores de texto y paquetes gráficos. (Pereyra, 2020)

2.2.2.5 *Quinta generación:*

En esta generación los sistemas de inteligencia artificial toman un gran protagonismo, el objetivo principal que se persigue en esta generación es que las computadoras puedan realizar procesamiento de tareas en paralelos. (Molero Prieto, 2016)

2.2.3 Tipos de computadoras

2.2.3.1 *Supercomputadora:*

A este tipo de computadora se la considera como una de las más rápidas y costosas que existen, el motivo es que no suelen usarse por parte de usuarios comunes, sino que están destinadas para realizar múltiples operaciones numéricas a una gran velocidad de procesamiento (Chaos Garcia et al., 2017).

2.2.3.2 *Macro computadoras:*

Vasconcelos (2018) define como aquellos ordenadores que están destinados para mantener interconectados a una gran cantidad de personas, gracias a estos y a sus miles de Terabytes en discos duros y periféricos ayudan a que grandes compañías puedan manejar datos de su organización de manera eficiente.

2.2.3.3 *Minicomputadoras:*

Por otro lado, están este tipo de computadoras que son para los usuarios comunes, que buscan utilizarlas como un soporte para guardar información personal o de trabajo y como instrumento de recreación, dentro de estas están las computadoras personales, o asistentes digitales como PDA que buscan ofrecer todas las funciones de un ordenador en formatos más accesibles de transportar. (Molero Prieto, 2016)

2.2.4 Periféricos

Chaos et.al (2017) describe a estos objetos como equipos que permiten la comunicación con el exterior sirviendo de apoyo, como para archivar información o manejarla, los más comunes que se pueden encontrar son:

- **Teclado y ratón:** Son los más comunes actualmente, el teclado es el dispositivo principal para la entrada de datos alfanuméricos y el ratón es el elemento que apunta lo que se desea seleccionar en la interfaz gráfica de la computadora.

- **Monitor o pantalla:** Aquel muestra la información que procesa el equipo y lo expresa en una interfaz gráfica para facilidad de manejo del usuario.

- **Impresora:** Este dispositivo permite la extracción de información en un medio físico como papel y se basa en un sistema que utiliza cartuchos de tinta o tecnología láser.

- **Altavoces:** Permite la comunicación de audio entre el ordenador y el usuario a través de una tarjeta de sonido.

- **Disco duro portátil:** Gracias a este dispositivo se puede mejorar la gestión de archivos y aplicaciones gracias a su capacidad de lectura o escritura.

2.2.5 Redes de ordenadores

Con esta técnica se logra que dos o más ordenadores puedan tener comunicación entre sí, uno de los fines es la transmisión de archivos y servicios, por ende, aumenta las capacidades que pueden ofrecer los ordenadores y esto a través de varias formas, por conexión de cables o con el uso de las redes inalámbricas, el uso más frecuente que tienen actualmente es el compartir acceso de internet. (Sanchez Cascado & Mingo , 2017)

2.2.5.1 *Tipos de redes*

a) **Redes locales:** Se encuentran en lugares no tan grandes, por medio de estas los ordenadores de establecimientos como escuelas o edificios pueden compartir archivos dentro de una misma área.
b) **Redes con servidores:** En este tipo de redes existen programas instalados en el servidor, permiten que el ordenador que funciona como servidor actúe como potente, mientras que los demás ordenadores clientes, con estas redes se busca controlar el acceso a la red desde los clientes por medio de permisos de utilización de archivos.

2.2.5.2 *Protocolos de red*

Moro Vallina (2021) menciona en su libro que el establecer comunicación entre varios dispositivos electrónicos y conectarlos a su vez a la red puede ser una tarea complicada, el protocolo desempeña un papel importante como si se tratara de una conversación entre dos personas, de la misma manera es aquel paso que permite que la comunicación se transmita y se entienda de forma mutua, la sintaxis y la semántica son complementos importantes, la sintaxis define la estructura y el formato de los datos, mientras que la semántica le da significado a cada conjunto de bits.

2.2.6 Modelos de Red

2.2.6.1 *Modelo TCP/IP:*

Este modelo funciona en base a cuatro capas, se omite la de nivel físico y la de enlace se reduce a una interfaz entre la red física que se usa y el protocolo IP de la red, esta forma da una ventaja pues no es necesario especificar cuáles son las características físicas de la red y por ende no se la ligaba a una tecnología en concreto. Además, no existe una separación entre protocolos, pues usa diferentes interfaces que permiten que el modelo sea muy difícil de implementar en otras redes, por esa razón es que la planificación y la implementación de esta se debe hacer con extremo cuidado, para que las futuras tecnologías puedan ser adaptadas sin ningún problema de compatibilidad. Jiménez et.al (2017) detalla que las capas que utiliza este modelo son:

- **Capa de aplicación:** Esta especifica el formato y control de la información para encontrar compatibilidad con la mayoría de las funciones que se encuentran dentro del internet.
- **Capa de enlace:** Tiene la función de actuar como interfaz entre el nivel de red y la red física en uso, se encarga de convertir y transportar los paquetes por medio de un controlador que garantiza la llegada de la información al destino indicado.

- **Capa de red:** Se encarga de incorporar protocolos de apoyo como ICMP para comunicación de mensajes de error e IGMP para la gestión de envio de mensajes a grupos de procesos que pueden tener direcciones IP dispersas.

- **Capa de transporte**: Implementa protocolos de extremo a extremo que conecte el nodo de origen con el destino, para ello están los protocolos TCP que están orientados a una conexión fiable y con control de seguimiento y UDP que no garantiza un secuencia de datos pero da una gran velocidad.

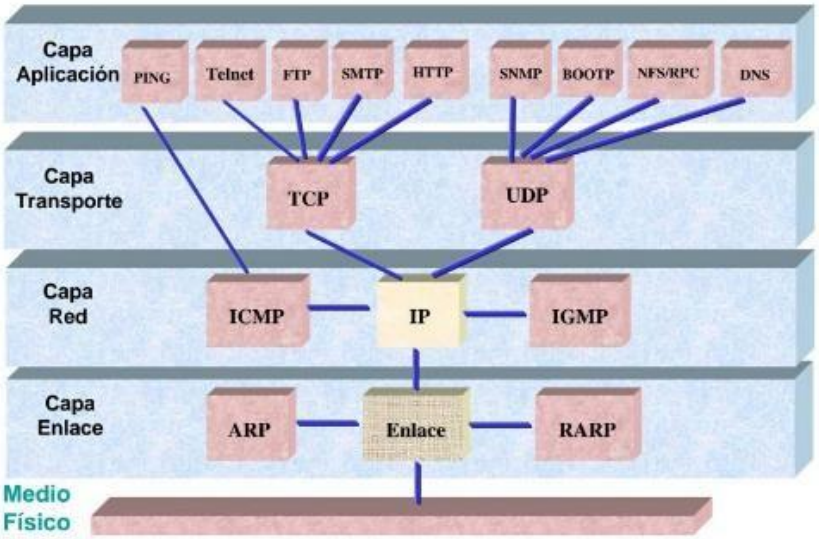


Ilustración 2 Modelo TCP IP

Extraído de: Sistemas distribuidos, arquitectura y aplicaciones (2017)

2.2.6.2 *Modelo OSI:*

Concejero et.al (2020) mencionan que este modelo a su vez que el TCP/IP es bastante complejo, solo que este en vez de cuatro utiliza siete capas, sin embargo, el objetivo no vario pues con él se desea interconectar sistemas de información para que puedan intercambiar información sin ningún tipo de restricción, para ello se descomponen los procesos en varias capas, estas son:

- **Capa física:** Define los aspectos que relacionan los elementos físicos que intervienen en la transmisión de datos, para ello se utilizan diferentes

elementos como mecánicas, componentes eléctricos, funcionales y de procedimiento, en si ayuda al proveer mecanismos para enviar y recibir bits empleando un canal de comunicación.

- **Capa de enlace de datos**: La función de esta capa es agrupar los bits en tramas, estas tramas son las letras o números y este se encarga de transformarlos en frases que todos podamos entender.

- **Capa de red:** Proporciona los medios necesarios para la transferencia de la información, encamina la petición a través de internet para que llegue al sitio adecuado.

- **Capa de transporte:** Esta capa provee los mecanismos para el intercambio de datos entre sistemas de extremo a extremo, es muy parecida a la capa de enlace de datos, salvo que se llevan a cabo entre los dos extremos de la comunicación como un PC y el servidor web.

- **Capa de sesión:** La función de esta etapa es iniciar la comunicación entre emisores y receptores, así mismo gestiona y administra la estabilidad de la conexión para que permanezca lo más sólida posible.

- **Capa de presentación:** Por medio de esta capa se preparan los paquetes de datos y se los convierte en un lenguaje que pueda ser entendible para cualquier red o dispositivo, se la conoce más como la capa traductora, de la misma forma cifra y reduce el tamaño de los paquetes.
- **Capa de aplicación:** Es la última y se caracteriza por ser la capa con la que el usuario interactúa, puede tratarse de una aplicación como el cliente de correo electrónico o un explorador web.

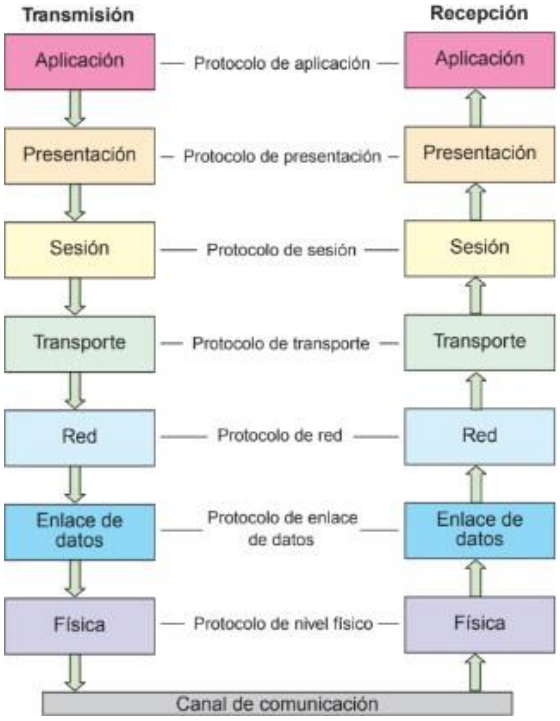


Ilustración 3 Proceso de comunicación con el modelo OSI

Extraído de: Redes locales 3era edición (2020)

2.2.7 Sistemas operativos

Hoy por hoy se considera a un sistema operativo como un software base, pues funciona como un conjunto de programas que funcionan dentro de un ordenador nada más al encender la máquina, se le puede facilitar al usuario el manejo del hardware y así simplificar la dificultad de diferentes tareas. (Alegre Ramos, 2019)

Posee diferentes funciones como:

- Gestionar los recursos de hardware y software
- Administrar la gestión de los programas
- Mantener funcional el sistema de archivos
- Solucionar errores que se puedan producir con el hardware y software del ordenador.

2.2.8 Licencias de software

Moro Vallina (2021) define estas como un contrato que se establece entre el dueño de los derechos de un sistema y el usuario que adquiere el mismo, por lo general estas se expresan en un contrato que contiene los términos y condiciones para el uso del software, esto existe para proteger la propiedad intelectual del autor al restringir la reproducción de su trabajo. Esta modalidad se introdujo en los años sesenta y ampara el código fuente del autor para que no sea distribuido públicamente.

Por otra parte, existen aquellas licencias que permiten al usuario realizar modificaciones de su obra con el fin de mejorar la experiencia en base a sus contribuciones, a continuación, las diferentes clases de licencias de software que se encuentran son:

- **Software libre:** Se llama así porque respeta la libertad de los usuarios y su comunidad, pues se les permite estudiar, modificar y mejorar el software, por lo general este se distribuye de manera gratuita, la única condición es que de la misma manera los usuarios que realicen modificaciones las compartan para que estén disponibles para el resto del mundo. (Muñoz López, 2017)

- **Software propietario:** Este tipo de software se crea por compañías que permiten la utilización de copias del mismo pero establecen que ellas le pertenecen a la misma y no al usuario, en la mayoría de los casos la obtención de una licencia va acompañada por un pago de contraprestación económica, de esa forma evitan que los usuarios distribuyan copias ilegales de este, para prevenir esto en la última década se han utilizado métodos como licencias de uso temporal que solo dan un periodo de prueba para utilizar dicho software, códigos de seguridad o claves para evitar la distribución y por ultimo dispositivos físicos que se conectan a un ordenador el momento de instalación como si fuesen una llave.

2.2.9 Estructura general de un sistema operativo

a) **Gestión de E/S:** Otra de sus múltiples tareas es el gestionar que todos los dispositivos de entrada y salida como periféricos funcionen de una forma eficaz y sencilla con relación al usuario. (Sánchez Cascado & Mingo , 2017)
b) **Gestión de archivos:** Un archivo es un objeto que se almacena dentro de una unidad lógica en directorios o ficheros especiales, estos se caracterizan por tener atributos que en la mayor parte son modificables, estos pueden ser nombre, fecha de creación, propietarios, permisos, etc. Con un fichero se pueden realizar diversas operaciones como crear, leer, escribir o borrar información. (Sánchez estella, 2021)
c) **Gestión de la seguridad:** Una de las funciones principales que debe cumplir el sistema operativo es el controlar el acceso a los usuarios con relación a los recursos del sistema, para ello usan técnicas como la protección de memoria, particionamiento, intercambio, compartición, reubicación, fragmentación, entre otras. (Pereyra, 2020)

2.2.10 Aplicaciones informáticas

Las aplicaciones informáticas son aquellos programas que proporcionan diferentes funcionalidades al sistema operativo con la finalidad de aprovechar al máximo los recursos de un ordenador se manejan con instrucciones a través del sistema operativo y tienen características como envergadura, complejidad y ámbito de aplicación. (Chaos et al., 2017)

Algunas aplicaciones que son de vital importancia para el correcto funcionamiento del ordenador son:

a) **Procesadores de texto:** Por medio de este software se permite realizar archivos de tipo texto, aquellos como libros, cartas, folletos, etc. Estos se adaptaron al ordenador a partir de los modelos de las máquinas de escribir, por ello se propuso el adaptar ese concepto y mejorarlo para obtener una experiencia más cómoda con respecto a la información mecanografiada. (Sanchez Cascado & Mingo , 2017)

b) **Hojas de cálculo:** A través de estos programas se pueden realizar operaciones con cierto grado de complejidad, son capaces de obtener valores reales que son actualizables, una de sus principales funcionalidades es el crear gráficos a partir de los datos que se han introducido. (Pereyra, 2020)
c) **Bases de datos:** Con estas herramientas se pueden almacenar, consultar, editar o eliminar información de un modo rápido y eficaz, a través de creación de tablas relacionales que permitan guardar campos de manera ordenada y sencilla para el entendimiento del usuario promedio. (Alegre Ramos, 2019)
d) **Programas de imágenes y audios:** Estos programas son capaces de permitir la realización de archivos como fotos, iconos y sonidos que se pueden usar en presentaciones sean de un documento, libro o una página web, con relación a las imágenes pueden ser dibujadas o escaneadas directamente de un papel por medio de un escáner, mientras que los sonidos pueden ser grabados a través de periféricos como micrófonos. (Chaos Garcia et al. 2017)

2.2.11 Ofimática

El termino ofimática se puede desglosar de dos palabras sencillas, ofi de oficina e matica por la informática, teniendo conocimiento de aquello se puede deducir que la ofimática relaciona todo tipo de tecnología informática a usos dentro de oficinas de diferentes empresas o negocios como escuelas, bancos, etc. Se utiliza bastante este término al referirse a todo aquello que permite gestionar de manera eficiente la información que se maneja dentro de un establecimiento, se puede ligar a tareas como manejo de documentos, archivos, así como su clasificación o consulta de datos a los mismos. (Aguilera López, 2021)

CAPÍTULO II

ESTUDIO DE CAMPO

3.1 Metodología de investigación

La metodología de la investigación es el conjunto de métodos y técnicas que se implementan para llegar a una conclusión lógica que resulte comprobable, además de ello, busca implementar soluciones a los problemas que parten de esas conclusiones para hacer la vida del hombre más fácil por medio de la organización, conocimiento, hipótesis y datos relevantes que guíen a esas conclusiones. (Reyes, 2020)

Se usó para determinar cuáles fueron las técnicas de instrumentos que se aplicaron en esta investigación.

3.2 Tipos de investigación

- **Investigación documental**

La investigación documental implementa el uso de documentos como recurso principal, hay que tener muy claro que un documento es toda información que haya dejado huella en el planeta, esta información está plasmada en libros, publicaciones como periódicos, revistas, folletos, volantes o desplegables, se la puede realizar de forma independiente. (Baena Paz, 2017)

Se usó de esta investigación al utilizar información almacenada en artículos y libros que se relacione con la aplicación de una auditoría de infraestructura informática.

- **Investigación de campo**

Para utilizar este tipo de investigación es necesario que el fenómeno no sea alterado, es decir, que se encuentre en su forma natural, para que se puedan obtener datos que se acerquen lo más posible a la realidad. Para ejecutar este

tipo de investigación es necesario recoger y registrar de manera ordenada los datos, esto utilizando técnicas como encuestas, entrevistas o cuestionarios.

Se aplicó este tipo de investigación a través de encuestas y entrevistas que se realizaron a personal de la institución.

3.3 Métodos de investigación

- **Observación científica**. – “Es un proceso riguroso que consiste en la percepción directa del objeto de investigación y permite conocer, de forma efectiva, el objeto de estudio para luego describir y analizar situaciones sobre la realidad estudiada.” (Hernández, et al., 2021)

  Se aplicó en el capítulo dos para recabar información sobre la auditoría informática y poder evaluar los potenciales riesgos que podrían estar presentes en la organización.

- **Inducción 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 de común en los fenómenos individuales. Como un proceso del pensamiento en el que, de afirmaciones generales, se llegaba a afirmaciones particulares que aplicaban las reglas de la lógica.” (Rodríguez et al., 2017)

  Este método se aplicó para realizar la auditoría informática con la metodología MAGERIT que permitirá prever los riesgos potenciales de los equipos informáticos en la institución.

3.4 Técnicas - instrumentos de investigación

3.4.1 Encuesta- guía de entrevista

“Es un método descriptivo con el que se pueden detectar ideas, necesidades, preferencias, hábitos de uso, etc. “(Paz et., 2016).

Se aplicó encuesta al personal administrativo de la Unidad Educativa Antonio José de Sucre.

3.4.2 Entrevista

“Es una de las herramientas para la recolección de datos más utilizadas en la investigación cualitativa, permite la obtención de datos o información del sujeto de estudio mediante la interacción oral con el investigador.” (Troncoso,et., 2016)

Se utilizó para recibir la información del encargado al rector y vicerrector de la institución educativa.

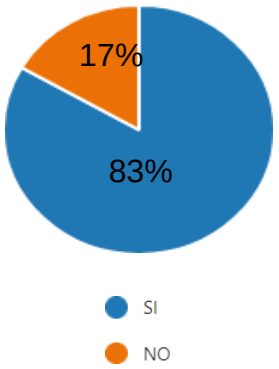
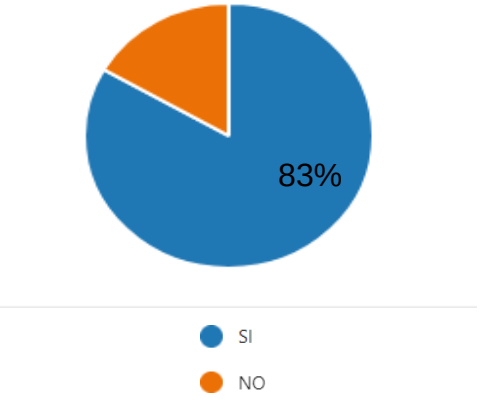
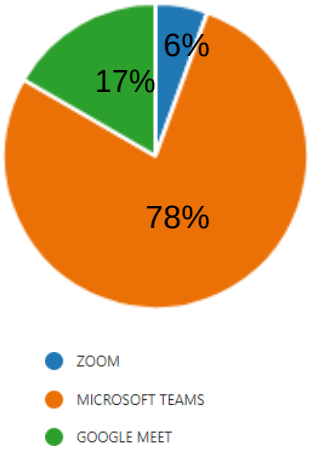
3.5 Población

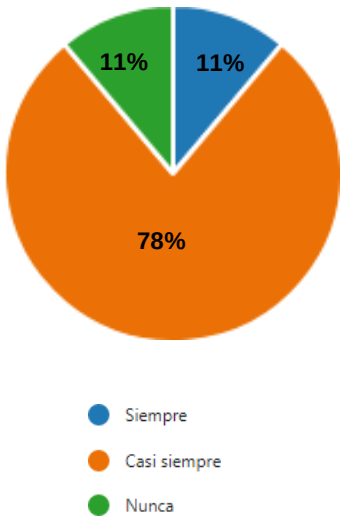
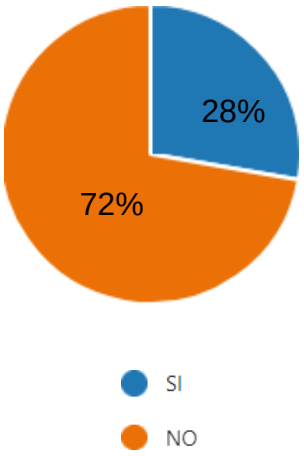
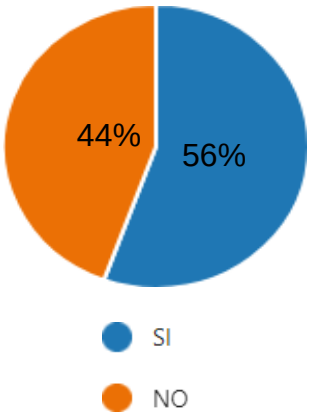
3.5.1 Población

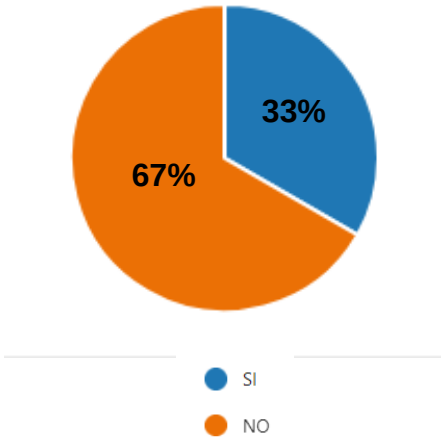
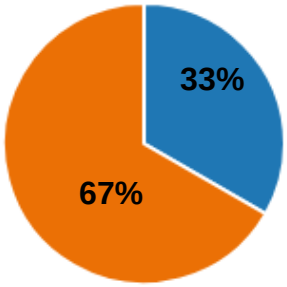
La población de estudio es un conjunto de casos, definido, limitado y accesible, que formará el referente para la elección de la muestra, y que cumple con una serie de criterios”. (Gómez et al., 2016)

Fueron 18 docentes que utilizaron el laboratorio en la Unidad Educativa Antonio José de Sucre y no se aplica muestreo porque la cantidad de persona es pequeña.

3.6 Resultados de la investigación de campo.

Pregunta	Gráfico	Interpretación
1. ¿La institución cuenta con un departamento encargado a las tecnologías de la información?		La mayoría de los docentes respondieron que si hay un departamento encargado de los dispositivos tecnológicos y se pudo detectar que los docentes si están al tanto que hay un departamento de tics.
2. ¿Se lleva un inventario de los dispositivos informáticos que posee la institución?		El resultado mayor de los docentes mencionó que si llevan un inventario sobre los dispositivos informáticos quiere decir que si están al tanto.
3. Seleccione cuál de las plataformas educativas utiliza la institución?		Un poco más de la mitad de los docentes afirma que trabajan con la plataforma Microsoft Teams

Pregunta	Gráfico	Interpretación
4. ¿Con que frecuencia se hace mantenimiento a los dispositivos informáticos?		Un poco más de la mitad del personal administrativo de la institución comentaron dando un resultado del casi siempre realiza el mantenimiento a los dispositivos informáticos del laboratorio.
5. ¿Alguna vez se ha extraviado información de los computadores de la institución?		Más de la mitad se le ha extraviado información académica siendo un problema para los docentes de la institución.
6. ¿Los datos de todos los estudiantes y personal administrativo de la institución se encuentran protegidos por alguna contraseña de seguridad?		Un poco más de la mitad de los administrativos respondió que los datos si los protegen a través de contraseñas, mientras que la menor parte contradijo que estos datos no están protegidos por ningún medio de seguridad como una contraseña u otros.

Pregunta	Gráfico	Interpretación
7. ¿En caso de un daño, existen formas de recuperar la información de los ordenadores de la institución?		La mayoría de la población contesto que la unidad educativa no tiene medios para recuperar la información en caso de sufrir pérdidas de la misma, mientras que pocos dicen que si existe un sistema para ello.
8. ¿Para acceder a las instalaciones informáticas existe algún tipo de política para el acceso a las mismas?		Un poco más de la mitad de los docentes y administrativo manifiestan que no existe algún tipo de política a la hora de ingresar al laboratorio mientras que la menor parte dicen que si tienen políticas para ingresar.

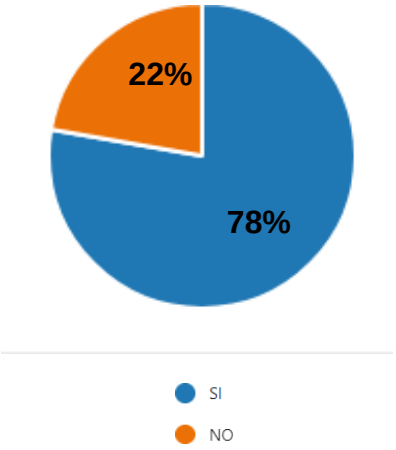
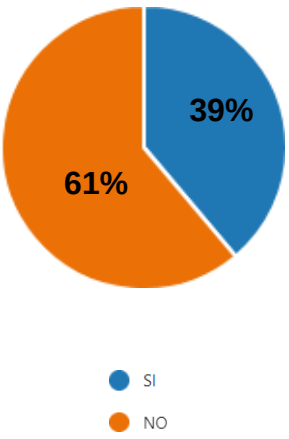
Pregunta	Gráfico	Interpretación
9. ¿Los equipos están protegidos contra imprevistos como aumento de corriente eléctrica o sobrecalentamiento?		Un poco más de la mitad de los administrativos manifiestan que los equipos que encuentran en la institución no están protegidos contra daños de corriente eléctrica o sobrecalentamiento, mientras que la menor parte dice que si existen algunos aparatos que protegen los ordenadores en contra esos daños.
10. Existen avisos que ayuden a prevenir desastres dentro de los centros informático la institución		Un poco más de la mitad contestaron que no existen avisos que permitan prevenir desastres dentro del centro informático, mientras que pocos dicen que si existen avisos es esta parte del establecimiento.

Tabla 1 Encuesta

Entrevista

Dirigida a: Rector de la institución educativa Ing. Luis Arteaga

Entrevistador: Leonela Paladines

1. ¿Sabe si existe personal que se encargue del departamento de tics en la unidad educativa?

Sí, hay una docente encargada pero no sabe nada de instalación o mantenimiento de las máquinas.

2. ¿Existen registros del inventario que posee la unidad educativa en cuanto a equipos tecnológicos?

Sí, existe inventario y lo lleva el rector de la institución.

3. Conoce la cantidad de equipos informáticos que posee la institución

Hay 30 máquinas en el laboratorio y 5 en oficina.

4. ¿Se lleva algún tipo de control en mantenimiento a los equipos que se usan en la institución educativa?

Cuando hay problema con alguna maquina el rector hace un oficio para que los del distrito manden a alguien de tics para las máquinas.

5. ¿Cómo manejan la seguridad de los datos tanto de estudiantes como del personal administrativo?

La mayoría de los docentes guardan en la nube la información, otros en flash memory y los estudiantes guarda en laboratorio.

6. ¿Posee algún plan de riesgos dentro de los laboratorios de informática en caso de que se presente uno?

No, existe un plan de riesgos.

7. ¿Existen alguna política que se deba respetar al momento de acceder a los laboratorios de informática?

Solo hay recomendaciones como no ingresar con comida y bebidas, solo consultas académicas y lo que quieren pedir es tener una herramienta que permita controlar de manera académica a los estudiantes.

8. ¿Cómo protegen los equipos informáticos de problemas como exceso de corriente o sobrecalentamiento?

No, habido problemas y también hay reguladores en cada computadora.

9. ¿Las áreas donde se trabajan con equipos informáticos son seguras?

Por el momento no habido problemas.

10. ¿Cada sala informática cuenta con espacio suficiente para alumnos y equipos?

Si hay suficiente espacio suficiente espacio porque cuando los estudiantes van por paralelo no supera los 20 estudiante.

Entrevista

Dirigida a: Inspectora Lic. Mónica Andrea Mejía Guerrero. Mgs

Entrevistador: Leonela Paladines Chuez

1. **¿Sabe si existe personal que se encargue del departamento de tics en la unidad educativa?**

Sí, hay una docente encargada pero no sabe nada de informática.

2. **¿Existen registros del inventario que posee la unidad educativa en cuanto a equipos tecnológicos?**

Sí, existe inventario

3. **Conoce la cantidad de equipos informáticos que posee la institución**

Sí, hay 30 máquinas en el laboratorio y 5 en oficina.

4. **¿Se lleva algún tipo de control en mantenimiento a los equipos que se usan en la institución educativa?**

El rector hace un oficio y pasa al distrito para que manden a alguien de Tics.

5. **¿Cómo manejan la seguridad de los datos tanto de estudiantes como del personal administrativo?**

La mayoría de los docentes guardan en la nube la información, otros en flash memory y los estudiantes guarda en laboratorio.

6. **¿Posee algún plan de riesgos dentro de los laboratorios de informática en caso de que se presente uno?**

No, existe un plan de riesgos.

7. **¿Existen alguna política que se deba respetar al momento de acceder a los laboratorios de informática?**

Solo hay recomendaciones como no ingresar con comida y bebidas, solo consultas académicas y lo que quieren pedir es tener una herramienta que permita controlar de manera académica a los estudiantes.

8. **¿Cómo protegen los equipos informáticos de problemas como exceso de corriente o sobrecalentamiento?**

No, ha sufrido problemas y a la vez el laboratorio cada computadora tiene reguladores para el sobrecalentamiento.

9. **¿Las áreas donde se trabajan con equipos informáticos son seguras?**

Por el momento no habido problemas.

10. **¿Cada sala informática cuenta con espacio suficiente para alumnos y equipos?**

Si hay suficiente espacio suficiente espacio porque cuando los estudiantes van por paralelo no supera los 25 estudiante.

3.7 Análisis de resultados

- La pregunta 4 de la encuesta comentan que casi siempre se realiza mantenimiento en el laboratorio de la institución que cuentan con un departamento informático para los dispositivos informáticos, Por lo que la pregunta 4 de la entrevista asegura llevar un control en mantenimiento de los equipos que se encuentran en uso dentro del laboratorio de la Unidad Educativa Antonio José de Sucre.
- La pregunta 8 de la encuesta manifiestan que no existe algún tipo de política a la hora de acceder al laboratorio de la institución, mientras que la 7 de la entrevista brindada por la inspectora Mónica Andrea Mejía Guerrero afirma que solo hay ciertas recomendaciones para el buen uso al momento de hacer el ingreso del centro informático.
- La pregunta 9 de la encuesta ratifican los docentes administrativos de la institución Antonio José de Sucre que no cuentan con protección adecuada ante daños de corriente eléctrica o a su vez de sobrecalentamiento en los equipos informáticos del laboratorio, y 8 de la entrevista afirman que los equipos están protegidos para que ayude a prevenir el sobrecalentamiento dentro del centro informático y a su vez no se ha presentado problemas de estos riesgos.
- La pregunta 10 de la encuesta los docentes describen que no existen avisos que permitan prevenir sobre los desastres u otros en el laboratorio informático, por lo que la pregunta 6 de la entrevista resalta no han elaborado un plan de riesgo para dichos desastres que se puedan suscitar en el laboratorio informático en la unidad Educativa Antonio José de Sucre.

CAPÍTULO III

DESARROLLO DE LA PROPUESTA

4.1 Antecedentes

HISTORIA

Lo que hoy es el sitio “Unión de Colonape” perteneciente a la parroquia y cantón El Carmen fue territorio colonizado en la década de los 50,algunos de los primeros habitantes son compatriotas y otros de origen colombiano que han hecho de este lugar su pequeña patria.

La primera educación que recibieron los niños de este sector fue impartida por un padre de familia el Sr. Julio Bolívar Macías, a unos 15 niños del sitio El Achiote, el Sr. Bolívar laboro desde 1960 a 1962 ganando 5 sucres por niño. Esta escuela luego se traslada a un terreno más plano, bajo sostenimiento particular, la estructura era de material de la zona (caña, pambil).

En el año 2010 se declara a nivel Nacional la universalización del Primer año de Educación General Básica. En 2007 el FISE comienza la construcción de 5 aulas, para finalmente ser entregadas en el 2008.En el 2010’ mediante oficio 0169-DEPM-DP 2010 de fecha 10 de agosto del 2010 se crea el Centro General de Educación Básica.

Para el inicio del periodo 2014-2015 se considera a la institución con la creación del nivel de Educación Inicial y el periodo 2017- 2018 se crea el Primer año de Bachillerato Unificado.

4.2 DATOS INFORMATIVOS

NOMBRE DE LA INSTITUCIÓN:	Unidad Educativa “Antonio José de Sucre”
CÓDIGO AMIE	13H01595
UBICACIÓN GEOGRÁFICA	RURAL
ZONA	04
DISTRITO	13D05
CIRCUITO	13D05C03
CIUDAD	El Carmen
NIVELES EDUCATIVOS	• Educación Inicial • Educación General Básica • Bachillerato General Unificado
CARÁCTER	Fiscal
JORNADA	Matutina
GENERO	Mixto
NÚMERO DE ESTUDIANTES	360

NÚMERO DE DOCENTES	16
E-mail	d13h01595ajs@gmail.com

Tabla 2: Datos de la institución Antonio José de Sucre

4.3 Organigrama

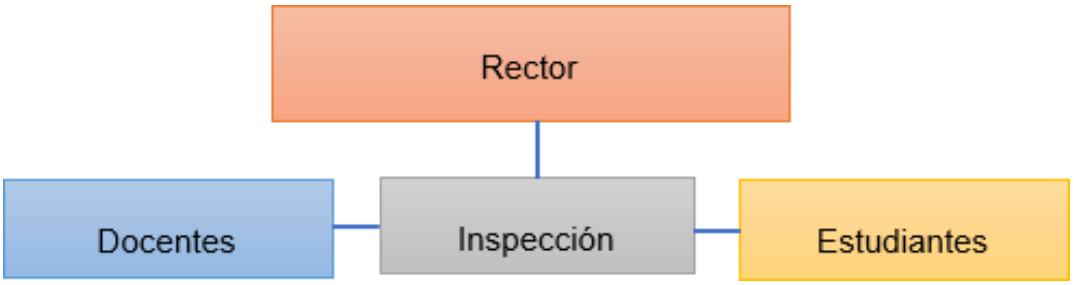


Tabla 3: Organigrama institucional

4.4 Misión

La Unidad Educativa “Antonio José de Sucre”, es una institución facilitadora de aprendizajes significativos e innovadores, formando ciudadanos investigadores, críticos, honestos y responsables contribuyendo a una educación integral, basada en la inclusión, procurando la protección del medio ambiente con formación académica transcidiplinaria, manteniendo una convivencia armónica con todos los actores de la comunidad Educativa, con el desafío de preparar a los educadores para el mundo que nos rodea haciendo uso responsable de las herramientas tecnológicas y recursos del medio, con docentes capacitados para impartir sus clases desde e nivel inicial hasta el bachillerato logrando el desarrollo de sus facultades intelectuales, físicas y efectivas en el mundo que nos rodea.

4.5 Visión

Al 2022 la unidad Educativa “Antonio José de Sucre” brindara educación de calidad y una formación respetuosa, solidaria, justa, autónoma, emprendedora,

responsables competentes e innovadora a niños, niñas y adolescentes de nuestra comunidad y zonas aledañas, con capacidades de liderazgos, el bien común que vayan en beneficio de cultivar una cultura de paz para la sociedad y responsables con el medio ambiente.

PROGRAMA DE AUDITORÍA INFORMÁTICA DE SEGURIDAD DE LA INFORMACIÓN		
OBJETIVOS: 1. Identificar principales riesgos de seguridad que existen en la institución. 2. Verificar el nivel de seguridad de la infraestructura tecnológica que posee la Unidad Educativa Antoni José de Sucre.		
TÉCNICAS Y PROCEDIMIENTOS	**REFERENCIA**	**FECHA**
1.1 Investigar sobre la seguridad de la información y normas, leyes, políticas, relacionada a la misma.	I_1	(S1,S2)
1.2 Revisar metodología MAGERIT junto a los pasos de su ejecución.	I_2	(S3,S4)
1.4 Definir activos	J1	(S5,S6)
1.5 Definir Amenazas	J2	(S7,S8)
1.6 Elaborar instrumentos de auditoría con base a normas, leyes, políticas. (Diseño de instrumento)	K	(S9)
1.7 Aplicación de instrumentos de investigación.	K	(S10)
1.8 Tabulación y análisis de datos.	L1	(S11)
2 identificación de salvaguardas (Medidas de prevención)	L2	(S11)
2.1 Evaluación de riesgos (Matriz de riesgos)	L4	(S12)
2.2 Tratar los riesgos y elaboración del manual de contingencia.	M	(S12)
3. elaborar del informe	N	(S13)

Tabla 4 Programa de auditoría

4.5.1 Informe de auditoría

En el presente informe se muestran los resultados de la auditoría de seguridad informática en la Unidad Educativa Antonio José de Sucre, definiendo los riesgos asociados a vulnerabilidades dentro de la infraestructura tecnológica de la institución y la soluciones o medidas que se deben aplicar o tomar en consideración para prevenir dichos eventos en cada una de ellas; de esta manera, se logra disminuir en cierta parte el impacto al momento que se presenta algún riesgo.

4.5.2 Dirigido a:

Rector de la Unidad Educativa Antonio José de Sucre Ing. Luis Arteaga Este informe de auditoría informática de seguridad de la información va dirigido a la Unidad Educativa Antonio José de Sucre.

4.5.3 Objetivos:

Para desarrollar la auditoría se establecieron objetivos que ayudaron a tener una orientación mucho más clara de que era lo que se iba a evaluar dentro de la institución:

- Identificar principales riesgos de seguridad que existen en la institución.
- Verificar el nivel de seguridad de la infraestructura tecnológica que posee la Unidad Educativa Antonio José de Sucre.

4.5.4 Personal relacionado:

En esta auditoría de seguridad informática están involucrados el rector, inspectora y personal administrativo de la Unidad Educativa Antonio José de Sucre encargados del manejo de información, los cuales brindaron la información necesaria que se necesita para poder recolectar los datos suficientes que le den veracidad e importancia a esta auditoría.

4.5.5 Alcance

Como parte fundamental de esta auditoría de seguridad informática física se aplicó la metodología de análisis de Riesgo Magerit.

Este tipo de metodología de análisis de gestión de riesgo nos permitió identificar las vulnerabilidades y amenazas en la tecnología de la información por lo cual hace referencia a cincos pasos importantes a emplear dentro de la investigación a realizar, como determinar los activos a evaluar en la institución para así poder determinar las amenazas y riesgos que están expuesto dichos activos, a su vez evaluar el impacto logrando obtener un resultado efectivo. Teniendo, así como objetivo principal concienciar a los responsable de la institución Antonio José de Sucre de la existencia de los riesgos y a la vez analizar las amenazas existentes de cada uno de los equipos informáticos, ayudando a analizar y planificar el tratamiento oportuno para mantener los riesgos bajo control.

En este tipo de metodología incluye etapas que sirvieron para el proceso de evaluar el nivel de seguridad de cada uno de los riesgo que se presentan dentro del laboratorio informático de la institución, y además se aplicaron dos herramientas para poder analizar los posibles riesgos que se encuentran en los dispositivos informáticos, siendo así la primer herramienta la encuesta con el instrumento de cuestionario donde está compuesta por 25 preguntas cada riesgo los cuales se detallan a continuación, robo, virus, robo de información, incendio, inundación, daño de equipos con un total de 150 preguntas aplicadas en una encuesta dirigida al Rector Luis Arteaga .

Se realizó una entrevista donde se le aplico al rector Luis Arteaga y a la inspectora con un total de 10 preguntas donde se pudo recabar información sobre el nivel de riesgo detectado en el laboratorio informático Tal cual una de las principales riesgos no tener políticas de seguridad al ingresar al laboratorio.

4.5.6 Definir activos

Los activos definidos dentro de la metodología Magerit está constituidos en dos tipos que son:

- Software
- Hardware

CODIGO	NOMBRE DEL ACTIVO
CE0001	COMPUTADORAS DE ESCRITORIO
IL0001	IMPRESORA
PL0001	PROYECTOR
RL0001	ROUTERS

Tabla 5: Definir Activos

4.5.7 Definir amenazas

En el laboratorio de la institución Antonio José de Sucre las amenazas más frecuentes que enfrentan, son perdidas, ataques a los sistemas educativos y robos de información, tal cual como datos almacenados de los estudiantes y docentes en el ámbito académico.

4.5.8 Ataques en internet más comunes en el laboratorio de la institución Antonio José de Sucre

Ataque	Descripción
Robo	Se produce con fines de obtener datos sensibles que puedan afectar al funcionamiento de un establecimiento, por esa razón continúan guardando su información de manera local, muchos al no contar con un departamento enfocado a la seguridad de los sistemas donde entra y sale en los departamentos de TICS, por ello es importante pensar si existe un respaldo de la data que puede perderse o dañarse por causa de individuos. (Barreneche, 2020)
Incendio	Los incendios son especialmente relevantes dentro del campo de la informática, una de las causas más comunes son los cortocircuitos, estos suelen ser imperceptibles pues ocurren en zonas ocultas como bandejas de cables o por mal funcionamiento del equipo, al no tener un mantenimiento adecuado puede llegar a colapsar en cuanto se empiece a propagar el fuego. (Maya, 2017)
	Esto porque el agua arruina los circuitos de un ordenador una vez que los toca, por ende desencadena fallas como descompostura,

Inundación	bloqueo, desconfiguración o por último daño total de un equipo, la causa más común para que ocurra una inundación dentro de una centro informático puede ser la acumulación de agua dentro de un desagüe tapado, esto ocasiona que el agua pueda filtrarse y llegar a los dispositivos, lo que causaría cortocircuitos. (Cuenca, 2018)
Virus	Los virus informáticos puede ser devastadores todos ellos a medida que se extienden pueden causar pérdidas como la sustracción de datos, detener el rendimiento de los ordenadores y producir estragos que aquejen el funcionamiento de los mismos. Cuando un virus se propaga hacia un equipo informático de forma reservada. (Matachana, 2020)
Robo de información	El robo de datos es el acto de robar información digital recopilada en equipos informáticos, correo electrónico. Los datos hurtados pueden incluir información de notas de estudiantes. Esto también se debe a que los beneficiarios utilizan contraseñas debilidades, vulnerabilidades de los sistemas, error humano, descargas comprometidas, información expuesta públicamente. (Canfranc, 2019)

Daño de equipos	Los equipos informáticos en la actualidad son tan potentes que caben inclusive en nuestra mano, sin embargo, de la misma forma son muy frágiles ante factores como golpes, descargas o falta de mantenimiento. Los ordenadores son muy vulnerables ante la falta de limpieza y atención, inclusive perdida de las instalaciones en dónde estos se encuentran ubicados. (R.A, 2022)

Tabla 6: Riesgos

4.5.9 Diseño de instrumento

Se realizó una encuesta al Rector Luis Arteaga de la institución Antonio José de Sucre donde se aplicó el instrumento de encuesta-cuestionario donde se formaron 25 preguntas por los riesgos que por lo general pueden acontecer. En donde fueron robo, incendio, daños de equipos, inundación, virus, robo de información para así poder afectar los riesgos del laboratorio.

Cuestionarios para identificar riesgos	K

Evaluar Riesgo Robo

PREGUNTA	SI	NO	OBSERVACIÓN
1. Existe protectores de hierro en la puerta principal del laboratorio.	X		
2. Se registra el acceso de ingreso del centro de cómputo de personas ajenas	X		
3. Se ha establecido controles de seguridad como es sondeo del carro de la policía cerca de la institución.		X	
4. Las ventanas del laboratorio tienen rejas protectoras.	X		
5. Hay una persona encargada para cuidar el laboratorio.	X		
6. Cerca de la institución hay un UPC	X		
7. Existe control de acceso de contraseña(al ingresar al laboratorio	X		
8. Cuentan con cámaras de seguridad en la puerta de la institución.	X		
9. Tienen accesos personas no autorizadas en hora de la noche para acceder al laboratorio.		X	
10. Se encuentra definido el perímetro de seguridad física.		X	
11. Hay alarmas de antirrobos en la institución		X	
12. El docente registra la lista del estudiante que ingresan al laboratorio.		X	
13. Tiene establecido Controles como es la Cedula de identidad para el acceso al área de TI	X		
14. Para ser movilizados los equipos, software o información fuera de las instalaciones requiere de una autorización	X		
15. Se registran las personas que ingresan y salen del laboratorio	X		
16. Existe una persona responsable a tiempo completo.		X	
17. Cuenta con cámaras de vigilancia el centro de cómputo.	X		
18. Los docentes necesitan autorización para el ingreso		X	
19. Tiene un horario especifico para el uso del laboratorio	X		
20. Hay algún tipo de control como patrullaje en horas de la noche.		X	

Cuestionarios para identificar riesgos	K

Evaluar Riesgo inundación

PREGUNTA	SI	NO	OBSERVACIÓN
1. El laboratorio se encuentra en un lugar libre de inundación.			
2. El techo ha tenido incidentes como agujeros, goteras, fisuras que pueda ingresar el agua.			
3. Cuentan con alarma de humedad			
4. Cuentan con canaletas para los cables que están en el piso para posible inundación.			
5. Se encuentran los CPU en un lugar alto sobre el nivel del suelo.			
6. Las paredes del laboratorio tiene fisuras, partiduras.			
7. Cuentan con un techo impermeable para evitar el paso de agua (Lluvias).			
8. El centro de cómputo se encuentra en parte bajas.			
9. Cuenta con un sisterna de drenaje la institución			
10. El piso del laboratorio cuenta con al menos 30 cm de su piso normal.			
11. Cuentan con protección de hierro al interior de la puerta.			
12. Alguna vez el laboratorio sufrido de inundación.			
13. En la parte de afuera del laboratorio existen lados que almacenen aguas (charcos)			
14. Los materiales con que esta constituidos el piso del centro de cómputo poseen características anti estáticas.			
15. Las ventanas del laboratorio cuentan con protector adicional para lluvias.			
16. Existe un mecanismo para la fuga o derramamiento de líquido (agua).			
17. En alguna ocasión usted ha presenciado o escuchado sobre accidente (inundación) en el laboratorio informático.			
18. El laboratorio cuenta con un teléfono de emergencias para comunicarse con las oficina centrales			
19. En la infraestructura del laboratorio cruza tubería de agua por debajo del piso			
20. La institución está cerca de algún rio			

Ilustración 4 Diseño de instrumento para analizar riesgo

1.5.9. Aplicación

Para poder realizar la investigación se aplicó la herramienta de cuestionario donde aplicaron 25 preguntas para determinar los riesgos dentro del laboratorio

de la institución educativa, mediante la encuesta aplicada al rector donde las respuestas estuvieron constituidas en sí o no. Obteniendo así los resultados de los riesgos como: robo, incendio, daño de equipo, inundación, virus, robo de información las cuales fueron un total de 150 preguntas.

4.5.10 Tabulación

Para lograr la respectiva tabulación de los datos se lo realiza mediante la herramienta excel para alcanzar de manera más ordenada la información obtenida mediante la indagación al rector de la unidad educativa dentro del laboratorio de la institución Antonio José de Sucre.

	RIESGO DE ROBO	
	PREGUNTA	RESPUESTA
1	Existe protectores de hierro en la puerta principal del laboratorio.	0
2	Se registra el acceso de ingreso del centro de cómputo de personas ajenas	1
3	Se ha establecido controles de seguridad como es sondeo del carro de la policía cerca de la	1
4	Las ventanas del laboratorio tienen rejas protectoras.	0
5	Hay una persona encargada para cuidar el laboratorio.	1
6	Cerca de la institución hay un UPC	0
7	Existe control de acceso de contraseña(al ingresar al laboratorio	0
8	Cuentan con cámaras de seguridad en la puerta de la institución.	1
9	Tienen accesos personas no autorizadas en hora de la noche para acceder al laboratorio.	1
10	Se encuentra definido el perímetro de seguridad física.	0
11	Hay alarmas de antirrobos en la institución	0
12	El docente registra la lista del estudiante que ingresan al laboratorio.	1
13	Tiene establecido Controles como es la Cedula de identidad para el acceso al área de TI	0
14	Para ser movilizados los equipos, softw are o información fuera de las instalaciones requiere de una au	1
15	Se registran las personas que ingresan y salen del laboratorio	0
16	Existe una persona responsable a tiempo completo.	0
17	Cuenta con cámaras de vigilancia el centro de cómputo.	0
18	Los docentes necesitan autorización para el ingreso	0
19	Tiene un horario específico para el uso del laboratorio	1
20	Hay algún tipo de control como patrullaje en horas de la noche.	0
21	En alguna ocasión usted ha presenciado a un estudiante o persona entrar al laboratorio informático si	1
22	El uso del laboratorio es exclusivamente para docentes y estudiantes de la institución.	1
23	Existe personal adicional para realizar vigilancia en la institución para el laboratorio.	2
24	La persona que hace vigilancia en la noche tiene acceso al laboratorio.	1
25	Personas particulares con autorización de terceros hacen uso del laboratorio.	0
	TOTAL CONTROLES NO APLICADOS:	1
	TOTAL DE CONTROLES EVALUADOS	24
	TOTAL CONTROLES SEGURIDAD:	11
	TOTAL CONTROLES RIESGO:	13
	PORCENTAJE SEGURIDAD	46%
	PORCENTAJE RIESGO	54%
		100%

Ilustración 5 Tabulación de datos riesgo de robo

	RIESGO INCENDIO	
	PREGUNTA	RESPUESTA
1	El laboratorio cuenta con extintor en caso de incendio.	1
2	Últimamente se ha revisado las conexiones de los equipos del laboratorios	1
3	Las sillas del laboratorio son de fácil consumo al fuego	0
4	Dentro del centro computo existen materiales que puedan ser inflamables	0
5	Los docentes saben el uso del extintor en caso de algún incidente.	1
6	Tienen alguna norma de evacuación para incendio.	0
7	Al suscitarse un incendio el laboratorio cuenta con una salida de emergencia	0
8	La temperatura en que trabajan los equipos es la adecuada bajo la norma que se rigen	1
9	Existen mangueras para apagar incendios	0
10	Cuenta con Swits en caso de emergencia dentro del centro de cómputo.	0
11	Los interruptores de energía están debidamente protegidos y sin obstáculos para alcar	1
12	Cuenta con hidratantes "Conocidos como boca de incendios "dentro de la institución.	0
13	La institución cuenta con transformador de energía propio.	0
14	Tienen breakers de uso exclusivo para el laboratorio.	1
15	Cuentan con conexión energía eléctrica puesta a tierra (Toma de tierra) enterrada en e	1
16	Últimamente se le ha realizado mantenimiento el aire acondicionado.	1
17	Existe señalización visibles para la salida de emergencia	0
18	Las instalaciones de los equipos informáticos se encuentran en buen estado.	1
19	Cuentan con alarma de temperaturas	0
20	El laboratorio cuenta con objetos de fácil consumo al fuego.	2
21	El centro de cómputo cuenta con suficiente espacio para los equipos informáticos.	1
22	El cableado se encuentra correctamente instalados.	1
23	Si cuentan con planos de instalación eléctrica.	1
24	La instalación eléctrica del centro de cómputo es independiente de otras instalacione	1
25	Los dispositivos informáticos cuentan con regulador de voltaje.	1
	TOTAL CONTROLES NO APLICADOS:	1
	TOTAL DE CONTROLES EVALUADOS	24
	TOTAL CONTROLES SEGURIDAD:	14
	TOTAL CONTROLES RIESGO:	10
	PORCENTAJE SEGURIDAD	58%
	PORCENTAJE RIESGO	42%
		100%

Ilustración 6 Tabulación de datos riesgo incendio

Dentro de la tabulación que se realizó en Excel se utilizó una hoja de código para poder identificar de una mejor manera los Riesgos que suscitan en el laboratorio de la institución donde el **1= Representa seguridad, 2= No aplica y el 0= Representa riesgo** para el poder identificar y analizar cada respuesta.

Hoja de códigos	
1	Representa seguridad
2	No aplica
0	Representa riesgo

Ilustración 7 Hoja de códigos

4.5.11 Análisis de Riesgos

Mediante el análisis de riesgo se obtuvieron como resultado que el virus es el único riesgo que posee un nivel muy grave puesto que se presentan con más frecuencia, los estudiantes y docentes suelen pasar archivos infectados o dañados que se pueden propagar de una a varias máquinas y esto ocasiona un daño grave. Mientras que los riesgos como robo, incendio, daño de equipos, inundación, y robo de información no se presentan con mucha frecuencia y da como nivel de riesgo importante, y si llega a ocurrir los docentes pueden seguir impartiendo sus conocimientos a los estudiantes de la institución.

4.6 Matriz de riesgo

MATRIZ DE RIESGOS				
RIESGO	Aparición	Gravedad	Valor del Riesgo	Nivel de Riesgo
ROBO	4	3	12	Importante
INCENDIO	3	3	9	Importante
DAÑO DE EQUIPOS	3	4	12	Importante
INUNDACIÓN	3	4	12	Importante
VIRUS	5	5	25	Muy grave
ROBO DE INFORMACIÓN	5	2	10	Importante

Ilustración 8 Matriz de riesgo

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

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

Ilustración 9 Matriz de riesgo leyenda

4.6.1 Hallazgos

NIVEL DE SEGURIDAD GENERAL

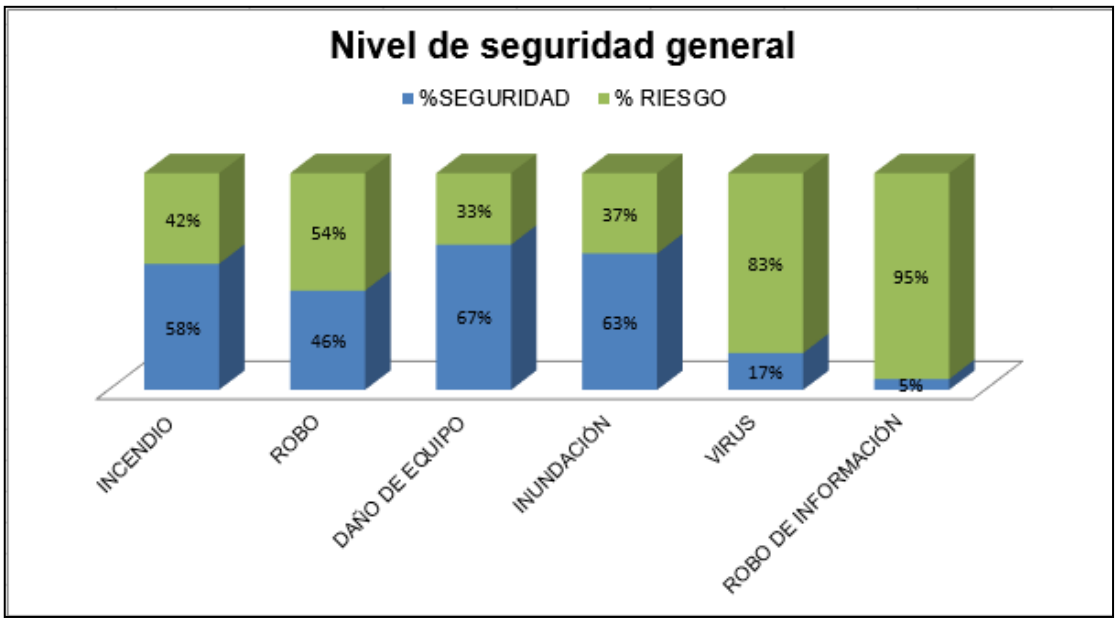
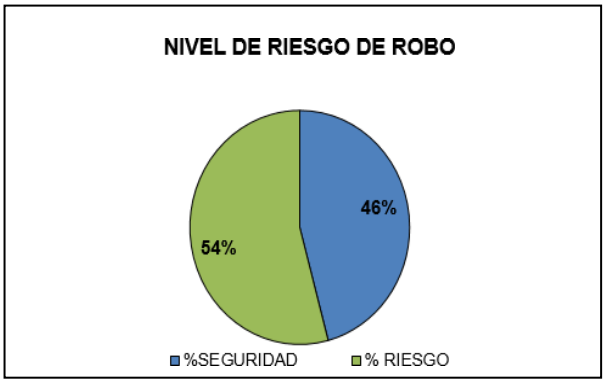


Ilustración 10 Nivel de seguridad general

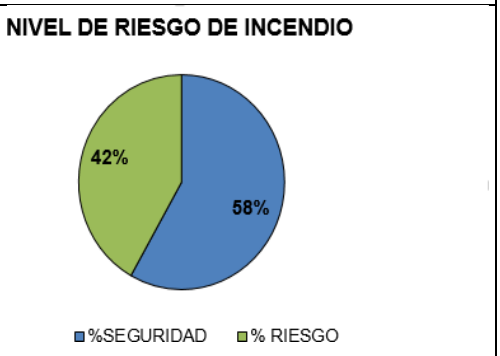
Interpretación: Tomando en consideración el resultado del nivel de seguridad general, se obtiene un nivel alto de riesgo la mayoría correspondiente a virus que afectan las máquinas que se encuentran dentro del laboratorio de la institución, además con 95% se aprecia una exposición muy alta el riesgo de robo de información.

Nivel de Riesgo de Robo

GRÁFICO:	**CAUSAS:**
	• Unas de las causas principales son que no cuentan con protectores de hierro en la puerta principal ni ventana del laboratorio. • No tienen cámaras de seguridad en el laboratorio. • No cuentan con personas que cuiden el laboratorio a tiempo completo. • No llevan un registro de ingreso y salida del laboratorio cuando hacen uso. • No cuentan con una autorización para el ingreso del laboratorio. • No existe patrullaje oficial fuera de la institución en hora de la noche.

Interpretación: Al analizar el nivel de riesgo de robo en el laboratorio de la institución Antonio José de Sucre, se obtiene que el nivel de seguridad es de menor y esto corresponde a un nivel medio de seguridad, representando así un alto nivel de porcentaje en riesgo de robo.

GRÁFICO:



CAUSAS:

- Existen materiales inflamables fáciles en consumarse en el fuego.
- No cuentan con una salida de emergencia.
- No existe implementarías anti incendio (hidratantes, mangueras y alarmas de temperatura).
- No cuentan con la conexión eléctrica adecuada.

Interpretación: Al efectuar el análisis por el nivel de riesgo de incendio, es prescindible el resultado obtenido en un nivel bajo en la cual corresponde a riesgo de incendio.

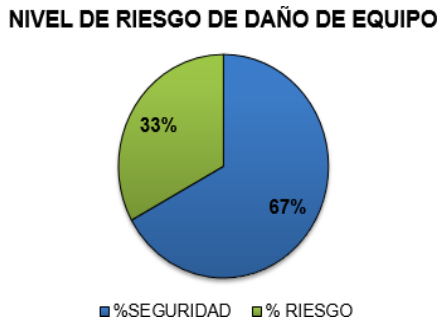
GRÁFICO:	CAUSAS:
	• Cierta temporada los equipos sufren daño en los sistemas. • Mantienen con equipos de varios años en funcionalidad. • Los dispositivos no cuentan con antivirus para protegerse de daños. • No existe con mantenimiento continuo en los equipos. • No cuentan con actualizaciones los sistemas de operativos.
Interpretación: Conforme con el análisis de los resultado obtenido en el nivel riesgo de daño de equipo, se refleja el porcentaje mayor al nivel de seguridad, teniendo en cuenta el nivel medio representado en riesgo de daño de equipo.	

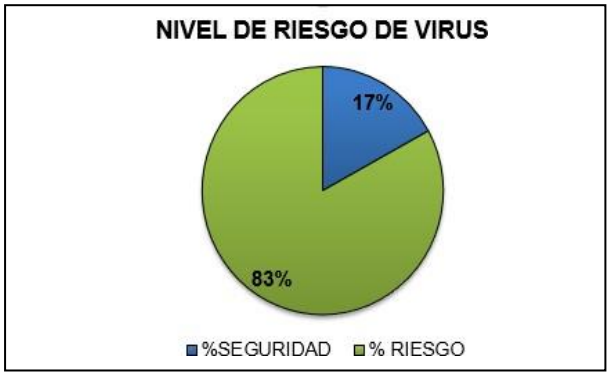
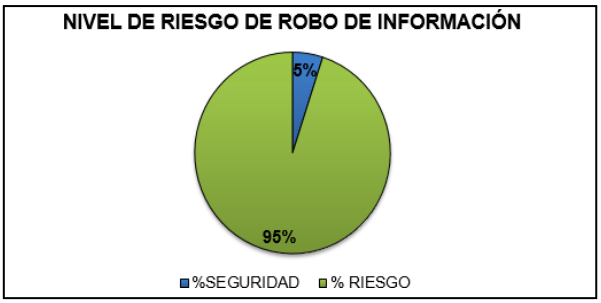
GRÁFICO:	CAUSAS:
	• No existe un departamento que realice el monitoreo pertinente de la red. • No cuentan con control adecuado ante la propagación de los virus en los equipos. • El mal uso de la navegación de la red. • Los equipos informáticos son vulnerables. • Fallas continuas en los sistemas operativos.
Interpretación: De acuerdo con el análisis efectuando mediante la investigación, se pudo verificar el nivel alto en riesgo de virus con un porcentaje considerado más alto al nivel de riesgo de virus que los equipos informáticos mantienen dentro del laboratorio de la institución.	

GRÁFICO:	CAUSAS:
	• No realizan formateos en los dispositivos informático • Ni utilizan una seguridad adecuada en los equipos (contraseñas). • No mantienen aplicaciones actualizadas.

	• No efectúan los respaldos correspondientes de la información almacenada.
Interpretación: En el nivel de riesgo en robo de información, dentro del análisis efectuado los resultados obtenidos mediante la investigación exhaustiva se pudieron recabar que por la falta de formateos en los dispositivos que se encuentran en el laboratorio informático es la principal causa para que terceros intercedan a la información que se manipula dentro de la institución Antonio José de Sucre	

Tabla 7 Nivel de riesgo de robo

4.7 Conclusiones-Opinión de la auditoría

- De acuerdo con el objetivo planteado, se pudo identificar que los principales riesgos de seguridad que se encontraron dentro de la instalación informática fueron incendio, robo, inundación, daño de equipos, virus y robo de información.

- Al finalizar el análisis de riesgo de seguridad informática dentro de la auditoría se detectó el nivel de amenaza alto en virus y robo de información en los equipos informáticos de la institución al nivel de exposición que se encuentra los datos e información.

- La evidencia presentada nos lleva a concluir que el centro de informática del establecimiento educativo no está del todo seguro contra muchas de las amenazas presentadas con anterioridad, pues en base a la investigación se reflejó que su nivel de seguridad es menor al 50%.

- En conclusión, en base a toda la información que se ha recopilado se pudo ejecutar a una guía de recomendaciones que servirán para prevenir desastres en la infraestructura tecnológica dentro de la Unidad Educativa Antonio José de Sucre

4.8 Recomendaciones de la auditoría

- En base al efecto de la auditoría de seguridad informática se exhorta a los docentes y estudiantes de la institución a tomar medidas preventivas de seguridad al momento de utilizar el laboratorio de cómputo y poner en práctica las siguientes buenas prácticas.

- Se recomienda seguir las indicaciones de la guía de buenas prácticas que se formuló para lograr reducir la probabilidad de que ocurran algunos de los riesgos previamente citados, esto con la ayuda de docentes y autoridades que laboran en la unidad educativa.

<table>
<tr><td rowspan="2">Guía de recomendaciones para el laboratorio de la Unidad Educativa Antonio José de Sucre Universidad LaicaEloy Alfaro de Manabí extensión en el Carmen</td><td rowspan="2">Unidad educativa Antonio José de Sucre</td><td colspan="3">Fecha</td><td rowspan="2">PT1</td></tr>
<tr><td>06</td><td>01</td><td>23</td></tr>
<tr><td colspan="5">LEONELA PALADINES</td></tr>
<tr><td colspan="6">Guía de recomendación para laboratorio de la unidad educativa Antonio José de Sucre</td></tr>
<tr><td colspan="6">Objetivo:
• Establecer medidas preventivas para garantizar el funcionamiento seguro del laboratorio de cómputo.</td></tr>
<tr><td>Riesgos</td><td colspan="5">Recomendación</td></tr>
<tr><td rowspan="3">ROBOS</td><td colspan="5">• Instalar alarmas de seguridad para monitorear las actividades realizadas.</td></tr>
<tr><td colspan="5">• Gestionar y solicitar a la policía rondas por el sector.</td></tr>
<tr><td colspan="5">• Instalar sistemas antirrobos para la estar prevenido ante estos sucesos.</td></tr>
<tr><td></td><td colspan="5">• Instalar en puntos estratégicos alarmas contra incendios</td></tr>
</table>

<table>
<tr><td rowspan="3">Guía de recomendaciones para el laboratorio de la Unidad Educativa Antonio José de Sucre Universidad LaicaEloy Alfaro de Manabí extensión en el Carmen</td><td rowspan="3">Unidad educativa Antonio José de Sucre</td><td colspan="3">Fecha</td><td rowspan="2">PT1</td></tr>
<tr><td>06</td><td>01</td><td>23</td></tr>
<tr><td colspan="4">LEONELA PALADINES</td></tr>
<tr><td rowspan="4">INCENDIO</td><td colspan="5">• Instalar extintores en el laboratorio de cómputo de la unidad educativa.</td></tr>
<tr><td colspan="5">• Adecuar con la señaléticas pertinentes con el número de los bomberos</td></tr>
<tr><td colspan="5">• Preparar las salidas de emergencias dentro del laboratorio</td></tr>
<tr><td colspan="5">• Realizar una instalación eléctrica adecuada mediante canaletas</td></tr>
<tr><td rowspan="4">DAÑO DE EQUIPOS</td><td colspan="5">• Contar con programas de restricción de instalación de software</td></tr>
<tr><td colspan="5">• No ingresar alimentos al laboratorio de computo</td></tr>
<tr><td colspan="5">• Que los estudiantes después de hacer uso de equipos dejen apagado.</td></tr>
<tr><td colspan="5">• Cubrir los equipos con protectores adecuados para el polvo y otros.</td></tr>
<tr><td></td><td colspan="5">• Monitorear las actividades de los estudiantes al momento de navegar.</td></tr>
</table>

<table>
<tr><td rowspan="2">Guía de recomendaciones para el laboratorio de la Unidad Educativa Antonio José de Sucre Universidad LaicaEloy Alfaro de Manabí extensión en el Carmen</td><td rowspan="2">Unidad educativa Antonio José de Sucre</td><td colspan="3">Fecha</td><td rowspan="2">PT1</td></tr>
<tr><td>06</td><td>01</td><td>23</td></tr>
<tr><td colspan="5">LEONELA PALADINES</td></tr>
<tr><td rowspan="6">VIRUS</td><td colspan="5">• No ingresar a los equipos informáticos, flash memory sin ser primero analizadas.</td></tr>
<tr><td colspan="5">• Proteger con antivirus los dispositivos informáticos.</td></tr>
<tr><td colspan="5">• No descargar archivos de páginas no recomendadas</td></tr>
<tr><td colspan="5">• Respaldar los archivos guardado en la nube.</td></tr>
<tr><td colspan="5">• Evitar abrir enlaces o link no seguros en los correos u otros lugares.</td></tr>
<tr><td colspan="5">• Usar contraseñas seguras para la red de internet</td></tr>
<tr><td rowspan="3">ROBO DE</td><td colspan="5">• Instalar programas de licencia original.</td></tr>
<tr><td colspan="5">• Realizar instalaciones eléctricas adecuada</td></tr>
<tr><td colspan="5">• Dar capacitaciones a los docentes para el buen uso de las herramientas tecnológicas</td></tr>
</table>

<table>
<tr><td rowspan="2">Guía de recomendaciones para el laboratorio de la Unidad Educativa Antonio José de Sucre Universidad LaicaEloy Alfaro de Manabí extensión en el Carmen</td><td rowspan="2">Unidad educativa Antonio José de Sucre</td><td colspan="3">Fecha</td><td rowspan="2">PT1</td></tr>
<tr><td>06</td><td>01</td><td>23</td></tr>
<tr><td colspan="5">LEONELA PALADINES</td></tr>
<tr><td rowspan="2">INFORMACIÓN</td><td colspan="5">• Utilizar distintas contraseñas al momento de utilizar las aplicaciones</td></tr>
<tr><td colspan="5">• No compartir datos personales a desconocidos ni por redes sociales</td></tr>
<tr><td rowspan="3">INUNDACIÓN</td><td colspan="5">• Limpiar zanjas cercas del laboratorio</td></tr>
<tr><td colspan="5">• Evitar dejar basura cerca de alguna canaleta y limpiar el tejado del laboratorio</td></tr>
<tr><td colspan="5">• Movilizar a un lugar alto los equipos informáticos</td></tr>
</table>

Conclusiones

- En base a lo expuesto con anterioridad, se puede deducir que la información que se obtuvo de fuentes tales como libros y artículos científicos mejoró el entendimiento de cómo funciona una auditoría dentro de un entorno informático, lo que permitió que las bases para la realización de este proyecto de investigación fueran solidas al momento de aplicar la teoría extraída de tales documentos.

- Tras el análisis, se puede concluir que la información proporcionada por los involucrados en este estudio a través de las técnicas e instrumentos como la encuesta y entrevista fue de gran ayuda, pues proporcionaron información importante de cómo funcionaban las operaciones dentro de la infraestructura tecnológica y con ello se pudiera evaluar si existía un problema que se pudiera solucionar.

- Se puede concluir, que mediante el informe de auditoría que se realizó se dejó en evidencia que la infraestructura tecnológica de la unidad educativa contaba con ciertos riesgos de seguridad importantes, por lo cual fue necesario realizar una guía de recomendaciones para que se pongan en práctica y así reducir la probabilidad de que estos ocurran o se sigan incrementando.

Recomendaciones

- A la Unidad Educativa Antonio José de Sucre realizar una revisión cada seis meses de la infraestructura tecnológica de la institución basándose en las recomendaciones dadas en la guía que se le proporciono a la institución.

- Se recomienda al encargado de la infraestructura tecnológica crear protocolos que fomenten el estudio de seguridad informática para que mediante la aplicación periódica de estos se pueda aumentar la detección de riesgos dentro del establecimiento educativo.

- A la Carrera de Tics que sigan haciendo auditorías en diferentes instituciones del país para que observen a que riesgo están expuestos como institución y puede prevenir para que a futuro no sea un problema grave.

Bibliografía

ACISSI. (2018). *Seguridad informática: Hacking Ético: conocer el ataque para una mejor defensa.* Barcelona: ENI.

Aguilera Lopéz, P. (2021). *Aplicaciones ofimáticas: Ciclos Formativos.* EDITEX.

Alegre Ramos, M. D. (2019). *Sistemas operativos monopuestos 2a edicion.* Paraninfo.

Amutio Gómez, M. A. (2017). *Metodología de Análisis y Gestión de riesgos de los sistemas de información.* Ministerio de hacienda y administraciones públicas.

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). *Ciberseguridad.* Consejo superior de Investigaciones Científicas.

Baena Paz, G. M. (2017). *Metodología de la investigación (3a.ed.).* Ciudad de México: La dimensión metodológica del diseño de la investigación científica.

Barreneche, I. O. (2020). *Protección y Seguridad Contra Incendio.* Aútonoma de Buenos Aires: 1era ed.

Canfranc. (2019). *Ciberseguridad: Protegiendo la información vunerables (Vol.2).* Bogotá: Fundación Teléfonica.

Chaos García, D., Gómez Palomo, S. R., Letón Molina, E., San Juan, C. R., & Rubio Gonzáles, M. Á. (2017). *Introducción a la informática básica.* Madrid: Universidad Nacional de Educación a Distancia.

Chicano tejada, E. (2016). *Auditoría de seguridad informática.* Málaga: Ic editorial .

Concejero Barbancho, J., Benjumea Mondéjar, J., Rivera Romero, O., Romero Ternero, M., Ropero Rodriguéz, J., Sánchez Antón, G., & Sivianes Castillo , F. (2020). *Redes locales 3era edicion.* Parainfo.

Cuenca, N. (2018). *Prevención de riesgos laborales: sector Servicios.* España: : riesgos específicos del trabajo del personal informático (2a. ed.).

Fernández Ramírez, L. O. (2016). *Auditoria informática.* Academia.

Gris, M. (2018). *Iniciación a internet.* Barcelona: ENI.

Hernández-Rodríguez, A. A., Argüelles-Pascual, V., & Palacion, R. H. (2021). Métodos empíricos de la investigación. *Ciencia Huasteca*, 2.

Jiménez, L. M., Puerto, R., & Payá, L. (2017). *Sistemas distribuidos: Arquitectura y aplicaciones.* Universitas Miguel Hernández.

Lederkremer, M. (2020). *REDES INFORMATICAS Avanzado.* Buenos aires: Six ediciones.

Loor Venegas, L., & Esparza Bernal, F. (2018). *Guía metodológica para la evaluación técnica informática de la implementación de educación y capacitación virtual- COBIT 5.* Alicante: Área de innovación y desarrollo.

Maillo Fernández, J. A. (2022). *Hackers: Técnicas y herramientas para atacar y defendernos.* Bogotá: Ra-ma.

Matachana, Y. L. (2020). *Los virus informáticos: Una amenaza para la sociedad.* Cuba: Editorial Universitaria .

Maya, R. P. (2017). *Los cibercrimenes: un nuevo paradigma de criminalidad.* Bogotá: Ibañez Careño I.

Molero Prieto, X. (2016). *Un viaje a la historia de la informática .* Valencia: Universitat politécnica de Valencia.

Moro Vallina, M. (2021). *Ofimática y proceso de la información 2da edición.* Paraninfo.

Muñoz López, F. J. (2017). *Instalación y actualizacion de sistemas operativos.* Parainfo.

Palacios Postigo, A. (2020). *Seguridad Informática.* Asturias: Paraninfo.

Pardo Clemente, E. (2017). *Microinformática de gestión.* Oviedo: Universidad de Oviedo.

Paz Abdo, K. S., & Torres, M. (2016). *Métodos de recolección de datos para una investigación.* Universidad Rafael Landívar.

Pereyra, L. E. (2020). *Informática I.* Ciudad de México: Vlik.

R.A, M. (2022). *Modelo Metrópoli de Gerencia Social.* Bogotá: Ediciones Nandela .

Reyes, B. (2020). *Metodología de la investigación edicion Gamma 2020.* Aguascalientes: Universidad autónoma de Aguascalientes.

Rodriguez Jiménez, A., & Pérez Jacinto , A. O. (2017). Métodos científicos de indagación y de construccion del conocimiento . *Revista Ean*, 22.

Romero Castro, M. I., Figueroa Morán, G. L., Naverrete Vera, S. D., Cruzatty Álava, E. J., Parrales Anzúles, R. G., Mero Álava, C. J., . . . Merino Castillo, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante: Área de innovación y desarrollo.

Sanchez Cascado , G., & Mingo , G. (2017). *Ordenadores, programas informáticos e internet (operaciones administrativas) y documentacion sanitaria.* Editex.

Sánchez estella, Ó. (2021). *Sistema operativo, busqueda de información: Internet/Intranet y correo.* Paraninfo.

Troncoso-Pantoja, C., & Amaya-Placencia, A. (2016). Entrevista: Guía practica para la recoleccion de datos cualitativos en investigación de salud. *Facmed*, 4.

Urbina Baca, G. (2017). *Introduccion a la seguridad informática.* Nuevo León: Patria.

Vasconcelos Santillán, J. (2018). *Introducción a la computación.* Patria.

Weber, J. (2020). *Fundamentos de informática.* Córdoba: Universitas.

Anexos

Entrevista

Objetivo: Tiene como objetivo principal recabar datos de los principales riesgos que hay en el laboratorio de la institución Antonio José de Sucre.

Dirigida a: Rector de la institución educativa Ing. Luis Arteaga

Entrevistador: Leonela Paladines

1. **¿Sabe si existe personal que se encargue del departamento de tics en la unidad educativa?**
2. **¿Existen registros del inventario que posee la unidad educativa en cuanto a equipos tecnológicos?**
3. **Conoce la cantidad de equipos informáticos que posee la institución.**
4. **¿Se lleva algún tipo de control en mantenimiento a los equipos que se usan en la institución educativa?**
5. **¿Cómo manejan la seguridad de los datos tanto de estudiantes como del personal administrativo?**
6. **¿Posee algún plan de riesgos dentro de los laboratorios de informática en caso de que se presente uno?**
7. **¿Existen alguna política que se deba respetar al momento de acceder a los laboratorios de informática?**
8. **¿Cómo protegen los equipos informáticos de problemas como exceso de corriente o sobrecalentamiento?**
9. **¿Las áreas donde se trabajan con equipos informáticos son seguras?**

10. **¿Cada sala informática cuenta con espacio suficiente para alumnos y equipos?**

Anexo 1 : Diseño de la estructura de la entrevista

Encuesta dirigida a docente y rector de la institución

Encuesta

1. **¿La institución cuenta con un departamento encargado a las tecnologías de la información?**
   - **Si**
   - **No**

2. **¿Se lleva un inventario de los dispositivos informáticos que posee la institución?**
   - **Si**
   - **No**

3. **¿Seleccione el sistema operativo que poseen las computadoras de la institución?**
   - **Windows**
   - **Linux**
   - **Mac OS**
   - **UNIX**

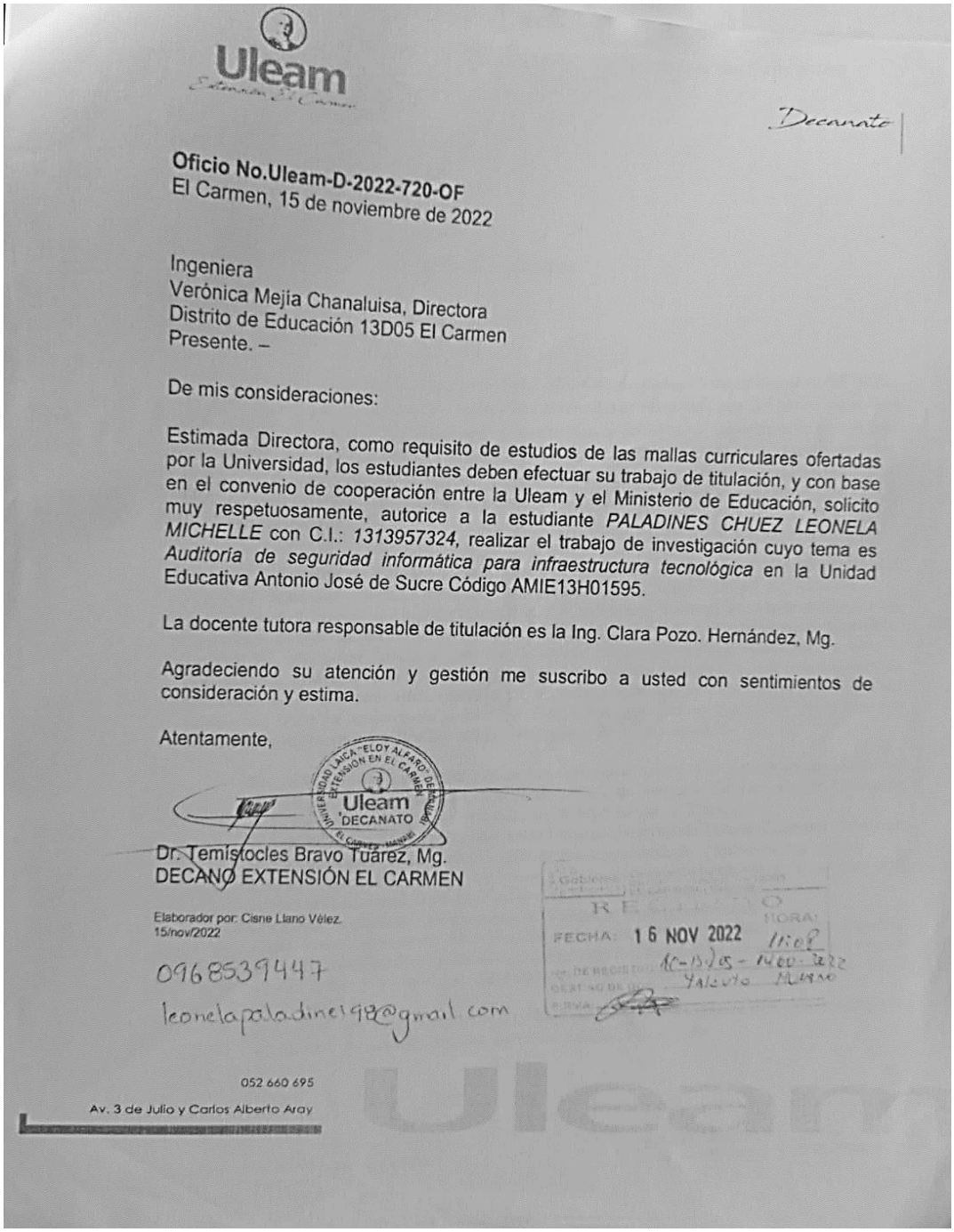
4. **¿Con que frecuencia se hace mantenimiento a los dispositivos informáticos de la institución?**
   - **Siempre**
   - **Casi siempre**
   - **Nunca**

5. **¿Alguna vez se ha extraviado información de los computadores de la institución?**
   - **Si**
   - **No**

6. **¿Los datos de todos los estudiantes y personal administrativo de la institución se encuentran protegidos por alguna contraseña de seguridad?**
   - **Si**
   - **No**

Anexo 2 : Encuesta dirigida a los docentes

Oficio de la ULEAM al Distrito de Educación 13D05 El Carmen



Uleam
Extensión El Carmen

Decanato

Oficio No.Uleam-D-2022-720-OF
El Carmen, 15 de noviembre de 2022

Ingeniera
Verónica Mejia Chanaluisa, Directora
Distrito de Educación 13D05 El Carmen
Presente. –

De mis consideraciones:

Estimada Directora, como requisito de estudios de las mallas curriculares ofertadas por la Universidad, los estudiantes deben efectuar su trabajo de titulación, y con base en el convenio de cooperación entre la Uleam y el Ministerio de Educación, solicito muy respetuosamente, autorice a la estudiante *PALADINES CHUEZ LEONELA MICHELLE* con C.I.: *1313957324*, realizar el trabajo de investigación cuyo tema es *Auditoría de seguridad informática para infraestructura tecnológica* en la Unidad Educativa Antonio José de Sucre Código AMIE13H01595.

La docente tutora responsable de titulación es la Ing. Clara Pozo. Hernández, Mg.

Agradeciendo su atención y gestión me suscribo a usted con sentimientos de consideración y estima.

Atentamente,

Uleam
DECANATO

Dr. Temístocles Bravo Tuárez, Mg.
DECANO EXTENSIÓN EL CARMEN

Elaborador por: Cisne Llano Vélez.
15/nov/2022

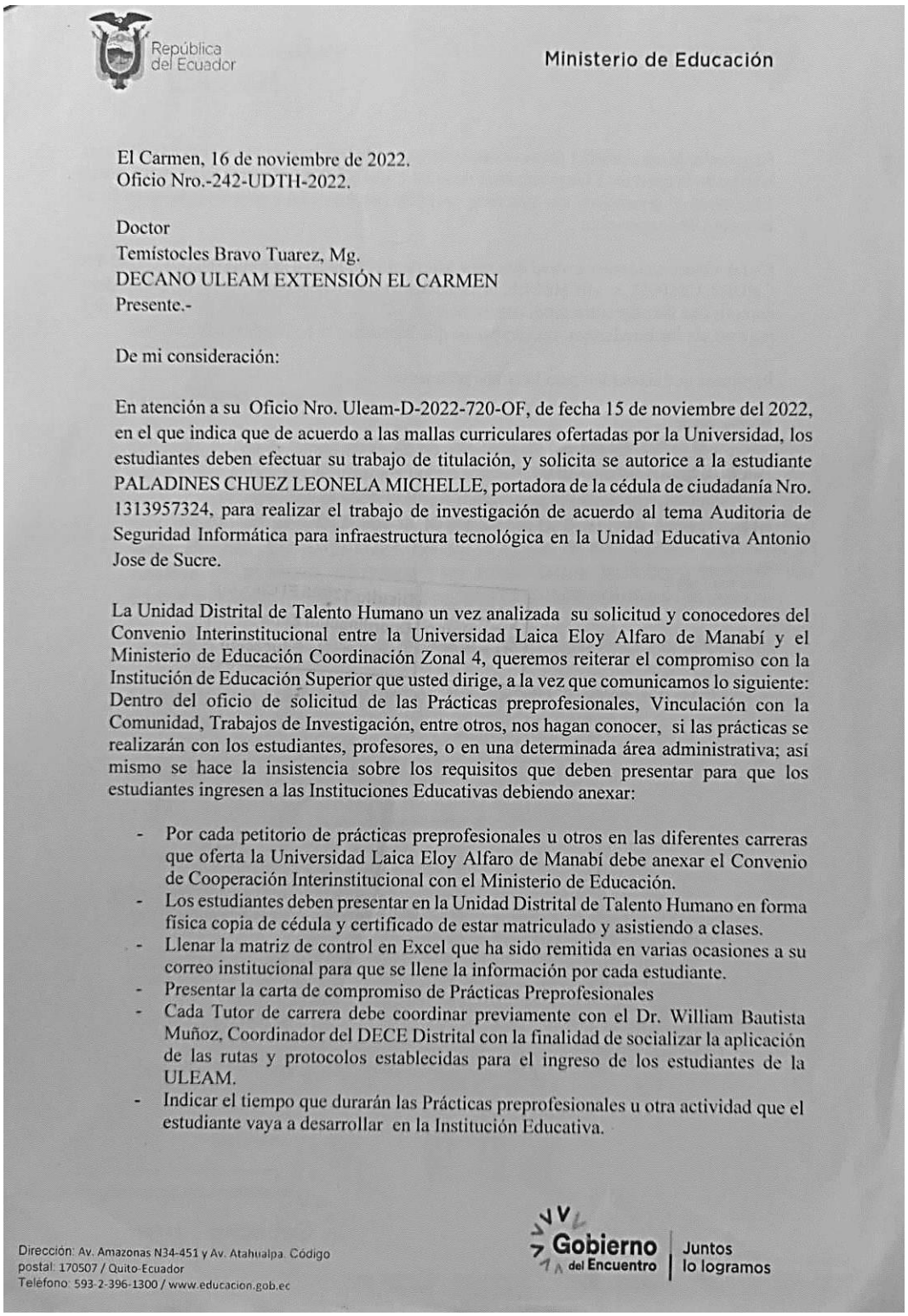
0968539447
leonelapaladines98@gmail.com

RECIBIDO
FECHA: 16 NOV 2022 HORA: 11:08

052 660 695
Av. 3 de Julio y Carlos Alberto Aray

Anexo 3: Oficio de la Uleam al Distrito de Educación 13D05 El Carmen

Autorización de la unidad Distrital del departamento del talento humano



República del Ecuador

Ministerio de Educación

El Carmen, 16 de noviembre de 2022.
Oficio Nro.-242-UDTH-2022.

Doctor
Temístocles Bravo Tuarez, Mg.
DECANO ULEAM EXTENSIÓN EL CARMEN
Presente.-

De mi consideración:

En atención a su Oficio Nro. Uleam-D-2022-720-OF, de fecha 15 de noviembre del 2022, en el que indica que de acuerdo a las mallas curriculares ofertadas por la Universidad, los estudiantes deben efectuar su trabajo de titulación, y solicita se autorice a la estudiante PALADINES CHUEZ LEONELA MICHELLE, portadora de la cédula de ciudadanía Nro. 1313957324, para realizar el trabajo de investigación de acuerdo al tema Auditoria de Seguridad Informática para infraestructura tecnológica en la Unidad Educativa Antonio Jose de Sucre.

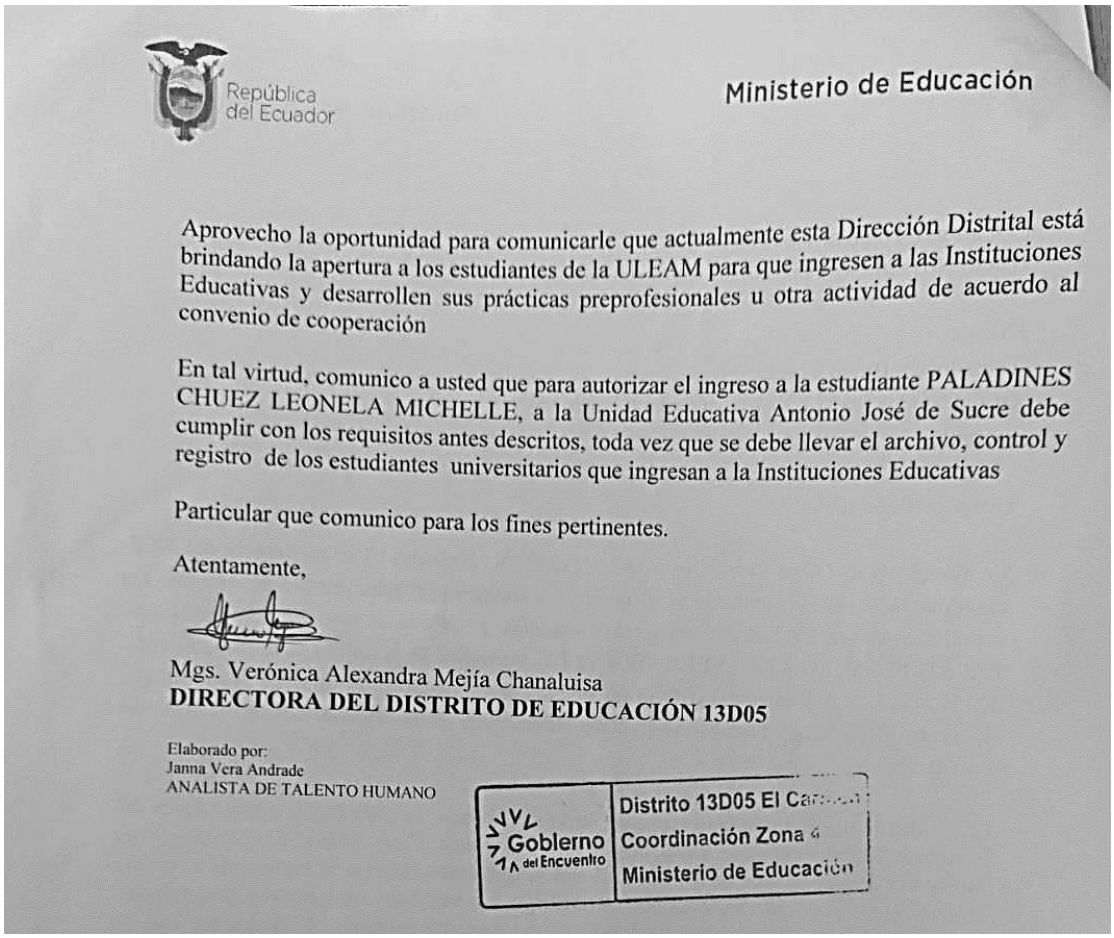
La Unidad Distrital de Talento Humano un vez analizada su solicitud y conocedores del Convenio Interinstitucional entre la Universidad Laica Eloy Alfaro de Manabí y el Ministerio de Educación Coordinación Zonal 4, queremos reiterar el compromiso con la Institución de Educación Superior que usted dirige, a la vez que comunicamos lo siguiente: Dentro del oficio de solicitud de las Prácticas preprofesionales, Vinculación con la Comunidad, Trabajos de Investigación, entre otros, nos hagan conocer, si las prácticas se realizarán con los estudiantes, profesores, o en una determinada área administrativa; así mismo se hace la insistencia sobre los requisitos que deben presentar para que los estudiantes ingresen a las Instituciones Educativas debiendo anexar:

- Por cada petitorio de prácticas preprofesionales u otros en las diferentes carreras que oferta la Universidad Laica Eloy Alfaro de Manabí debe anexar el Convenio de Cooperación Interinstitucional con el Ministerio de Educación.
- Los estudiantes deben presentar en la Unidad Distrital de Talento Humano en forma física copia de cédula y certificado de estar matriculado y asistiendo a clases.
- Llenar la matriz de control en Excel que ha sido remitida en varias ocasiones a su correo institucional para que se llene la información por cada estudiante.
- Presentar la carta de compromiso de Prácticas Preprofesionales
- Cada Tutor de carrera debe coordinar previamente con el Dr. William Bautista Muñoz, Coordinador del DECE Distrital con la finalidad de socializar la aplicación de las rutas y protocolos establecidas para el ingreso de los estudiantes de la ULEAM.
- Indicar el tiempo que durarán las Prácticas preprofesionales u otra actividad que el estudiante vaya a desarrollar en la Institución Educativa.

Dirección: Av. Amazonas N34-451 y Av. Atahualpa. Código postal: 170507 / Quito-Ecuador
Teléfono: 593-2-396-1300 / www.educacion.gob.ec

Gobierno del Encuentro | Juntos lo logramos

Anexo 4: Autorización de la Unidad Distrital de talento humano



República del Ecuador

Ministerio de Educación

Aprovecho la oportunidad para comunicarle que actualmente esta Dirección Distrital está brindando la apertura a los estudiantes de la ULEAM para que ingresen a las Instituciones Educativas y desarrollen sus prácticas preprofesionales u otra actividad de acuerdo al convenio de cooperación

En tal virtud, comunico a usted que para autorizar el ingreso a la estudiante PALADINES CHUEZ LEONELA MICHELLE, a la Unidad Educativa Antonio José de Sucre debe cumplir con los requisitos antes descritos, toda vez que se debe llevar el archivo, control y registro de los estudiantes universitarios que ingresan a la Instituciones Educativas

Particular que comunico para los fines pertinentes.

Atentamente,

Mgs. Verónica Alexandra Mejía Chanaluisa
DIRECTORA DEL DISTRITO DE EDUCACIÓN 13D05

Elaborado por:
Janna Vera Andrade
ANALISTA DE TALENTO HUMANO

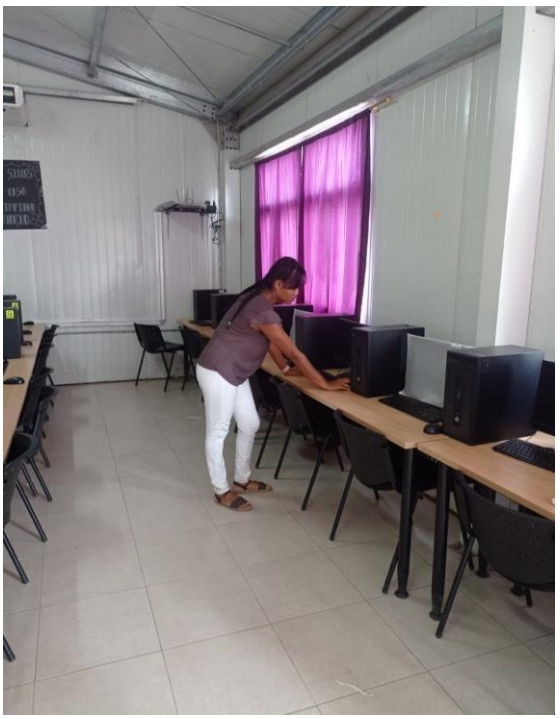
Gobierno del Encuentro
Distrito 13D05 El Ca...
Coordinación Zona 4
Ministerio de Educación

Anexo 5: Autorización de la Unidad Distrital de talento humano

Entrevista al rector de la unidad Educativa Antonio José de Sucre

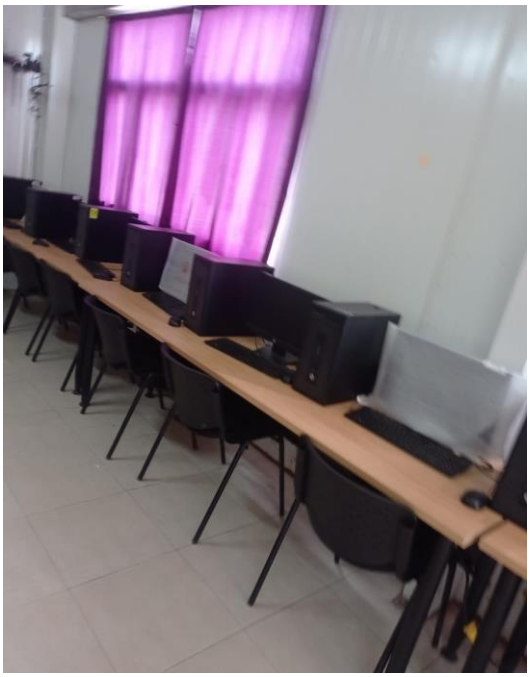
Anexo 6: Entrevista al Ing. Luis Arteaga, rector de la Unidad Educativa

Revisión del Laboratorio de Computo de la institución Antonio José de Sucre



Anexo 7: Revisión del centro de cómputo

Inspección del Centro de Computo de la Institución Educativa Antonio José de Sucre.



Anexo 8: Laboratorio de la institución Antonio José de Sucre

Infraestructura del laboratorio la Unidad Educativa Antonio José de Sucre

Anexo 9: Infraestructura Tecnológica de la Unidad Educativa