UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PROPUESTA DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA UNIVERSIDAD CATÓLICA DE CUENCA, CAMPUS AZOGUES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: DIEGO EDUARDO LEÓN PACHECO

DIRECTOR: ING. CÉSAR ÁLVARO CORONEL GONZÁLEZ

AZOGUES – ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PROPUESTA DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA UNIVERSIDAD CATÓLICA DE CUENCA, CAMPUS AZOGUES.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: DIEGO EDUARDO LEÓN PACHECO

DIRECTOR: ING. CÉSAR ÁLVARO CORONEL GONZÁLEZ

AZOGUES - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARACIÓN DE AUTORÍA Y RESPONSABILIDAD

Universidad Católica de Cuenca	DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD	CÓDIGO: F – DB – 34 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

Declaratoria de Autoría y Responsabilidad

Diego Eduardo León Pacheco portador de la cédula de ciudadanía Nº **0301961819**. Declaro ser el autor de la obra: "**Propuesta de un Laboratorio de Informática Forense en la Universidad Católica de Cuenca, Campus Azogues"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Azogues, **18 de enero de 2023**

F: .....

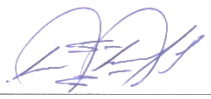
Diego Eduardo León Pacheco

C.I. **0301961819**

CERTIFICACIÓN

CERTIFICACIÓN DEL TUTOR

Certifico que el presente trabajo fue desarrollado por el estudiante Diego Eduardo León Pacheco, bajo la supervisión del tutor designado (Ing. César Coronel González); la investigación propuesta sirve como requisito previo a la obtención del título de Ingeniero en Sistemas de Información, el tema **"PROPUESTA DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA UNIVERSIDAD CATÓLICA DE CUENCA, CAMPUS AZOGUES"** cumple con todas las observaciones realizadas por el tribunal evaluador, por lo que las ideas, opiniones vertidas en el presente, son de exclusiva responsabilidad de los autores.



Ing. César Coronel González.

DIRECTOR

DEDICATORIA

Mi trabajo de tesis va dedicado con gran cariño y amor a mis padres: Miguel León y María Pacheco. Gracias por formarme como persona, por su apoyo y por enseñarme a seguir adelante aun cuando exista adversidades.

A mi papá, que a pesar de la distancia me alentó, apoyo y, sobre todo, agradezco todos sus esfuerzos que hizo durante toda mi vida académica.

A mi mamá, quien me dio la fuerza para seguir adelante, agradezco todos los sacrificios que hizo por mí y los consejos que me brindo.

Estoy eternamente agradecido con ustedes.

AGRADECIMIENTOS

Primeramente, quiero agradecer a Dios por la sabiduría y entendimiento que me ha otorgado para realizar este trabajo de investigación.

Agradezco a mi sobrino: Andrés, quien estuvo ahí para echar algunas risas en los momentos difíciles.

Agradezco a mis hermanos: Bertha, Marco y Fernando que a pesar de la distancia me dieron aliento para seguir esforzándome.

Quiero agradecer a mi tutor; Ing. César Álvaro Coronel por orientarme, brindar conocimiento y por las sugerencias proporcionadas para la culminación de esta investigación.

Quiero agradecer a todos los catedráticos de la Universidad Católica de Cuenca, quienes fueron una parte importante en mi formación como profesional.

Agradezco a mis compañeros, quienes me apoyaron y compartieron sus esfuerzos para cumplir con las metas planteadas.

Por último, pero no por ello menos importante, agradezco a mí mismo por no rendirme y esforzarme en todo lo que me he propuesto.

RESUMEN

La informática forense es de gran importancia para la investigación, rastreo y enjuiciamiento de los delincuentes informáticos, cuya finalidad es encontrar evidencias significativas que relacionen al autor con el delito, por medio del uso de varias técnicas y herramientas tecnológicas para hacer esto posible. En este presente proyecto de tesis tiene como objetivo proponer un Laboratorio de Informática Forense (LIF) con el fin que permita analizar, investigar y estudiar los diferentes tipos de delitos informáticos que afectan al país, a la vez de proporcionar pruebas digitales ante el proceso legal descrito en el Código Orgánico Integral Penal del Ecuador relacionado con los ciberdelitos, para el cuál se sugieren diferentes herramientas tanto de software como de hardware que conforman un LIF, acorde a las especificaciones de los equipos que disponen los laboratorios de informática dentro de la Universidad, también se propone diferentes lineamientos para la creación de estos tipos de laboratorios con el objetivo de fortalecer el diseño propuesto, de la misma forma, se menciona un personal adecuado para su funcionamiento, metodologías a seguir y presupuesto necesario para adquirir dichas herramientas.

El proyecto también tiene la intensión, diseñar un laboratorio de informática forense, mismo que podría beneficiar tanto profesores como estudiantes en el campo de la enseñanza y aprendizaje, favoreciendo así el aumento de profesionales en el área y consecuentemente satisfacer la necesidad social de poder acudir a un experto en caso de ser víctima de algún delito informático.

Palabras clave: delitos informáticos**,** laboratorio de informática forense, metodología de análisis forense, informática forense

ABSTRACT

Digital forensics is crucial for investigating, tracking, and prosecuting cybercriminals. It aims to find significant evidence linking the perpetrator to the crime through various techniques and technological tools. This thesis project seeks to propose a Digital Forensic Laboratory (DFL) to analyze, investigate, and study the different types of cybercrimes that affect people while providing digital evidence before the legal process described in the Comprehensive Organic Criminal Code of Ecuador related to cybercrime. For this, different tools have suggested software and hardware for creating a FL are suggested according to the specifications of the equipment available in the computer laboratories of the University.; the project also offers other guidelines for developing these spaces, intending to strengthen the proposed design. Similarly, the need for adequate staff for its operation, methodologies, and the required budget to acquire these tools are mentioned.

The project also intends to design a computer forensics laboratory, which could benefit teachers and students in the teaching and learning process, favoring the increase of professionals in the area and consequently satisfying the social necessity to consult an expert in case of being a victim of a computer crime.

Keywords: Computer crimes, computer forensics laboratory, forensic analysis methodology, computer forensics

ÍNDICE

Lista de Tablas

Lista de Figuras

Lista de Anexos

CAPITULO 1

1.1 Introducción

Hoy en día la tecnología ha evolucionado de una manera increíble, tanto que cada aspecto de nuestras vidas se encuentra relacionado con las TICs (Tecnología de la información y la comunicación), innovándose a sí misma cada vez más para lograr cubrir las necesidades de las personas; provocando que su propio crecimiento se convierta en inseguridad y más si se habla de conexiones a internet, donde es más frecuente encontrar todo tipo de vulnerabilidades donde cualquier individuo puede cometer diferentes tipos de delincuencia informática [1].

Es así que surge la Informática forense (IF), donde poco a poco va tomando más importancia debido a que funciona como un medio para poder poner en evidencia los delitos informáticos que se presenten. Sin embargo, la IF no está destinada a prevenir delitos, sino más bien ayuda a la obtención de pruebas que demuestren donde, cuando, como y/o quien comete estos crímenes o fraudes [2].

Es importante mencionar que, durante una investigación forense, se hace uso de una gran cantidad de herramientas y técnicas, donde además de facilitar los procesos que conlleva tal tarea, contribuyen a obtener mejores resultados, a la par de contar con profesionales que garanticen la transparencia de la investigación.

En el presente documento se considera temas sobre la informática forense y las herramientas que se utilizan durante los procesos de obtención de evidencia, además del personal que podría conformar un laboratorio de informática forense, para aquellos que necesitan consultar estos aspectos. De la misma manera, forma parte de la propuesta para el diseño de un LIF donde se pueda identificar, preservar y analizar evidencias digitales.

En el capítulo 2, se analizan conceptos relacionados a la informática forense, características del delito informático, también se describe distintos tipos de ataques que realizan los ciberdelincuentes, ejemplos de delitos informáticos, el derecho informático, los artículos del Código Orgánico Integral Penal Ecuatoriano (COIP) relacionados con los ciberdelitos, entre otros, mismos que son valiosos para la investigación.

En el capítulo 3, se describen los equipos tecnológicos que podrían conformar los distintos laboratorios de informática de la Universidad Católica de Cuenca, Campus Azogues, con el fin de determinar cuál de los laboratorios llegaría a ser la mejor opción para diseñar un laboratorio de informática forense, a la vez que se aprovecharía los recursos que disponen dentro de los mismos.

En el capítulo 4, se mencionarán consideraciones generales para el diseño del LIF, normas relacionadas con la informática forense, guías de buenas prácticas y metodologías, de igual manera, se propondrá un modelo propio para trabajar en la investigación forense, como también el personal necesario para el funcionamiento del mismo. Por último, se realizará un diseño adecuado de un laboratorio enfocado en esta área pericial, con una propuesta de adquisición de herramientas de software y hardware para consolidar el diseño.

En el capítulo 5, se presentan las conclusiones y recomendaciones correspondientes al trabajo de investigación.

1.2 Planteamiento del problema

Hoy en día, el avance tecnológico ha hecho posible un sin número de innovaciones y más aún si consideramos que está al alcance de todos, existe mayor consumo de nuevos servicios; que de una u otra manera, han hecho más sencilla la vida cotidiana de las personas, tanto en el ámbito laboral, así como también en lo personal, la educación, las

comunicaciones, etc., existiendo mayores posibilidades de que la información pueda ser vulnerada y en mucho de los casos expropiada a quien le pertenece. Estos delitos son cada vez más frecuentes, provocando pérdidas económicas, daños contra entidades gubernamentales, empresas y personas.

Conforme ha crecido la tecnología se ha incrementado la generación y el almacenamiento de información como datos personales y/o confidenciales en diferentes lugares: Base de datos, redes sociales, programas informáticos, computadoras personales, smartphones, etc., mismos que pueden ser fácilmente manipulables, interceptados, duplicados o redirigidos por personas con gran conocimiento en la informática, cuyo objetivo es el de cometer algún hecho delictivo con la información extraída.

Debemos tener presente que, existen diferentes tipos de delitos informáticos como, la negación de servicios, piratería, ataque a datos, hackeo, phishing, ransomware, redirección de paquetes, virus, fraudes, grooming entre otras más, que son perpetrados por hackers, crackers, bucaneros, desarrolladores de virus que buscan como motivos la extorción o cometer actos inmorales.

En Ecuador una gran cantidad de delitos han sido denunciados en el año 2018 y 2019, cuyos casos registrados rondaban entre 9,571 y 10,279 respectivamente, hasta el mes de agosto del 2020 ya se registraban 5,048 casos y para el periodo de enero a septiembre del 2021 apenas se abrieran 1,265 investigaciones, esto debido a que, muchos de estos cargos no son investigados por falta de profesionales o laboratorios especializados para estos casos [3], [4].

Entonces, vemos que un laboratorio de informática forense podría ser la solución a los problemas anteriormente mencionados, que ayuden a analizar y salvaguardar las evidencias, teniendo como objetivo que un perito informático pueda emitir informes

judiciales o extrajudiciales para emplear cualquier proceso penal dentro del marco legal del país y así lograr cubrir exigencias de la sociedad.

Cabe mencionar que, en la provincia del Cañar y en especial en la Universidad Católica de Cuenca, Campus Azogues, donde a pesar de contar con equipos y una base estructural adecuada, no se cuenta con laboratorios de informática forense, donde se pueda obtener, proteger y preservar la evidencia digital a través de la tecnología, misma que logra conservar la integridad de los procedimientos durante estas tareas., de igual forma, por medio de seminarios: recrear, investigar y analizar casos de delitos informáticos, donde se busque alentar a los estudiantes a interesarse más por esta ciencia, donde cada vez más organizaciones demandan conocimiento, habilidades y capacidades en el área de la informática forense.

1.3 Justificación

La intención del proyecto es proponer el diseño de un laboratorio de informática forense con herramientas e infraestructura necesaria tanto como software y hardware para lograr cumplir con una investigación digital acorde a los marcos legales que regulan el país.

Hacer un estudio de esta área nos permitirá saber el alcance de esta ciencia, sus características, herramientas que se emplean durante los procesos de la recolección de pruebas y el tratamiento de las evidencias. Para lograr esta investigación se procederá a revisar fuentes bibliográficas, documentos, revistas, páginas web, artículos con el objetivo de adquirir conocimientos e información necesaria para lograr llevar a cabo la propuesta.

Un LIF favorecerá en gran medida a la población debido a que en los laboratorios se podrían analizar casos de fraudes o delitos que se hayan ocasionado o de igual forma

reabrir casos archivados, con el fin de otorgar pruebas necesarias que puedan ser utilizadas en un tribunal, además beneficiara a la sociedad quienes busquen culpables a la vez que servirá también para ayudar a demostrar la inocencia de aquellos que hayan sido acusados injustamente.

Por último, se presentará una propuesta de diseño de un LIF para la Universidad Católica de Cuenca, Campus Azogues, mismo que podría llegar a ser usada como un aporte tecnológico para futuras generaciones de estudiantes con el fin de lograr aumentar índices de profesionales que demandan la sociedad en el área de informática forense a la par que forma una oportunidad de incrementar el catálogo de servicios que ofrece la Universidad.

1.4 Objetivos

Objetivo General

Elaborar una propuesta de un laboratorio de informática forense mediante un estudio de la viabilidad técnica para la Universidad Católica de Cuenca, Campus Azogues.

Objetivos Específicos

1. Consultar información relacionada a la informática forense y las normativas legales ecuatorianas que permitan desarrollar un estudio para la propuesta de diseño de un LIF.
2. Identificar infraestructura, organización del personal, tecnología (Hardware y Software) y presupuestos necesarios para la propuesta del laboratorio de informática forense.
3. Establecer lineamientos para el diseño de un laboratorio de informática forense.

1.5 Alcance

El proyecto finalizará con la propuesta de diseño, donde se abarcará las condiciones mínimas para el funcionamiento de un laboratorio de informática forense en la Universidad Católica de Cuenca campus Azogues.

Los alcances considerados para la propuesta son:

- Proponer un diseño de un laboratorio de informática forense para la Universidad.
- Propuesta de una metodología de trabajo para el laboratorio y organización del personal para llevar a cabo las tareas dentro de las distintas áreas.

Además, la propuesta del LIF en la Universidad Católica de Cuenca, Campus Azogues, permanecerá en la jurisdicción de los directivos quienes tomaran las decisiones correspondientes.

1.6 Metodología

La metodología de esta investigación será de tipo cualitativo, haciendo uso de la técnica de la investigación bibliográfica o documental, con el objetivo de adquirir conocimientos a través de páginas web, libros electrónicos, documentos, artículos e investigaciones similares al proyecto planteado. Útil para este trabajo, debido a que abarca la observación, revisión de fuentes que puedan ser apropiadas para recoger información, cotejo de datos obtenidos donde se evalúa su confiabilidad e interpretación de la información necesaria para la investigación [5].

En donde se evaluará lo siguiente:

- Estudiar la legislación ecuatoriana acorde a los delitos informáticos.
- Definiciones de la informática forense, que lo compone y las herramientas tanto software como hardware que conforman un LIF.

- Evaluar la infraestructura y equipos de los laboratorios de la universidad para determinar la necesidad de equipamiento y establecer un presupuesto para una futura implementación.
- Determinar personal para el funcionamiento del laboratorio de informática forense.

1.7 Estado del arte

Investigación en Europa

Un estudio realizado en el año 2018 en España, se estableció la importancia de la ingeniería forense, la necesidad de la sociedad y la demanda de profesionales en esta área para lograr resolver problemas que tengan implicaciones legales relacionado con el uso de la tecnología, a la vez en la contribución a que no vuelvan a ocurrir, donde además el mismo autor resolvió un caso en particular, consiguiendo resultados satisfactorios [6].

Investigaciones en Sudamérica

También en 2019, Fabián González y Juan González Sanabría, propusieron el uso de laboratorios de informática forense para la solución de problemas de evasión fiscal en Colombia, como consecuencia, se demostró que al implementar nuevas tecnologías ayuda a agilizar procesos fiscales y la obtención de resultados más eficientes con la ayuda de laboratorios enfocados en esta área pericial [7].

Los autores Sergio Ortega y Stiven Paez en el año del 2020 en Colombia, generaron una serie de laboratorios y guías para el apoyo de la asignatura de informática forense del programa de Ingeniería de Sistemas, cuyo resultado fue la entrega de un documento completo acerca de esta ciencia, desde lo más básico a lo más complejo a la Universidad ECCI con el objetivo que funcione como referencia y apoyo para la asignatura de informática forense a la vez que es útil para orientar a los estudiantes con menos conocimientos en el área [8].

En el año 2021, una investigación que tenía como objetivo analizar la influencia que tiene la informática forense con relación a la calidad de servicios ofrecidos por el centro de cómputo en la Universidad Tecnológica de los Andes, Perú. Los resultados demostraron que con la ayuda de la IF no solo se puede identificar a los responsables de los delitos, si no también sirve para generar un historial con la intención de no volver a cometer los mismos errores de seguridad, evidenciando la importancia de la informática forense, a la vez, comprobando la correlación que tiene con la calidad de los servicios [9].

Investigaciones Nacionales

En 2016, en una investigación donde se estudió las diferentes metodologías existentes para realizar un análisis forense digital, cuyo objetivo fue establecer las mejores prácticas, normas operativas y procedimientos para la implementación de un laboratorio de informática forense en la Universidad de Guayaquil, donde el autor demostró la importancia de estos laboratorios para conseguir evidencia y así determinar la ejecución de un crimen. A la vez, la investigación forma parte de una guía para el aprendizaje de los estudiantes sobre procesos de tratamiento de la evidencia digital [10].

Por último, en 2019, se desarrolló una propuesta de implementación de un laboratorio de informática forense en la Universidad Politécnica Salesiana sede Quito, donde se estudió y analizó diferentes delitos informáticos considerando las herramientas usadas durante el proceso que se realiza en un laboratorio de informática forense, donde además propusieron otro conjunto de software y hardware útil para reforzar el laboratorio con el objetivo de lograr aportar evidencia digital útil para procesos jurídicos. Comprobando la importancia que tiene dentro de la sociedad una área de esta índole y además como la universidad puede darse la posibilidad de implementarlo [11].

CAPÍTULO 2

2.1 Informática Forense

Se refiere a todo un conjunto de técnicas y procedimientos metodológicos con el fin de cumplir con tareas como: Extracción, identificación, preservación, interpretación y presentación de evidencias obtenidas de diferentes dispositivos electrónicos, redes de computadoras, base de datos, entre otras, con el objetivo de lograr presentar evidencias aptas para procedimientos legales pertinentes dentro del país [12].

Esta ciencia a pesar de utilizar la tecnología para realizar tareas con el fin de preservar la integridad de los datos, también necesita de profesionales que cumplan con avanzados conocimientos sobre los sistemas informáticos para lograr descubrir los hechos que han ocurrido dentro de los dichos dispositivos electrónicos [13].

La informática forense surge de la necesidad de la sociedad, con el fin de responder ante sucesos ocasionados por delitos informáticos. El FBI (Buró Federal de Investigaciones) es la identidad federal líder en las investigaciones de este tipo, donde se encargan de desenmascarar todo tipo de acciones cibernéticas mal intencionadas alrededor del mundo.

2.1.1 Computación forense (Computer forensics)

A veces denominada como ciencia forense informática, permite la identificación y recuperación de los datos que se encuentran almacenados en todo tipo de dispositivo informático cumpliendo normativas legales con el objetivo que la evidencia obtenida sea aceptada dentro de un caso judicial [14].

También se encuentra especializada en la recuperación de datos de unidades fallidas, sistemas operativos, servidores bloqueados o en equipos de cómputo que dejaron de funcionar repentinamente.

2.1.2 Forensia en Redes (Network forensics)

Es una rama del análisis forense digital, se encuentra encargada de investigar todo tipo de tráfico de red, configuraciones entre la comunicación de equipos, infraestructuras, etc., con el fin de registrar los eventos en la red y así detectar o interceptar intrusos que busquen afectar la seguridad del sistema [15].

2.1.3 Forensia Digital (Digital forensics)

Esta disciplina se encarga de conseguir evidencias en medios informáticos o digitales por medio de herramientas de software y hardware, de tal forma que, dichas pruebas puedan ser presentadas ante procesos judiciales [16].

2.2 Ciencias forenses (Forensic science)

Son un conjunto de disciplinas, encaminados a investigar los sucesos ocurridos basándose en las pruebas obtenidas, a fin de llegar a conocer la veracidad de los hechos, para relacionarlos con el autores de dicho evento [17].

2.3 Delitos informáticos

Los delitos informáticos se refieren todo aquel acto delictivo, ilegal o poco ético a través del uso de la tecnología e internet con el fin de perjudicar a entidades gubernamentales, personas, empresas, etc., estos actos incluyen delitos tradicionales, aunque con un alcance aun mayor, como las estafas, robo, extorsión. Estos pueden ser sancionados siempre que se encuentren vigentes en código penal [18].

Debido a las innovaciones tecnológicas que han aumentado en los últimos años, los delitos informáticos se han vuelto más diversos acorde a la imaginación del delincuente, la disposición que tiene de la tecnología, la debilidad de la seguridad del sistema informático o que tan incauto es su víctima [19].

2.3.1 Características de los delitos informáticos

- Son perpetrados en su mayoría por personas con grandes conocimientos de la informática.
- Generan pérdidas económicas, daños e inseguridades.
- Tienden a aumentar y evolucionar, volviéndose cada vez más sofisticados, complicando más la identificación y/o enjuiciamiento de los mismos.
- Fáciles de cometer cuando se vincula con menores de edad.
- Gran parte de estos son imprudentes y con diferentes intenciones.
- Actos oportunistas, aprovechan de las ocasiones creadas.
- Pueden perpetrarse desde cualquier hora y lugar, debido a que, pueden cometerse en cuestión de segundos usando la tecnología.
- Anónimos, la identidad del delincuente e incluso la conexión donde realiza tal acto se vuelve oculta.
- Masivos, debido a la distribución inmensa que permite las TIC.
- Tienen a incrementar día a día debido a la poca regulación de la ley (independiente de cada país).

2.4 Tipos de atacantes

Los atacantes pueden formar grupos o también atacar de manera individual, cuya intención es aprovecharse de las vulnerabilidades existentes, con el objetivo de obtener ganancias personales, financieras o perjudicar a una sociedad [20].

También se puede mencionar que, la tecnología ha aportado al aprendizaje de estas maneras de cometer crímenes, lo que ha generado que aparezcan cada vez más individuos.

Se pueden clasificarlos como:

2.4.1 Scrip Kiddie

Este tipo de “hackers” usan programas descargados desde la internet, con la intención de entrar en las redes de computador, sistemas, páginas web, entre otros lugares más. Son individuos con poco conocimiento en la informática, su intención por lo general es conseguir renombre o alardear [21].

2.4.2 Lamer

Personas que se creen hackers, carecen de todo tipo de conocimientos en la informática mucho menos comprenden lo que realmente está pasando al utilizar alguna aplicación para penetrar la seguridad. Guardan y coleccionan todo tipo de guías, videos, libros con temáticas de hacking, sin embargo, su objetivo no es aprender, sino más bien presumir de ser hackers [21].

Aunque forma parte de los grupos que más perjudica con solo el hecho de utilizar todo tipo de software que encuentra en la red, provocando desastres al usar estas aplicaciones deliberadamente.

2.4.3 Newbie

Son principiantes que comienzan con curiosidad en el tema de hacking y terminan descargando todo tipo de programas de la internet con objetivo de ver que hace. A diferencia de los “Lamers”, estos sí están interesados en aprender, son prudentes con los pasos que siguen y comienzan adquiriendo conocimientos [21].

2.4.4 Phreaker

Individuos con gran conocimiento en la telefonía, realizan acciones ilegales por medio de los teléfonos y celulares. Crean todo tipo de dispositivos electrónicos caseros con la intención de interceptar e incluso efectuar llamadas telefónicas sin que el propietario note lo que está sucediendo. también eluden la trayectoria de la llamada de origen con la

finalidad de no ser atrapados, de la misma forma evaden las facturaciones de las compañías telefónicas [21].

2.4.5 Cracker

Son hackers “Black hat”, que tiene como propósito dañar sistemas, robar información, introducir malwares y se aprovecharse de las vulnerabilidades de los equipos para lucrase. Se dedican a crear ediciones desautorizadas de software con licencia, comúnmente llamadas “Crack”, para distribuirlos masivamente generando pérdidas económicas a las compañías [21].

2.4.6 Hacker

Poseen amplios conocimientos avanzados de los sistemas informáticos. Su intensa necesidad de conseguir información y superar retos intelectuales los lleva a infiltrase en los sistemas. Se los pueden llevar a confundir con los “crackers” debido a los accesos sin autorización a los sistemas por medio de internet. Sin embargo, también existen aquellos que buscan dar soluciones a las vulnerabilidades existentes en los sistemas, conocidos como “White hat”. De la misma forma están los “Grey hat” que pueden actuar de manera moral e inmoral acorde sus intereses, principalmente el dinero.

2.4.7 Carder

Es una persona que comete fraudes con tarjetas de crédito robadas, clonadas o adulteradas con el fin de adquirir bienes, alquilar servicios y realizar todo tipo de transacciones. La forma que operan estos tipos de hackers, es utilizando la ingeniería social o como también aprovecharse de las vulnerabilidades de los sistemas para obtener alguna BIN (Número de Identificación Bancario) [22].

2.4.8 Copyhackers

Individuo dedicado a crackear y falsificar hardware, principalmente se encuentran en el ámbito de las tarjetas inteligentes. También se copian los métodos de los hacker "Black hat" para crackear hardware o software, posteriormente se lo venden a los bucaneros [23].

2.4.9 Bucanero

No saben nada respecto a tecnología, se trata solo de un comerciante que revende los "productos" que obtuvo de los Copyhackers, motivado por conseguir dinero de manera rápida y sencilla.

2.4.10 Phiser

Conocidos también como "Ingenieros sociales", su forma de actuar es mediante engaños, haciéndose pasar por entidades oficiales, por medio de mensajes de texto, llamadas telefónicas, correos electrónicos, páginas web clonadas, etc., solicitando información como números de tarjetas, confirmaciones de identidad, usuarios, entre otras, con el fin que la víctima proporcione datos personales y así hacer uso de la misma de manera fraudulenta [24].

2.4.11 Spammer

Pueden ser tanto individuos como también empresas las culpables de enviar correos electrónicos no deseados (spam) de manera masiva, ocasionando la saturación del buzón de mensajes., como resultado, se vuelve difícil utilizar el e-mail como medio de comunicación.

2.4.12 Pirata informático

Se trata de una persona que distribuye, reproduce y/o apropia de contenido con propiedad intelectual sin autorización. Inconscientemente o no, nos convertimos en parte del

problema con el simple hecho de descargar aplicaciones, películas, música, videojuegos, e-books, etc., de forma ilegal de los sitios de que ofrecen estos contenidos digitales, sin embargo, al hacer esto somo susceptibles a varios riegos como ataques de malwares, demandas judiciales, multas, entre otras [25].

2.5 Tipos de ataques

2.5.1 Ingeniería social

Este tipo de ataque se trata de un conjunto de métodos para conseguir manipular o engañar a personas incautas, cuya finalidad es lograr que la víctima entregue todo tipo de datos sin que está se dé cuenta. Permitiendo que el atacante tenga el control de su información personal [26].

2.5.2 Ingeniería social inversa

Se basa en convencer a la víctima de que su dispositivo tiene ciertos problemas graves o que podría tenerlos, lo cual el atacante ofrece su "ayuda" para reparar dicho problema, ganándose así la confianza de la víctima, de esta forma el individuo logra acceder a la información personal sin que el usuario se percate.

2.5.3 Redes trampa

Consiste en crear redes wifi clonadas de sitios legítimos y confiables, utilizando nombres idénticos al original para pasar desapercibidos. El objetivo de este tipo de ataque es obtener los datos que accedemos en páginas web como: contraseñas de redes sociales, correos electrónicos, cuentas bancarias, etc., también pueden infectar al dispositivo de malware. Se encuentran mayormente en sitios con redes wifi públicas [26].

2.5.4 Ataques de inyección SQL

Se aprovechan de las vulnerabilidades del propio sitio web para introducir código SQL malicioso, para obtener acceso total o parcial a la base de datos anexada con el aplicativo web, logrando así extraer, modificar o dañar la información almacenada [26].

2.5.5 Ataque DDoS (Denegación distribuida de servicios)

Este tipo de ataque consiste en saturar el servidor mandando peticiones de manera masiva desde distintos equipos al mismos tiempo, su objetivo es causar el mal funcionamiento o la caída del servicio [26].

2.5.6 Ataques de fuerza bruta

El atacante intenta adivinar la contraseña mediante prueba y error, utilizando combinaciones al azar, mezclado palabras, números y nombres con los datos personales que ya hayan obtenido previamente, hasta llegar con la contraseña e incluso pueden hacer uso de un diccionario de contraseñas, cual consiste de un software que contiene las claves más usadas por los usuarios, a fin de conseguir acceder.

2.5.7 Spyware

Es un tipo de malware que se aloja en el dispositivo, permitiendo al atacante controlarla de manera remota. Estos programas también pueden hacer uso de la cámara como del micrófono e incluso descargar otros tipos de software maliciosos [26].

2.5.8 Ataque Man-in-the-Middle

"Hombre en el medio" o por su nombre en inglés, Man in the middle, es un ataque que realiza el ciberdelincuente al situarse en medio de la comunicación sin autorización entre un servidor y el cliente, con el fin de interceptar, modificar o leer todo tipo de trafico de información que fluya y esta sea su interés, como: números de tarjetas, información

personal, contraseñas etc., también puede hacerse pasar por cualquiera de las partes involucradas [27].

2.5.9 Keyloggers

Es un software o hardware que tiene por objetivo registrar y capturar todo tipo de pulsaciones que realiza el usuario en su teclado, obteniendo patrones de escritura, consiguiendo así; contraseñas, usuarios, cuentas bancarias y cualquier otro dato personal de la víctima [28].

2.5.10 Adware

Un malware desarrollado para la masiva presentación de publicidades no deseadas, son capaces de abrir ventanas con anuncios, redireccionar sitios web e inclusive recopilar las costumbres de la víctima como horarios de conexión, páginas web frecuentes y búsquedas comunes [28].

2.6 Tipos de delitos informáticos

La tecnología en manos incorrectas ha generado nuevas formas de cometer actos ilícitos provocando todo tipo de daño, pérdidas económicas, la apropiación de información y hasta imposibilitar la utilización de equipos informáticos o servicios. En años recientes se ha considerado el terrorismo electrónico y la pornografía infantil como nuevas formas de ciberdelitos.

2.6.1 Cyberbullying (Ciberacoso)

Es un tipo de agresión entre niños, adolescentes y jóvenes por medios de humillación, insultos e inclusive amenazas usando medios digitales como redes sociales, foros, videojuegos en línea entre otras, con el fin de generar daños psicológicos, a diferencia de bullying tradicional, al contar con medios digitales el agresor puede atacar a cualquier lugar en todo momento [29].

2.6.2 Grooming

Se trata de la acción que ejerce un adulto (hombre o mujer) de manera deliberada para establecer una comunicación con niños, niñas o adolescentes con el afán de ganarse la confianza del menor con el objetivo de obtener videos, imágenes e inclusive hasta conocerse en persona, provocando todo tipo de acciones como el abuso del menor. También aprovechan del contenido audio/visual conseguido con fines de extorción [29].

2.6.3 Suplantación de identidad

Este tipo de delito consiste en usurpar la identidad de la víctima para lograr cometer actividades delictivas en su nombre, dañando su reputación y la confianza en los demás. Estos hechos se pueden observar comúnmente en redes sociales.

2.6.4 Robo de datos (Phishing y Pharming)

Son formas de extraer información personal del individuo, por lo general, para beneficio económico. Tratándose el phishing como clones de páginas oficiales cuyo fin es conseguir que la víctima entregue su información sin percatarse, mientras que, el pharming consiste en un malware que se instala en el dispositivo al momento de abrir correos o descargar archivos de páginas poco confiables, tiendo por objetivo redirigir a otros sitios web engañosos [30].

2.6.5 Ransomware (Secuestro de datos)

Es un malware, cuya función es impedir al usuario acceder a su propios archivos, datos personales o equipos, donde por medio de amenazas de fuga o destrucción de la información, exigen un pago para el rescate dentro de un tiempo establecido. Este tipo de "secuestro virtual" son propagados por medio de spam, vínculos maliciosos, instalar programas crakeados o dispositivos infectados [31].

2.6.6 Filtración de información

También conocido como fuga de información, puede originarse de forma interna o externa, normalmente se ocasiona cuando los mismos empleados por descuido filtran todo tipo de información confidencial de la empresa u organización o caso contrario haciendo uso de dispositivos USB o discos, extraen todo tipo de datos importantes con la intención de venderla a la competencia [32].

2.6.7 Fake News

Tanto sitios web como redes sociales generan la difusión a gran escala de noticias engañosas, ficticias y elaboradas por los mismos usuarios, quienes a la vez se convierten en consumidores y distribuidores, provocando la desinformación en segundos. Este tipo de practica tienen como finalidad la manipulación del juicio personal, difamar o engrandecer instituciones, personas o partidos políticos [33].

2.6.8 Compras y ventas ilegales en Internet

Con la ayuda de la internet ha hecho posible el surgimiento de nuevos mercados, al mismo tiempo que ha generado nuevas formas de comercializar productos o servicios ilegales como: Pornografía infantil, animales exóticos o en peligro de extinción, armas, medicamentos ilegales, drogas, trata de blancas, bases de datos, información entre muchas otras cosas más, debido a la facilidad que ofrece el "anonimato" en la internet, esto agregado a las miles de formas de pagos ofrecidas por la tecnología hoy en día [34].

2.7 Derecho informático

El derecho informático se encarga de regular las implicaciones jurídicas ocasionados por el uso de la tecnología. Esta rama del derecho tiene como propósito analizar los ámbitos cambiantes que esta caracterizado las TICs en torno a sus usuarios, cuyo fin es establecer regulaciones, normativas y principios que moderen las acciones que se realizan con los

avances tecnológicos, logrando así prevenir situaciones peligrosas en relación a la sociedad [35].

En la actualidad el derecho informático va tomando cada vez más relevancia, debido a que ayuda a solucionar problemas vinculados con las tecnologías de la información, por medio de términos legales.

2.8 Perito Informático

El perito informático es un profesional en el área de la tecnología y se encargan de la recolección, preservación, análisis y la presentación de los datos obtenidos del peritaje. Su objetivo primordial es dar soporte, conocimientos y asesoramiento al tribunal o juez encargado del caso respondiendo interrogantes como: que se modificó, quien es el autor y como lo hizo, siendo totalmente imparcial al momento de actuar [36].

Sin embargo, las habilidades y capacidades del perito informático deben ser respaldadas por alguna institución que avale dichas aptitudes, para evitar que las evidencias presentadas sean puestas en duda.

2.9 Principios básicos para la manipulación de la evidencia digital

La evidencia o prueba digital son datos recogidos de los registros que son producidos por los sistemas informáticos como metadatos, discos duros, dispositivos USB, tráfico de red entre otras, clasificándose de dos formas: la volátil, definida como información temporal y la no volátil, la cual perdura a pesar de apagar los equipos. Estas mismas son utilizadas para investigaciones y juicios penales [37].

La importancia que tiene la evidencia digital es aportar a la reconstrucción de los sucesos que ocurrieron en dicho lugar, proporcionando hora y fecha de los acontecimientos que

relacionen al autor con el delito y su víctima. Sin embargo, estas pruebas pueden ser, modificadas, dañadas y/o destruidas puesto que se tratan de información delicada.

Por ello se debe tener en cuenta una serie de principios que ayuden a la recolección y manipulación de la información:

1. Las acciones realizadas para recolectar las pruebas no deben modificar de ninguna forma la evidencia obtenida [38].
2. Solo los profesionales forenses tienen autorización para acceder a la evidencia digital original [38].
3. Todas las actividades relacionadas con el acceso, recopilación, traslado y/o almacenamiento de la evidencia digital deben documentarse, conservarse y estar disponibles para su revisión en su totalidad en cualquier momento [38].
4. Las acciones realizadas con la evidencia digital son responsabilidad de la persona que las tenga en su momento [38].

2.10 Valorización de la evidencia digital

Para que la evidencia digital sea tomada en consideración debe de seguir un conjunto de reglas que acrediten que las pruebas presentadas sean validas frente a un tribunal.

- **Aceptables:** Las evidencias deben ser admisibles dentro de una corte [39].
- **Legitimo:** Las evidencias presentadas tienen que ser auténticas y deben de vincularse con el acontecimiento de forma significante [39].
- **Integro:** Toda evidencia debe ser capaz de mostrar una visión completa del asunto, además de demostrar la infracción o la inocencia del acusado [39].
- **Transparente:** Las evidencias no deben ser cuestionadas de su autenticidad [39].

- **Fiable:** Las evidencias otorgadas al jurado deben ser comprensibles, convincentes y claras [39].

2.11 Cadena de custodia

También conocida como documentación cronológica de la evidencia digital o enlace forense, es utilizada para indicar los procedimientos efectuados durante la recolección, análisis y transferencia de la evidencia, registrando con fecha y hora las actividades realizadas de cada una de las personas que manipulan la prueba digital. También se documenta los instrumentos que se utilizaron para la recolección y el objetivo de la transferencia [40].

La cadena de custodia es de gran importancia puesto a que permite salvaguardar la integridad de las evidencias obtenidas, evitando que se "contaminen", debido a que, si no se conservan de manera adecuada, las pruebas expuestas ante un tribunal podrían llegar a ser inadmisibles y descartadas.

2.12 Tipificación del delito informático en la legislación ecuatoriana

Los delitos informáticos son perpetrados en todo momento en cualquier lugar, debido a la facilidad de los delincuentes que tienen para realizar actos ilegales por medio de la tecnología. Ecuador no está exentó de estos delitos, es más, a lo largo de los años estos tipos de crímenes ha ido incrementado, para el año 2019, el país ya contaba con 40 millones de ataques cibernéticos, donde las entidades más afectadas se encontraban la Cancillería de Ecuador, el Banco Central del Ecuador, la Presidencia de la República, ministerios etc., e incluso estos ataques eran realizados por "hackers" de otros países [41].

Actualmente en el 2022, Ecuador comenzó a figurar en la lista de los países con más ataques cibernéticos recibidos, donde el 43% de estos ataques iban dirigidos a las

pequeñas y medianas empresas (PYMES), mismas que no tienen los recursos suficientes para invertir en mejor seguridad y son mucho menos prevenidos [42].

Por estos motivos se ha llegado a diseñar leyes y medidas que regulen estos actos, estos se encuentran plasmados en el Código Orgánico Integral Penal, mismo que fue presentado en al año 2014., donde los delitos informáticos se encuentran tipificados y sancionados de la siguiente manera:

El Articulo 173.- "*Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos"* [43], establece que todo individuo que haga uso de medios electrónicos o telemáticos para lograr concretar un encuentro con menores de edad con índole sexual, serán castigados con 1 a 3 años de pena privativa. Si el acercamiento se da por intimidación, fuerza o el perpetrador hace uso de una identidad falsa o suplanta la de un tercero con el fin de obtener contenido erótico o sexual del menor, será sancionado con 3 a 5 años.

De acuerdo al Artículo 174.- "*Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos*" [43], se menciona que todo individuo que utilice medios digitales como redes sociales, videojuegos en línea, correos electrónicos, chats, blog, mensajes instantáneos, etc., con el objetivo de ofrecer servicios sexuales a menores de edad, serán sancionados con pena privativa de 7 a 10 años.

En referencia al Artículo 178**.- "***Violación a la intimidad"* [43], indica que, cualquier persona que no cuente con la autorización legal o consentimiento, grabe, intercepte, examine, acceda, distribuya o venda cualquier tipo de información personal obtenida en dispositivos informáticos, comunicaciones reservadas o privadas de otras personas, tendrá una sanción de 1 a 3 años de pena privativa.

El Artículo 186**.- "***Estafa***"** [43]**,** establece que, cualquier persona que obtenga beneficio para terceros o para sí mismo, mediante la falsificación, clonación, hurto o uso sin consentimiento de tarjetas de débito, crédito u otro tipo de pago para perjudicar patrimonio del propietario, tendrá una pena privativa de 5 a 7 años.

De acuerdo al Artículo 190**.- "***Apropiación fraudulenta por medios electrónico"* [43], menciona que toda persona que haga uso de redes electrónicas, sistemas informáticos y de telecomunicación de forma fraudulenta con fin de conseguir un bien ajeno o apropiarse de algún valor o derecho por medio da la manipulación o modificación del funcionamiento de programas, redes electrónicas, equipos, sistemas informáticos y telemáticos, serán sancionados con pena privativa de 1 a 3 años.

En referencia al Artículo 195.- "*Infraestructura ilícita"* [43], establece que cualquier individuo que tenga a su disposición programas, base de datos, equipos, etiquetas o infraestructura que posibilite la manipulación, modificación, reprogramación y/o alteración de la información de equipos, será castigado con pena preventiva de 1 a 3 años.

Acorde al Artículo 229.- "*Revelación ilegal de base de datos"* [43], el individuo que revele la información guardada y registrada en archivos, ficheros, base de datos o semejantes, por medio de sistemas informáticos, electrónicos o telemáticos, será sancionado con 1 a 3 años de pena privativa, de igual manera si tal acción es cometida por un empleado/a, servidor público, internos etc., serán castigados con 3 a 5 años.

Según el Artículo 230.- "*Interceptación ilegal de datos"* [43], será sancionada con 3 a 5 años de pena privativa toda persona que escuche, guarde, grabe, visualice e intercepte todo tipo de información. De igual manera que utilice programas que redireccionen a otro sitio web clonado al original con el fin de obtener datos personales.

En el Artículo 231.- "*Transferencia electrónica de activo patrimonial"* [43], alude que el individuo que modifique o manipule el funcionamiento del sistema informático con el fin de apropiarse o transferir sin consentimiento el activo patrimonial de otro individuo, será castigado con 3 a 6 años.

En referencia al Artículo 232.- "*Ataque a la integridad de sistemas informáticos"* [43], toda persona que genere daño, suspensión, destrucción, eliminación, alteración o mal funcionamiento de los sistemas informáticos lógicos o físicos, serán sancionados con pena privativa de 3 a 5 años. Si la trasgresión es cometida a bienes destinados a la seguridad ciudadana o al servicio público, será de 5 a 7 años.

Acorde al Artículo 233.- "*Delitos contra la información pública reservada legalmente"* [43], indica que, la destrucción o inutilización que provoque un individuo a la información clasificada, será castigada con 5 a 7 años de pena privativa. Si la publicación o utilización sin autorización de la información reservada atenta contra la seguridad del estado, el encargado de la custodia de dicha información será castigado con 7 a 10 años.

En el Artículo 234.- "*Acceso no consentido a un sistema informático, telemático o de telecomunicaciones"* [43], se menciona que cualquier individuo que acceda o se mantenga dentro de los sistemas informáticos, telemáticos o de telecomunicación sin autorización del propietario, con el fin de modificar, dañar, manipular, interceptar, destruir, redireccionar o desviar cualquier tipo de tráfico de datos o use los servicios sin hacer su pago correspondiente al propietario, será castigado con 3 a 5 años de pena privativa.

En referencia al Artículo 456.- "*Cadena de custodia*" [43], donde establece que ofrecerá protección y seguridad a las evidencias digitales o elementos físicos, a la vez que todo cambio que realicen los profesionales durante la manipulación, envió, conservación y

análisis de estos elementos, quedará registrado con los cambios realizados con el fin de proteger la autenticidad y el estado original de la evidencia.

De acuerdo con el Artículo 457.- "*Criterios de Valoración*" [43], se menciona que, las evidencias digitales se someterán a un resguardo técnico y científico para corroborar su autenticidad y legitimidad frente a la evidencia original.

Según el Artículo 500.- "*Contenido digital"* [43], establece que todo contenido digital que se encuentre almacenado en sistemas informáticos, memorias volátiles, dispositivos no volátiles, medios digitales o físicos entre otros, serán recuperados, analizados y presentados usando técnicas digitales forenses correspondientes con el fin de conservar su integridad y asegurar su valoración.

2.13 ISO 27037:2012

La normativa ISO/IEC 27037:2012 brinda orientación para actividades específicas en el procesamiento de las pruebas digitales, es decir, identificar, recopilar, adquirir y salvaguardar cualquier dato que consiga ser evidencia probatoria potencial. Además proporciona soporte a organizaciones y empresas en procedimientos de preservación de la evidencia digital con el fin de que puedan ser usadas e intercambiadas en jurisdicciones legales distintas [44]. La ISO/IEC 27037:2012 otorga una guía para las siguientes circunstancias y dispositivos:

- Medios de almacenamiento internos y externos.
- Tarjetas de memoria, asistentes inteligentes, dispositivos móviles y funciones similares.
- Protocolos de red y digitales.
- Cámaras de video y fotografía.
- Computadoras interconectadas a la red.

- Sistemas GPS.

La normativa no está encaminada a proporcionar o mencionar las herramientas pertinentes que se deban utilizar en este tipo de actividades, al contrario, su objetivo es brindar soporte en los tratamientos especializados en identificar, recolectar, preservar, analizar y revisar la evidencia digital.

2.14 Criptografía

Es una herramienta muy útil para mantener la información segura, integra y confiable, sobre todo que se encuentre disponible cuando se requiera. La criptografía tiene como objetivo asegurar documentos y datos utilizando un código o clave de autorización que facilite a la información confidencial almacenada viajar por canales privados y públicos, pasando desapercibida. Permitiendo que solo puedan descifrarla y leerla aquellos que está destinada dicha información [45].

CAPÍTULO 3

3.1 Laboratorios actuales de la Universidad

Gracias a la información proporcionada por la Jefatura de Tecnología Informática, la Universidad Católica de Cuenca, campus Azogues, cuenta con siete laboratorios de informática, sin embargo, se procede a describir solamente tres laboratorios que se localizan en el Bloque Central del campus, debido a su ubicación y equipos tecnológicos que posee, esto con el objetivo de determinar cuál de estos es más adecuado para realizar un diseño interno y que se adapte a un laboratorio de informática forense, en donde se pueda hacer uso de hardware y software pertinentes.

3.2 Inventarios de los Laboratorios de la Universidad

Los laboratorios se encuentran el Bloque Central de la Universidad Católica de Cuenca, Campus Azogues, cada laboratorio cuenta con cámara de seguridad, doble puerta, detectores de incendios y extintores, además, disponen de un propio segmento de red administrativo en el Centro de Datos del campus. Estos laboratorios son:

- Laboratorio Nro. 104
- Laboratorio Nro. 208
- Laboratorio Nro. 209

Estos mismos se encuentran a cargo de los laboratoristas del campus y se pueden acceder a ellos en horarios de clases de lunes a viernes de 7H00 a 21H00.

3.2.1 Laboratorio Nro. 104

Datos generales: Es asignado por el Coordinador del campus en conjunto con el Laboratorista a cargo, a las distintas Carreras según solicitud de la Dirección de Carrera. Este dispone de computadores de escritorio con acceso a Internet, así como también a

programas utilitarios, ofimáticos y herramientas TIC a disposición de estudiantes, docentes e Instituciones.

Características: Cuenta con 21 computadoras de escritorio, un proyector multimedia marca Epson S31+, dentro de su jaula de seguridad empotrada en el techo y una pantalla de proyección enrollable sobre el pizarrón de tiza líquida; parlantes amplificados en caso de requerir audio; iluminación con lámparas de neón de luz blanca; señalización. En cuanto a conectividad dispone de un switch Cisco 2960 SERIES.

A continuación, en la Tabla 1 se muestran las características generales del Laboratorio Nro. 104.

Características generales	
Nombre del Laboratorio	Laboratorio 104
Ubicación	Bloque Central – Planta Baja, Laboratorio nro. 104
Número de Equipos	21 (1 Docente – 20 Estudiantes)
Capacidad	Mínimo 20 – 40 Máximo (Estudiantes)
Mobiliario	20 mesas
	1 escritorio
	41 sillas
Dimensiones	54,00 m^2

Conectividad	1 switch de 24 puertos Cisco Catalys 2960-S Series SI
Puntos de Red	21 puntos de red para acceso a 21 equipos de cómputo.
Proyector	Epson S31+

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 1. Características generales del Laboratorio 104

Fuente: Autor.

Ubicación Física: El laboratorio nro. 104 se encuentra ubicada en la Planta Baja (PB) del Bloque Central de la Universidad Católica de Cuenca, Campus Azogues. Ver Figura 1.

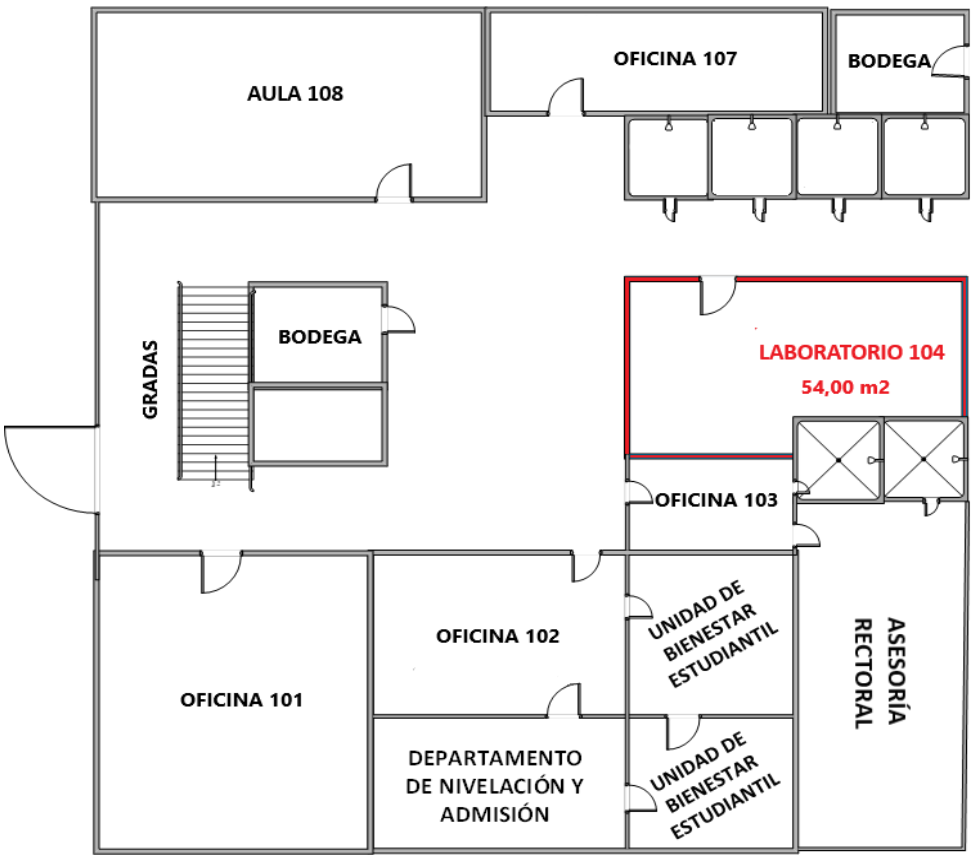


Figura 1. Ubicación Física del Laboratorio Nro. 104

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Distribución de equipos de cómputo: Dentro del laboratorio los equipos se encuentran distribuidos en 4 hileras en una superficie aproximadamente de 54,00 m^2. Ver Figura 2.

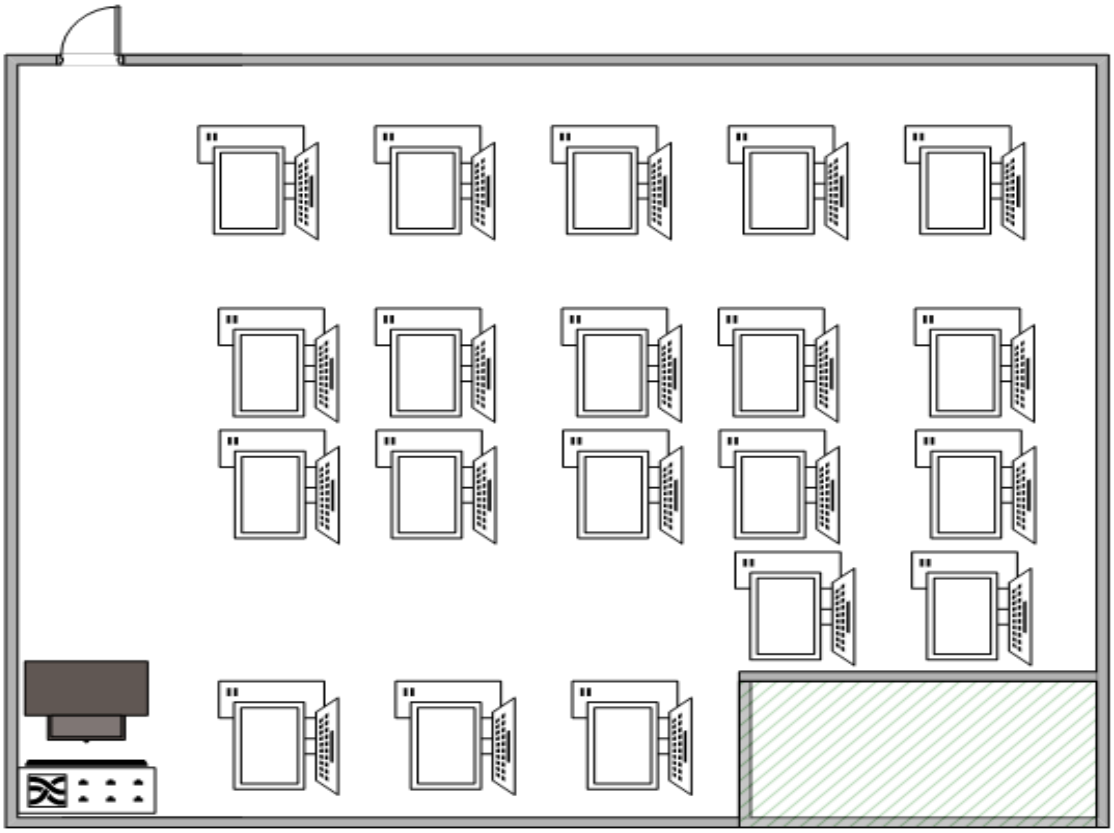


Figura 2. Distribución de equipos de cómputo del Laboratorio Nro. 104

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Cuenta con un extintor de incendios de polvo químico, ubicado junto a la puerta de ingreso.

Hardware: El laboratorio nro. 104, posee 21 equipos, 20 destinado para el uso de los estudiantes y 1 para el uso del docente, estos equipos de cómputo del laboratorio cuentan con las siguientes características. Ver Tabla 2 y 3.

20 equipos de cómputo	
MainBoard	Intel
Procesador	Intel Core i7-7700 de 3.60 GHz

Memoria RAM	8 GB
Disco Duro	SATA de 1 TB
Monitor	Pantalla Led de 19” (16 marca AOC y 1 marca LG)
Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 2. Características de hardware de los equipos para los estudiantes, Lab. 104

Fuente: Autor.

1 equipo de cómputo	
MainBoard	Intel
Procesador	Intel Core i5-3450 CPU 3.10 Ghz
Memoria RAM	6 GB
Disco Duro	SATA de 500 GB
Monitor	Pantalla Led de 17” marca Samsung
Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 3. Características de hardware del equipo para el docente, Lab. 104

Fuente: Autor.

Software: En los 21 equipos se encuentran instalado los siguientes utilitarios básicos y software para la disposición de los estudiantes y docentes, mismos que se detallan en la tabla. Ver Tabla 4.

Software Instalados en los 21 Equipos		
Sistema Operativo	Windows 10 – 64 bits	Licencia
Ofimática	Office 2016	Licencia
Antivirus	ESET Endpoint Security	Licencia
Navegadores	Mozilla Firefox	Libre
	Google Chrome	
	Internet Explorer	
Otros Programas	Adobe Reader	Libre

Tabla 4. Softwares instalados en los 21 equipos del Laboratorio Nro. 104

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Conectividad: La conectividad a la red del Laboratorio está manejada por 1 switch de 24 puertos Cisco Catalys 2960-S Series SI, que ofrece conectividad Gigabit Ethernet (10/100/1000). El mismo que se conecta con fibra de manera directa al Centro de Datos. Todos los equipos de cómputo se conectan utilizando cableado estructurado categoría 6A:

- Switch → puntos de red
- Puntos de red → PC

3.2.2 Laboratorio Nro. 208

Datos generales: Este laboratorio está destinado exclusivamente para uso de la Carrera de Ingeniería de Sistemas y Sistemas de Información, pues está designado a las prácticas

de Cisco. Este laboratorio de informática dispone de computadores de escritorio con acceso a Internet, así como también a programas utilitarios, ofimáticos y herramientas TIC a disposición de estudiantes, docentes e Instituciones.

Características: Este laboratorio ha sido destinado como Laboratorio de Redes. Cuenta con 20 computadoras de escritorio; proyector multimedia marca Epson S41+, dentro de su jaula de seguridad empotrada en el techo y una pantalla de proyección enrollable sobre el pizarrón de tiza líquida; parlantes amplificados en caso de requerir audio; iluminación con lámparas de neón de luz blanca; señalización. En cuanto a conectividad, esta apto para 21 equipos de cómputo, dispone de un Switch Cisco 2960 SERIES.

A continuación, en la Tabla 5 se muestran las características generales del Laboratorio Nro. 208.

Características Generales	
Nombre del Laboratorio	Laboratorio 208
Ubicación	Bloque Central – Primer Piso, Laboratorio nro. 208
Número de Equipos	20 (Estudiantes)
Capacidad	20 estudiantes
Mobiliario	10 mesas bipersonales
	1 escritorio
	21 sillas
Dimensiones	42,30 m^2

Conectividad	1 switch de 24 puertos Cisco Catalys 2960-S Series SI
Puntos de Red	21 puntos de red para acceso a 21 equipos de cómputo.
Proyector	Epson S41+

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 5. Características generales del Laboratorio 208

Fuente: Autor

Ubicación Física: El laboratorio nro. 208 se encuentra ubicada en el Primer piso (P1) del Bloque central de la Universidad Católica de Cuenca, Campus Azogues. Ver Figura 3.

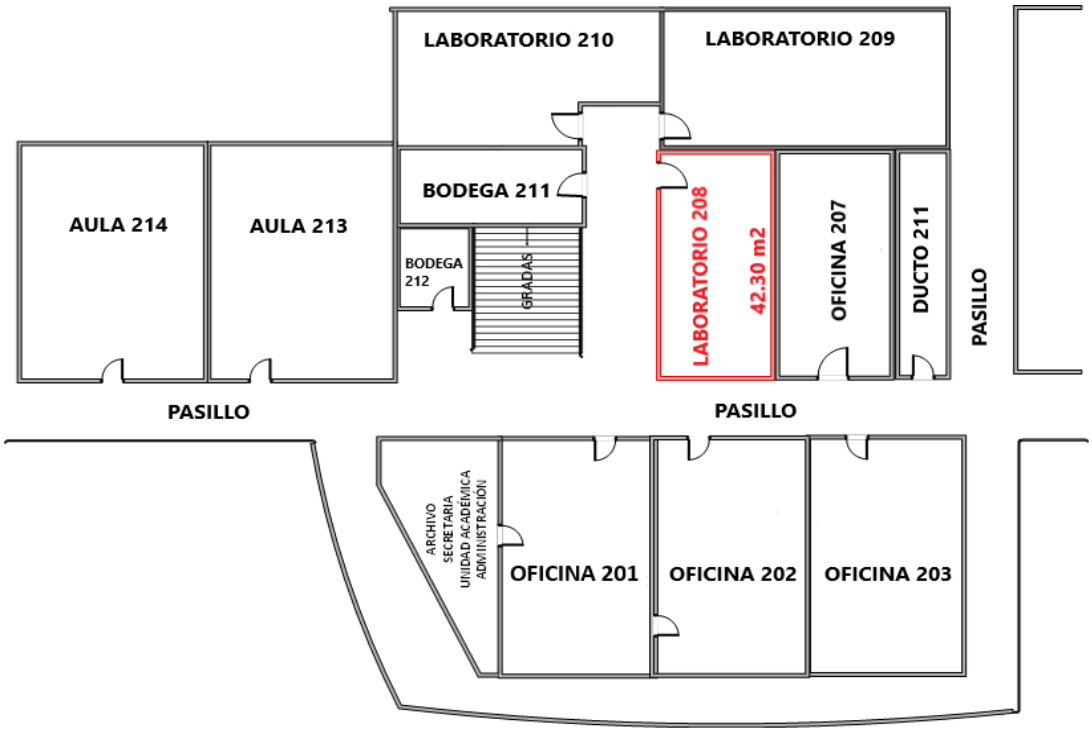


Figura 3. Ubicación del Laboratorio Nro. 208

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Distribución de equipos de cómputo: Los equipos se encuentran distribuidos en 4 hileras en una superficie aproximadamente de 42,30 m^2. Ver Figura 4.

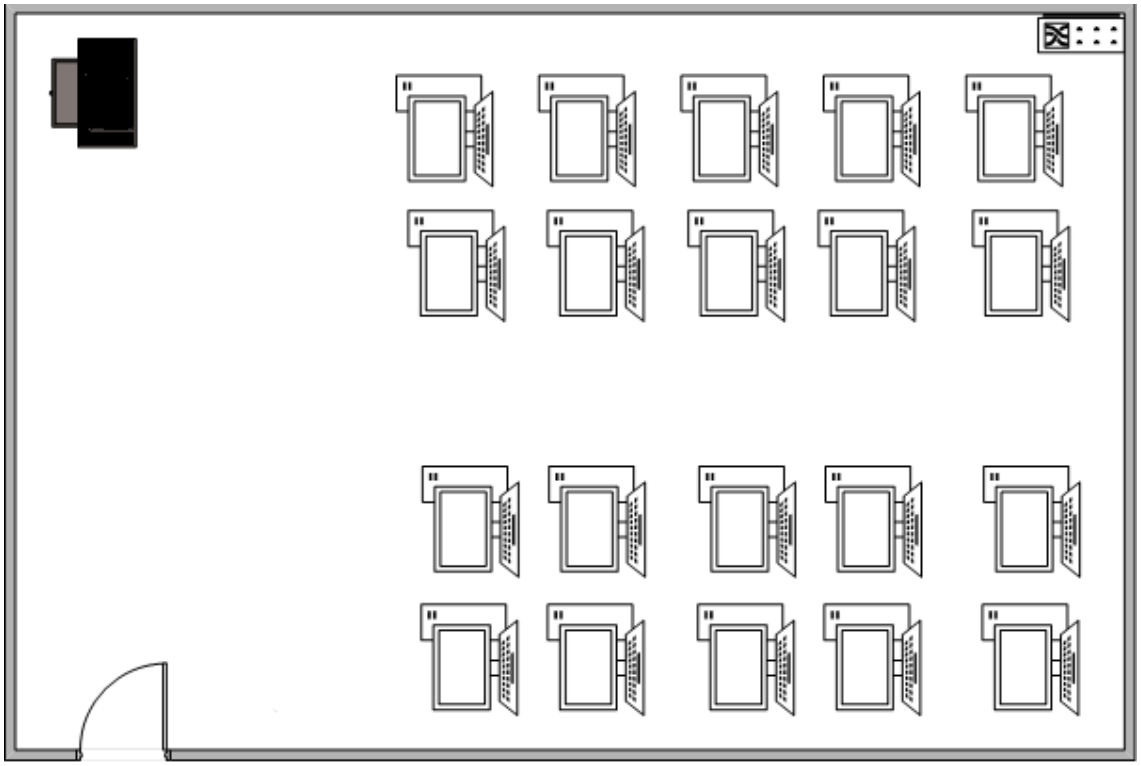


Figura 4. Distribución de equipos de cómputo del Laboratorio Nro. 208

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Posee un extintor de incendios de polvo químico, ubicado junto a la puerta de ingreso.

Hardware: El laboratorio posee 20 equipos de cómputo, así también cuenta con equipos Cisco para las prácticas de redes para los estudiantes. Ver Tabla 6 y 7.

20 equipos de Computo	
MainBoard	Intel
Procesador	Intel Core i7-7700 CPU 3.60 Ghz
Memoria RAM	8 GB
Disco Duro	SATA de 1 TB
Monitor	19 pantalla Led de 19”
	1 pantalla Led de 17”

Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 6. Características del hardware de los equipos para los estudiantes, Lab. 208

Fuente: Autor.

Hardware para prácticas de redes.

Equipos Cisco	
Switch Cisco Catalys 2960 Series	12
Routers Cisco 2800 series	6
Routers Cisco 1900 series	6

Nota: Información proporcionada por la Jefatura de Tecnología informática, Campus Azogues.

Tabla 7. Equipos Cisco para prácticas de redes para los estudiantes, Lab. 208

Fuente: Autor.

Software: En los 20 equipos se encuentran instalado el siguiente software para la disposición de los estudiantes. Ver Tabla 8.

Software Instalados en los 20 Equipos		
Sistema Operativo	Windows 10 – 64 bits	Licencia
Ofimática	Office 2016	Licencia
Antivirus	ESET Endpoint Security	Licencia
Navegadores	Mozilla Firefox	Libre
	Google Chrome	

	Internet Explorer	
Otros programas	Adobe Reader	Libre
Solicitados por Ingeniería de Sistemas y Sistemas de la Información	Microsoft SQL Server	Licencia
	Cisco Packet Tracer	Estudiantil
	NetBeans IDE 8.2	Libre
	JDK 8	Libre

Tabla 8. Softwares instalados en los 21 equipos del Laboratorio Nro. 208

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Conectividad: La conectividad a la red del Laboratorio está manejada por 1 switch de 48 puertos Cisco Catalys 2960-S Series SI, que ofrece conectividad Gigabit Ethernet (10/100/1000). El mismo que se conecta con fibra de manera directa al Centro de Datos. Todos los equipos de cómputo se conectan utilizando cableado estructurado categoría 6A:

- Switch → puntos de red
- Puntos de red → PC

3.2.3 Laboratorio Nro. 209

Datos Generales: Es asignado por el Coordinador del campus en conjunto con el Laboratorista a cargo, a las distintas Carreras según solicitud de la Dirección de Carrera, de la misma forma, este dispone de computadores de escritorio con acceso a Internet, programas utilitarios, ofimáticos y herramientas TIC a disposición de estudiantes, docentes e Instituciones.

Características: Dispone de 21 computadoras de escritorio; un proyector multimedia marca Epson S41+, dentro de su jaula de seguridad empotrada en el techo y una pantalla de proyección enrollable sobre el pizarrón de tiza líquida; parlantes amplificados en caso

de requerir audio; iluminación con lámparas de neón de luz blanca; señalización. En cuanto a conectividad dispone de un Switch Cisco 2960 SERIES.

A continuación, en la Tabla 9 se muestran las características generales del Laboratorio Nro. 209.

Características Generales	
Nombre del Laboratorio	Laboratorio 209
Ubicación	Bloque Central – Primer Piso, Laboratorio nro. 209
Número de Equipos	21 (1 Docente – 20 Estudiantes)
Capacidad	Mínimo 20 – 40 Máximo (Estudiantes)
Mobiliario	21 mesas
	1 escritorio
	41 sillas
Dimensiones	54,00 m^2
Conectividad	1 switch de 24 puertos Cisco Catalys 2960-S Series SI
Puntos de Red	21 puntos de red para acceso a 21 equipos de cómputo.
Proyector	Epson S41+

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 9. Características generales del Laboratorio 209

Fuente: Autor.

Ubicación Física: El laboratorio nro. 209 se encuentra ubicada en el Primer piso (P1) del Bloque Central de la Universidad Católica de Cuenca, Campus Azogues. Ver Figura 5.

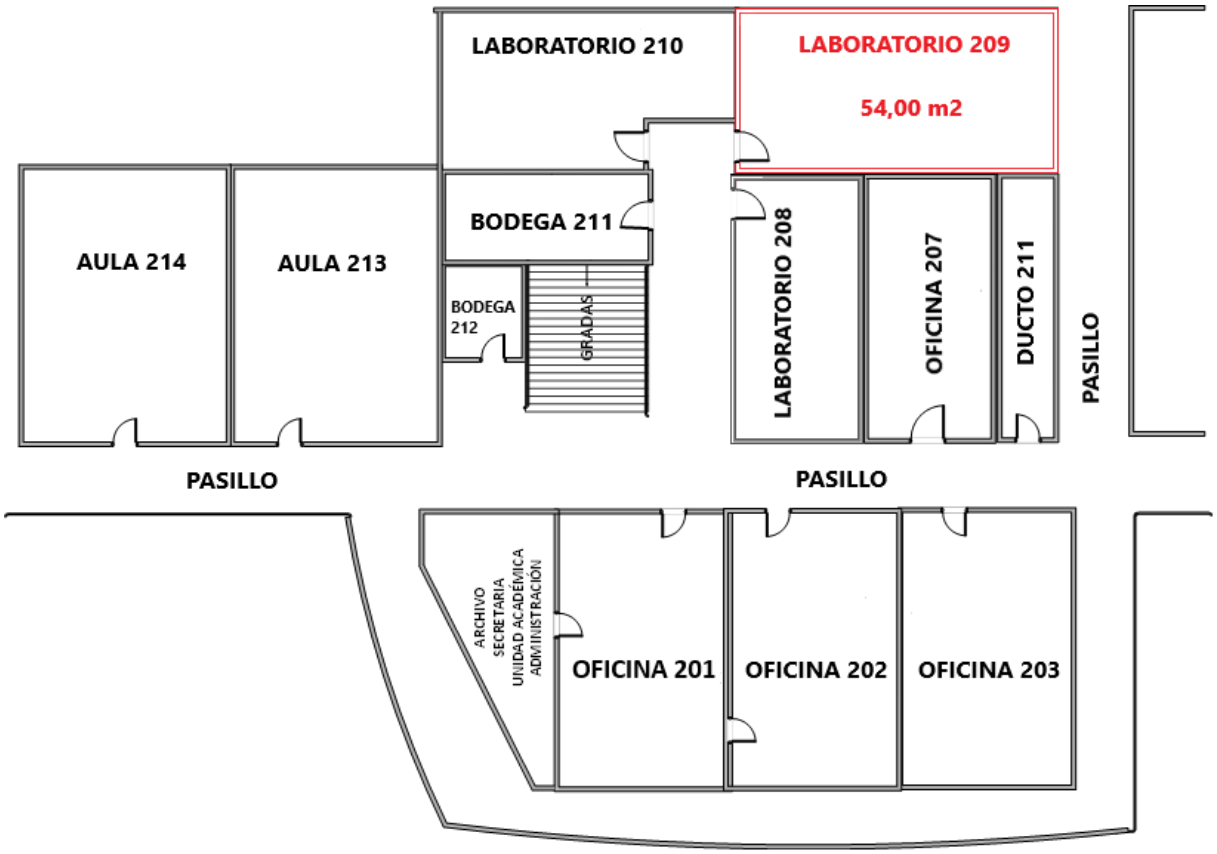


Figura 5. Ubicación del Laboratorio Nro. 209

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Distribución de los equipos de cómputo: Los equipos se encuentran distribuidos en 4 hileras en una superficie aproximadamente de 54,00 m^2. Ver Figura 6.

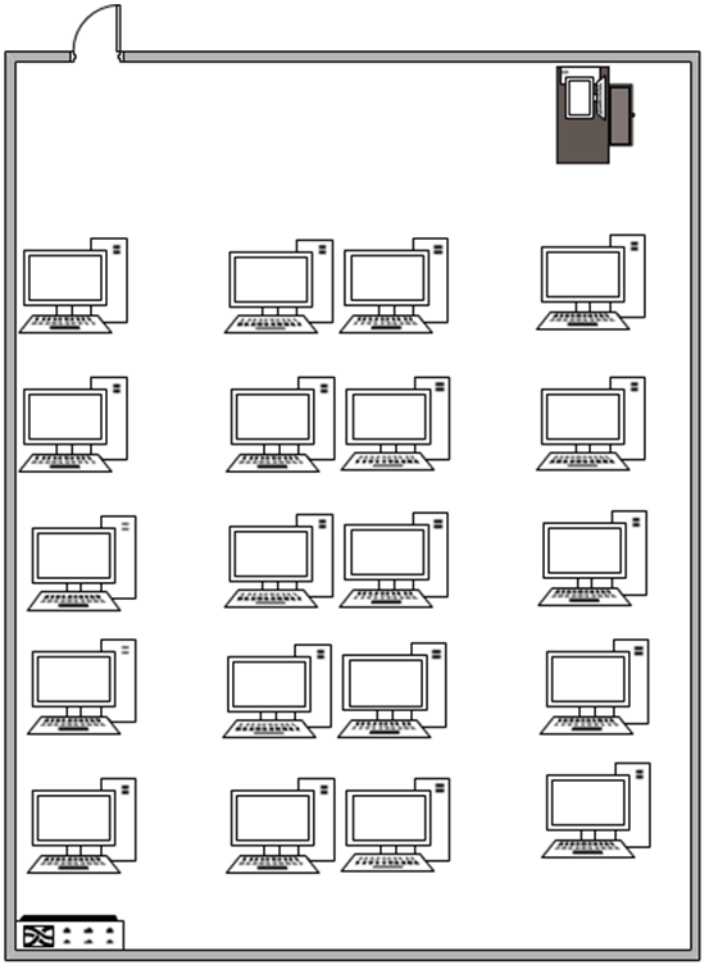


Figura 6. Distribución de equipos de cómputo del Laboratorio Nro. 209

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Cuenta con un extintor de incendios de polvo químico, ubicado junto a la puerta de ingreso.

Hardware: El laboratorio nro. 209, posee 21 equipos, 20 para el uso de estudiantes y 1 para el uso del docente, estos equipos de cómputo del laboratorio cuentan con las siguientes características. Ver Tabla 10 y 11.

18 equipos de cómputo	
MainBoard	Intel DH61SA
Procesador	Intel Core i5-3450 CPU 3.10 Ghz

Memoria RAM	4 GB
Disco Duro	SATA de 500 GB
Monitor	Pantalla Led de 17” marca Samsung
Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	
1 equipo de cómputo	
MainBoard	Intel H81H3-M4
Procesador	Intel Core i5-4440 CPU 3.10 Ghz
Memoria RAM	4 GB
Disco Duro	SATA de 500 GB
Monitor	Pantalla Led de 17” marca Samsung
Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	
1 equipo de cómputo	
MainBoard	Intel B85M-DS3H
Procesador	Intel Core i7-7700 de 3.40 GHz
Memoria RAM	8 GB
Disco Duro	SATA de 1 TB
Monitor	Pantalla Led de 17” marca Samsung

Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 10. Características de hardware de los equipos para los estudiantes, Lab. 209

Fuente: Autor.

1 equipo de cómputo	
MainBoard	Intel H81M-S1
Procesador	Intel Core i5-4460 CPU 3.20 Ghz
Memoria RAM	4 GB
Disco Duro	SATA de 500 GB
Monitor	Pantalla Led de 17” marca Samsung
Tarjeta de Red	
Unidad DVD Writer	
Teclado y Ratón Óptico	

Nota: Información proporcionada por la Jefatura de Tecnología Informática, Campus Azogues.

Tabla 11. Características de hardware del equipo para el docente, Lab. 209

Fuente: Autor.

Software: En los 21 equipos se encuentran instalado el siguiente software para la disposición de los estudiantes y docentes. Ver Tabla 12.

Software Instalados en los 21 Equipos		
Sistema Operativo	Windows 10 – 64 bits	Licencia

Ofimática	Office 2016	Licencia
Antivirus	ESET Endpoint Security	Licencia
Navegadores	Mozilla Firefox	Libre
	Google Chrome	
	Internet Explorer	
Otros Programas	Adobe Reader	Libre
Solicitados por Ingeniería de Sistemas y Sistemas de Información	Visual Studio	Licencia
	Microsoft SQL Server	Licencia
	NetBeans IDE 8.2	Libre
	JDK 8	Libre

Tabla 12. Softwares instalados en los 21 equipos del Laboratorio Nro. 209

Fuente: Jefatura de Tecnología Informática, Campus Azogues.

Conectividad: La conectividad a la red del Laboratorio está manejada por 1 switch de 24 puertos Cisco Catalys 2960-S Series SI, que ofrece conectividad Gigabit Ethernet (10/100/1000). El mismo que se conecta con fibra de manera directa al Centro de Datos. Todos los equipos de cómputo se conectan utilizando cableado estructurado categoría 6A:

- Switch → puntos de red
- Puntos de red → PC

3.3 Laboratorio de Informática Forense (UCACUE-LIF)

Acorde a la información descrita de la infraestructura de hardware y software, ubicación y características de los distintos laboratorios de informática que se encuentran en el Bloque Central de la Universidad, se procede a compararlos a fin de determinar cuál

laboratorio es el más viable para realizar el diseño del Laboratorio de Informática Forense. Ver Tabla 13.

Comparación entre los Laboratorios del Bloque Central				
	Dimensiones	**Ubicación**	**Características de los equipos de cómputo**	**Seguridad**
Laboratorio 104	54,00 m^2	No Favorable	Alta	Alta
Laboratorio 208	42,30 m^2	Favorable	Alta	Muy Alta
Laboratorio 209	54,00 m^2	Favorable	Media	Muy Alta

Tabla 13. Comparación entre los laboratorios del Bloque Central

Fuente: Autor.

- Se han descartado el Laboratorio Nro. 104, debido a que no se encuentra en una ubicación favorable, puesto que se ubica en un lugar donde no se puede observar al laboratorio a simple vista, además que es propenso a desastres naturales como posibles inundaciones.
- Se ha descartado el Laboratorio Nro. 208, debido a las dimensiones que presenta el lugar no son apropiadas para que cuente con todas las áreas pensadas para el diseño del LIF, a la vez que, dispone de ventanas con vista a las computadoras lo que evita la privacidad de las evidencias.
- El Laboratorio Nro. 209 presenta dimensiones adecuadas para establecer las diferentes áreas pensadas para realizar las diferentes actividades de la informática forense y la ubicación propicia para el diseño de un laboratorio de esta área.

El Laboratorio Nro. 209 cuenta con equipos de cómputo, mismos que se ocuparán 3 para temas de administración, como registros de casos, registros de evidencias que hayan llegado al laboratorio, supervisión de funcionamiento de las demás áreas, etc., por otro lado, se pretende utilizar 3 equipos del Laboratorio Nro. 104 o del Laboratorio Nro. 208, a fin de lograr aprovechar las características de los equipos. También se emplearán adecuaciones necesarias, consideraciones para la seguridad y el fortalecimiento del LIF, como también la propuesta de adquisición de hardware y software pertinente.

CAPÍTULO 4

4.1 Consideraciones generales para el diseño del LIF

Establecer un diseño para un Laboratorio de Informática Forense requiere de varios componentes como: la infraestructura, hardware y software, equipos informáticos, procedimientos, personal y la seguridad física de las instalaciones, con el fin que la evidencia se pueda resguardar de forma segura y confidencial.

4.2 Lineamientos para el diseño de un Laboratorio de Informática Forense

Se deben considerar lineamientos que ayuden a fortalecer el diseño de los laboratorios de informática forense, debido a que estos elementos sirven como apoyo para robustecer estas áreas periciales, estos pueden ser el uso de un modelo de trabajo, normas estandarizadas, buenas prácticas y metodologías forenses.

4.2.1 Modelo de trabajo de un LIF

Cualquier laboratorio de informática forense debe de tener un modelo de trabajo, en vista de hacer posible seguir los lineamientos entre todos los miembros del área.

A continuación, en la Figura 7 se puede observar seis factores a tener en cuenta para el modelo de trabajo:

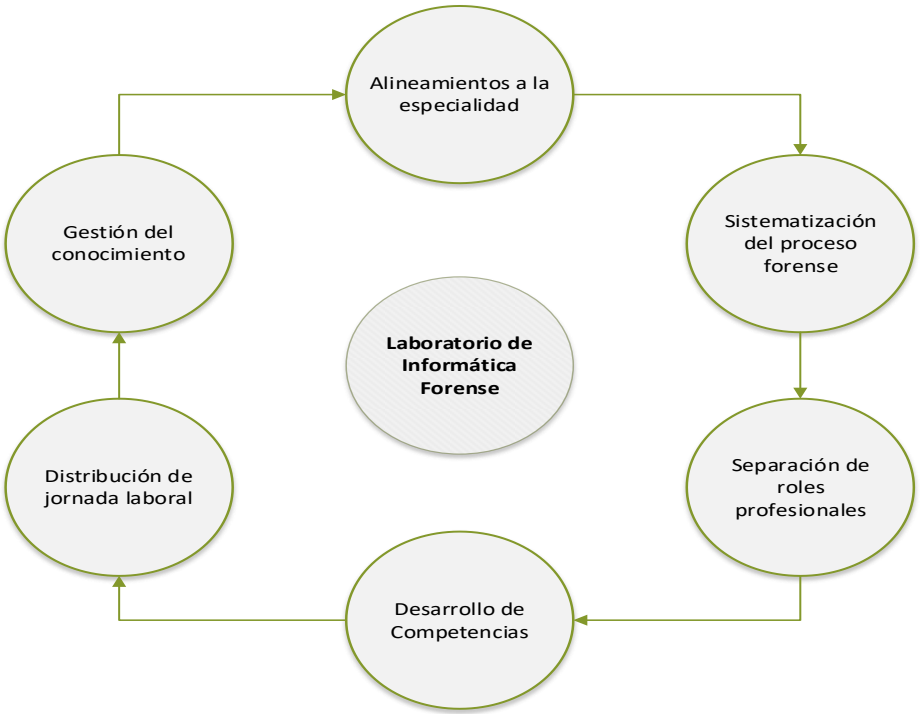


Figura 7. Modelo de Trabajo de un LIF

Fuente: Lineamientos para la creación de laboratorios informáticos forenses.

1. **Alineamientos a la Especialidad:** Se toman en cuenta todo tipo de principios de la misma como buenas prácticas, manuales de operación y procedimientos estandarizados [46].
2. **Sistematización del Proceso Forense:** Se evalúan técnicas forenses, herramientas y metodologías [46].
3. **Separación de roles profesionales:** La consideración de las funciones que cumplen los profesionales, peritos o responsables, asistentes y el director [46].
4. **Desarrollo de Competencias:** Especificación de informes periciales, investigaciones, documentos, lineamientos de servicio y desarrollo [46].
5. **Distribución de la jornada Laboral:** Se toman en cuenta todo tipo de actividades operativas, desarrollo de informes, capacitaciones y el control de la calidad [46].

6. **Gestión de conocimiento:** Se toman en cuenta la cooperación académica, acreditaciones y la cooperación entre pares [46].

Esta serie de factores nos permitirá ofrecer un servicio de calidad a largo plazo, a la par de tener un mejor control en la gestión del personal dentro del laboratorio.

4.3 Documentación

Es de vital importancia tomar notas de todo tipo de actividades como: fechas, procedimientos, metodologías, herramientas, propósitos, nombres de las personas que manipulan las evidencias, etc. a fin de llevar un seguimiento y control de las acciones, a la vez que, reducimos potenciales errores en la gestión del incidente.

También es necesario mantener una comunicación entre los diferentes tipos de personas involucradas, donde es habitual usar dos tipos de informes:

- **Informe técnico:** Se trata de un informe con el mayor grado de precisión y detalle, describe todos los procesos realizados, poniendo énfasis las técnicas empleadas para obtener resultados, donde se deja de lado la opinión personal. Son escritos por expertos empleando términos que solo lo pueden comprender otros expertos en el tema [47].
- **Informe ejecutivo:** En este tipo de informe se redacta en forma resumida las características más sobresalientes de la investigación, se omite detalles técnicos para mejorar su comprensión. Sin embargo, debe ser conciso, fiable y entendible para cualquiera [47].

4.4 Normas relacionadas con la informática forense

Existen otras normas que tienen relación con la informática forense, mismas que tienen como objetivo el proponer procedimientos adecuados para las investigaciones y métodos para el análisis de evidencias digitales, estas son:

4.4.1 ISO/IEC 27041:2015

Está orientada a garantizar la disposición y el método adecuado para la investigación de incidentes correspondientes a la seguridad de la información, además proporcionas buenas prácticas en la definición de requisitos y describe como considerar utilizar evidencias de terceros o proveedores [48].

4.4.2 ISO/IEC 27042:2015

Proporciona directrices para analizar e interpretar las evidencias digitales. Además, orienta a seleccionar mecanismos adecuados para la demostración de las habilidades competentes del perito informático, de la misma forma, describe lo que profesional debe incluir en el informe pericial [49].

Esta norma está pensada para que el perito pueda justificar la validez de los nuevos métodos empleados durante el examen de las evidencias digitales que no se hayan tomado en consideración antes, esto debido a lo complejo que puede llegar a ser a veces obtener resultados y se tenga que recurrir a idear otras alternativas.

4.4.3 ISO/IEC 27043:2015

Se centra en proporcionar procesos y principios generales para la investigación de incidentes, en donde se describe modelos idealizados para realizar procesos comunes de investigación de evidencias digitales en diferentes escenarios, desde las fases de preparación hasta la finalización de la investigación, además de, brindar advertencias y consejos en investigaciones digitales como: Violación de la seguridad, fallos en el sistema, accesos no autorizados, datos corruptos, entre otras [50].

A pesar de no detallar los principios y procesos que conlleva esta norma, se pueden usar otras normas internacionales relevantes que hagan referencias a la ISO 27043, donde detallen más sobre estos temas en investigaciones específicas.

4.5 Guías de buenas practicas

Son guías y recomendaciones relacionado a la adquisición de evidencia digital, adaptables al ambiente de trabajo con respecto a los involucrados, es importante tener en cuenta estas buenas prácticas, debido a que el mal manejo de las evidencias por parte del personal de la organización o institución puede llevar a comprometer la validez de los pocos datos relevantes recolectados.

4.5.1 NCJ 199408

Publicada por el Departamento de Justicia de los Estados Unidos en 2004 como una guía de buenas prácticas, en donde se mencionan procedimientos para la obtener, preservar, analizar y presentar la evidencia digital. También se desarrollan políticas y proponen el uso de diversas planillas en las distintas fases de la evidencia en su vida útil [51].

4.5.2 NCJ 219941

También publicada por el Departamento de Justicia de los Estados Unidos en el año 2008, en la cual se detalla los distintos dispositivos tecnológicos que pueden almacenar evidencias digitales, de la misma manera, especifica los procedimientos necesarios para para su recolección en la escena. Además, describe la evidencia digital que se pueden encontrar de los diversos tipos de delitos informáticos [51].

4.5.3 NIST 7387 & NIST 7559

Publicadas por el Instituto Nacional de Normas y Tecnología o por su nombre en inglés, National Institute of Standards and Technology (NIST), donde presenta guías de buenas prácticas como la NIST 7387, cual está relacionada con la investigación de los distintos dispositivos móviles y smartphones, donde propone herramientas necesarias para llevar a cabo un análisis forense, como también las técnicas y procedimientos para conservar, adquirir, analizar y realizar informes. De la misma forma publico la guía NIST 7559, la

cual está orientada a ofrecer información para realizar análisis de dispositivos asociados a la prestación de servicios web [51].

4.5.4 Scientific Working Group on Digital Evidence

Conocido también como SWGDE, donde se pueden encontrar una gran cantidad de guías de buenas prácticas desarrolladas por profesionales con respecto a la evidencia digital donde se puede hallar el análisis forense para computadoras "*Best Practice for Computer Forensic Acquisitions*" [52], también prácticas para la recolección de evidencia digital "*Best Practice for Digital Evidence Collection*" [53], otras guías como la adquisición de evidencia de servicios en la nube, como también la obtención de datos de ubicación inversa de Google con fines de investigación, por mencionar algunos.

4.5.5 ACPO - Good Practice Guide for Digital Evidence

Desarrollada por la Association of Chief Police Officers (ACPO), donde se describen procedimientos para identificar, incautar, recuperar y analizar la evidencia digital almacenada en los distintos dispositivos informáticos, de la misma manera se habla ciberdelitos relacionados con foros, blogs y sitios web y como desarrollar un análisis de redes [54].

4.5.6 RFC 3227

Esta guía de alto nivel centrada en la recolección y el archivado de las evidencias, desarrollada en el año 2002. Este documento proporciona buenas prácticas para definir los datos volátiles, elegir que recopilar, como recolectar y además como determinar la documentación y almacenamiento de dichos datos [55].

4.6 Metodologías forenses

Cualquier Laboratorio de Informática Forense debe poseer una metodología con la cual poder realizar los procesos y el tratamiento de la evidencia digital que se está investigando. Existe muchos modelos a tener en cuenta.

4.6.1 Modelo Publicado por el U.S Departement of Justice

Fue publicado en el año 2001 por el Departamento de Justicia de los Estados Unidos [56], donde se trata de un modelo sencillo de entender y aplicar, en vista que básicamente cuenta con 4 elementos que son clave para realizar un análisis forense, ver Figura 8.

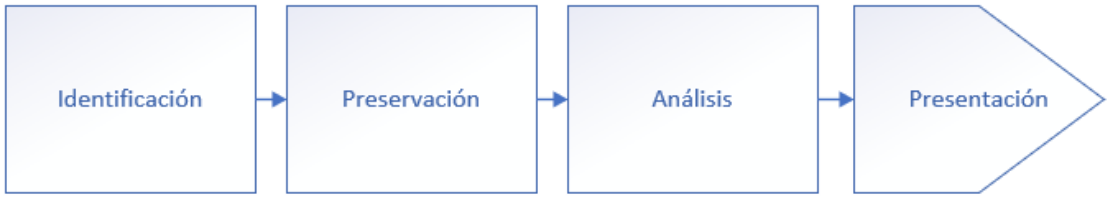


Figura 8. Fases del modelo del U.S Departament of Justice

Fuente: Autor

Este modelo fue clave para lograr establecer las bases en este campo, además sirvió de ejemplo para que otros autores desarrollaran sus propios modelos de investigación forense en dispositivos tecnológicos.

4.6.2 Modelo de DFRWS (2001)

DFRWS o Forensics Digital Research Workshop, no se trata de un modelo definitivo, al contrario, sirve como base o soporte para definir un modelo más completo a futuro. Es un modelo lineal sin embargo se menciona una retroalimentación de los pasos previos cuando es necesario [57]. Consta de 7 pasos:

1. Identificación.
2. Preservación.
3. Colección.

4. Examen.
5. Análisis.
6. Presentación.
7. Decisión.

4.6.3 Modelo Brian Carrier y Eugene Spafford (2003)

Este modelo consta de 5 grupos, mismos que están divididos en varias fases.

1. **Fase de Preparación:** Esta fase tiene como objetivo es garantizar que la infraestructura y operaciones estén listas para cumplir con una investigación completa [58].
    - Fase de Preparación de Operaciones.
    - Fase de Preparación de Infraestructuras.
2. **Fase de Despliegue:** Cuyo fin de esta fase es facilitar mecanismos para que los incidentes sean detectados y confirmados [58].
    - Fase de Detección y Notificación.
    - Fase de Confirmación y Autorización.
3. **Fase de Investigación Física de la escena del crimen**: La función de esta fase es poder recopilar y analizar todo tipo de evidencias físicas, con la intensión de reconstruir las acciones que tuvieron lugar en el transcurso del acontecimiento en su respectivo momento [58].
    - Fase de Conservación.
    - Fase de Inspección.
    - Fase de Búsqueda y Recolección.
    - Fase de Documentación.
    - Fase de Reconstrucción.
    - Fase de Presentación.

4. **Fase de Investigación de la Escena Digital del Delito:** Igual que la fase anterior, sin embargo, esta se encuentra encargada de recopilar y analizar todo tipo de evidencia digital a través de las evidencias obtenidas en la Fase de Investigación Física [58].
    - Fase de Conservación.
    - Fase de Inspección.
    - Fase de Documentación
    - Fase de Búsqueda y Recolección.
    - Fase de Reconstrucción.
    - Fase de Presentación.
5. **Fase de Revisión:** En esta fase se hace una revisión de la investigación completa con el objetivo de identificar áreas en las que se puedan mejorar [58].

4.6.4 Modelo Extendido de Séamus ó Ciardhuáin

Presentado en el año 2004, una versión mejorada a partir de sus anteriores metodologías, se trata de un modelo en cascada tardándose de 13 etapas. Este modelo se enfoca en cubrir todas las fases del procesamiento de la evidencia digital [59].

Las etapas son las siguientes:

1. La conciencia.
2. Autorización.
3. Planificación.
4. La notificación.
5. Buscar e identificar la prueba.
6. Colección de pruebas.
7. Transporte de pruebas.

8. Almacenamiento de pruebas.
9. Examen de la prueba.
10. Hipótesis.
11. Presentación de hipótesis.
12. Defensa de la hipótesis
13. Diseminación de la información

4.6.5 Modelo SANS

Desarrollada por el instituto SANS, organización que es encuentra encargada de educar a profesionales en seguridad y cooperación de la investigación. El modelo de SANS consta de 8 pasos que sigue de forma ordenada, con el fin de presentar de manera apropiada toda la evidencia del caso [60], cuyos pasos son:

1. Verificación.
2. Descripción del sistema.
3. Adquisición de evidencia.
4. Análisis de línea de tiempo.
5. Análisis de medios y artefactos.
6. Búsqueda de cadenas o bytes.
7. Recuperación de datos.
8. Informe de resultados.

4.6.6 Modelo de Casey (2004)

Evoluciono de su primer modelo publicado en 2001, este consta de 6 pasos, que son:

1. Autorización y preparación
2. Identificación
3. Documentación, Adquisición y Conservación

4. Extracción de la información y Análisis
5. Reconstrucción
6. Publicación de conclusiones

Toda la información obtenida en las diferentes fases puede dar paso a la siguiente fase como también volver a la anterior, esto debido a que la información conseguida en cualquier etapa puede servir para conseguir más datos existentes en las fases anteriores. De la misma forma toda información debe ser debidamente documentada a fin ser utilizada en la publicación final [61].

4.7 Cuadro comparativo entre las metodologías

A continuación, se observa una comparativa entre las diferentes metodologías presentadas, comparados en los 4 principios básicos presentados por el modelo del Departamento de Justicia de Estados Unidos. Ver Tabla 14**.**

Fases del análisis forense	**Metodologías**				
	Modelo DFRWS	Modelo Brian Carreir y Eugene Spafford	Modelo Extendido de Séamus ó Ciardhuáin	Modelo SANS	Modelo de Casey (2004)
Identificación	✓		✓	✓	✓
Recolección	✓	✓	✓	✓	✓
Análisis	✓	✓	✓	✓	✓
Presentación	✓	✓	✓	✓	✓

Tabla 14. Comparación de las metodologías para el análisis forense

Fuente: Autor

- El Modelo DFRWS, como ya se ha mencionado antes, no se trata de un modelo definitivo, sino más bien de un modelo que ayuda a definir que metodología usar a futuro.
- El Modelo de Brian Carreir y Eugene Spafford, está enfocada en estar preparado para el tratamiento de la evidencia y más no en su identificación.
- El Modelo extendido de Séamus ó Ciardhuán, trata de cubrir todos los aspectos de la investigación e inclusive acopla la cadena de custodia que rige dicho país en donde se vaya a emplearse dicha metodología.
- La metodología SANS esta metodología es exclusiva para sistemas operativos como Windows y Linux, dejando de lado a los dispositivos móviles.
- El Modelo Casey (2004) cubre todos los pasos para una investigación forense, a la vez que este modelo es uno no lineal, es decir, permite volver a cualquier etapa de la metodología a fin de conseguir datos.

Al decidir por cual modelo usar, se debe tener en cuenta que se debe cumplir al menos las etapas de identificación y recolección. Otra alternativa es la de combinar metodologías, como, por ejemplo, el Modelo extendido de Séamus ó Ciardhuán con el Modelo Casey (2004) con el objetivo de cubrir tanto el tratamiento y transporte de las evidencias como la retroalimentación y presentación de la información obtenida, para cubrir todos procedimientos necesarios.

Incluso se tiene la posibilidad de generar un modelo propio para trabajar dentro del laboratorio de informática forense.

4.8 Propuesta de Metodología para ser usada dentro del LIF

La propuesta de un modelo para el laboratorio de informática forense está conformada por seis fases (I Aseguramiento del área; II Identificación y Recolección de evidencia; III

Transporte de las evidencias; IV Preservación de la evidencia; V Examen y Análisis de la evidencia; VI Presentación de evidencias e Informes) y una subfase (Documentación), mismas que se describirán a continuación:

1. **Aseguramiento del área:** Aprobada la solicitud del caso, el especialista se acerca a la escena del suceso para evitar que se contamine las evidencias, a la vez de asegurar el área, además también establece protocolos como:

- Solo ingresó de personal autorizado
- Proteger las huellas dactilares
- Fotografiar todos los dispositivos intactos y el lugar de los acontecimientos.

- Documentar con detalle todo evento que ocurra dentro de la escena, también anotar los nombres de las personas involucradas en la escena, incluso el nombre del que llego a asegurar el lugar. (ver Anexo A)

2. **Identificación y Recolección de la evidencia:** Identificar todo tipo de dispositivo que pueda contener evidencia crucial para la investigación, tener presente que algunas evidencias pueden ser o no volátiles, tales como:

- Unidades de almacenamiento (USB, DVD, Discos duros externos, etc.)
- Dispositivos electrónicos (PC, Smartphones, Tablet, etc.)
- Correos electrónicos.
- Logs y eventos del sistema.
- Redes sociales, historiales, mensajes, etc.

- Documentar los equipos implicados con la escena y enlistar los nombres de sus propietarios.

Para la recolección de las evidencias se debe tener mucho cuidado con modificar las pruebas, establecer condiciones y procedimientos adecuados para el tratamiento de las evidencias, de la misma forma usar herramientas de hardware y software

apropiados para dicha manipulación. Cabe aclara que las evidencias se pueden extraer de dispositivos tanto encendidos como apagados. Se debe tener en cuenta:

- El orden de la recolección de evidencia.
- Si la evidencia es volátil, no apagar el dispositivo y recolectar las pruebas en ese momento.
- Hacer una imagen forense (Copia exacta del dispositivo bit a bit) o clonar el disco duro con las evidencias no volátiles para no dañar la integridad de las evidencias.
- Etiquetar cada dispositivo con el tipo de evidencia (Volátil/no Volátil).
- Documentar los procedimientos realizados, las herramientas utilizadas y la persona que haya hecho la recolección. (ver Anexo B)

3. **Transporte de la evidencia:** Luego de recolectar, las evidencias se deber trasladar a un lugar seguro para su preservación y su posterior examen y análisis. Es de suma importancia asegurar el proceso de transporte a fin de asegurar la valides de la evidencia, se debe tener en cuenta también:

- No exponerlas a campos magnéticos
- Evitar daños en los equipos.
- Utilizar materiales preparadas y sujetas a la cadena de custodia (Herramientas, bolsas de embalaje, etiquetado, etc.). (ver Anexo C)
- Documentar los procesos realizados para el trasporte (Nombres de los transportistas, equipos transportados, fechas/hora, etc.).

4. **Preservación de la evidencia:** Tener cuidado con la manipulación de la evidencia, un mal manejo de la misma puede invalidarlas. Se debe almacenar y resguardar las evidencias, para garantizar su autenticidad, integridad y utilidad para usarlas frente al tribunal, debido a que son la prueba original.

- Emplear y cumplir la cadena de custodia vigente del país, para evitar el rechazo de las pruebas.
- Asegurar su conservación sin tiempo definido.
- Crear respaldos**.**
- Resguardarlas en un lugar seguro con condiciones ambientales propicias.

- Documentar el estado de la evidencias y ciertas observaciones que puedan existir al momento de llegar al lugar de resguardo. (ver Anexo D)

5. **Examen y Análisis de la evidencia:** Con las fases anteriores tendremos una visión general de lo que tenemos que buscar, por ello en el momento del examen de las evidencias se debe emplear todo tipo de técnicas como también de herramientas pertinentes con el objetivo de encontrar pruebas significativas, no está demás decir que esto se lo realiza con las imágenes forenses con el propósito de no modificar la evidencia original.

- Documentar las herramientas, técnicas, procesos, nombres de la persona encargada con fecha y hora, utilizando bitácoras.

  El análisis de evidencias es de gran importancia, debido a que en esta fase se interpreta de manera ética y responsable la información obtenida de las evidencias examinadas. Se deben alcanzar pruebas relevantes que ayuden a determinar lo acontecido, con el objetivo de encontrar el autor, que hizo, como lo hizo, porque lo hizo, que consiguió y quien fue el afectado.

- Documentar los hallazgos más significativos de las distintas evidencias. (Ver Anexo E)

6. **Presentación de evidencias e informes:** En esta última etapa es la presentación de informes, donde se recurrirá a toda la documentación realizada a lo largo de todas las 5 etapas, en virtud de generar un informe detallado pero conciso de todo

lo realizado desde el primer contacto de las evidencias hasta los exámenes y análisis ejecutados, logrando así demostrar el cuidado y los procedimientos cumplidos hasta llegar a la presentación de la evidencia. Esta parte es muy importante debido a que es un informe que contiene resultados y conclusiones finales, además, será presentado ante el tribunal. También se debe tener en cuenta:

- Determinar el tipo de informe (Técnico o Ejecutivo), acorde a quien va dirigido, para así evitar desentendimientos por personas que no tengan los conocimientos técnicos.
- Deben presentarse con las evidencias que no puedan ser plasmados en papel, como audios y videos, a fin de dar soporte al informe.
- Incluir recomendaciones de prevención y seguridad para evitar a que vuelva a ocurrir.

A continuación, una vista general del modelo, ver Figura 9.

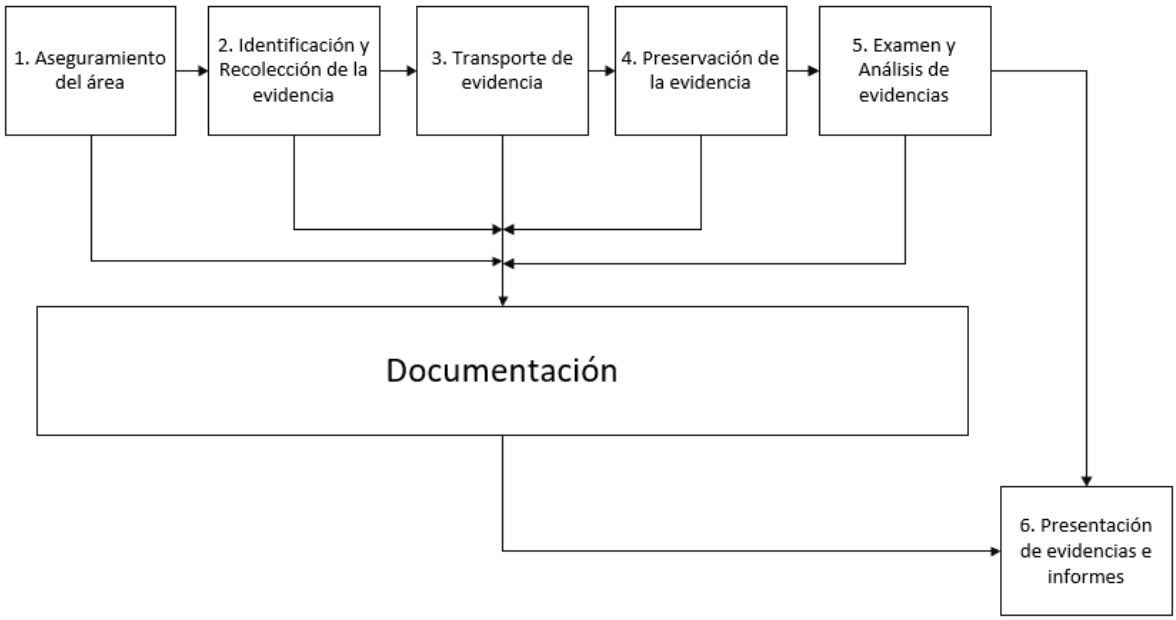


Figura 9. Modelo propuesto

Fuente: Autor

4.9 Propuesta de organización del personal para el LIF

Los miembros del Laboratorio de Informática Forense deberán tener conocimientos de leyes, procesos legales y normas correspondientes, se manejarán con la metodología acordada, además de contar con avanzados conocimientos en el área de la informática forense y de la tecnología tanto de software como de hardware.

La organización se empleará de la siguiente manera, ver Figura 10.

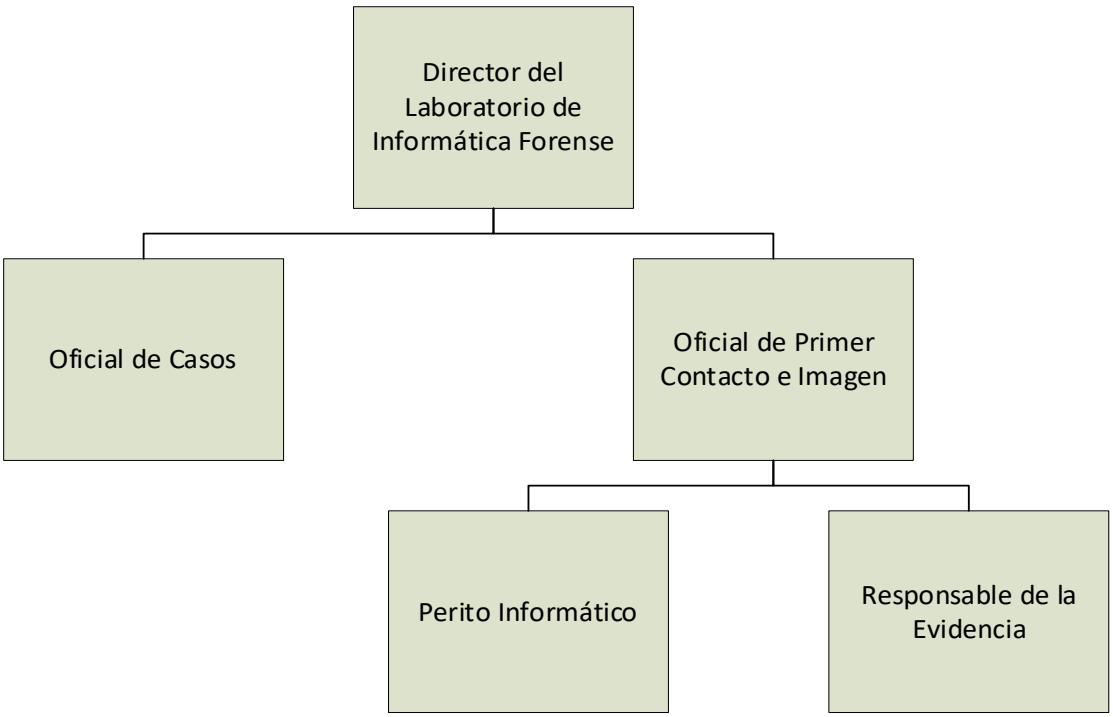


Figura 10. Organización Jerárquica del Laboratorio de Informática Forense

Fuente: Autor.

- **Director del Laboratorio de Informática Forense:** Líder del laboratorio, encargado de garantizar el funcionamiento del área forense, también de asegura la ética y la responsabilidad de los miembros, el mantenimiento de los equipos, distribución de responsabilidades y presupuestos [62].
- **Oficial de Casos:** Encargado de la asignación de actividades y las prioridades de los casos entre el personal del laboratorio, también se encargará de aceptar o negar

incidentes que lleguen, de la misma forma comunicará el estado de los casos al director [62].

- **Oficial de Primer Contacto e Imagen:** El primero en tener contacto del área del crimen, responsable de establecer los protocolos correspondientes**,** y encargado de generar copias (imágenes forenses) de las evidencias [62].
- **Perito Informático / Investigador:** Persona con alto conocimientos de la tecnología, también con avanzados conocimientos en informática forense, encargado de extraer todo tipo de evidencias o información necesaria que ayude a reconstruir los acontecimientos del crimen. También encargado de generar informes a fin de ser utilizadas en un tribunal [62].
- **Responsable de la Evidencia:** Encargado de mantener las evidencias a salvo, también es responsable de documentar fecha y hora de las evidencias que han sido solicitadas y por quien.

4.10 Diseño interno del Laboratorio de Informática Forense

Para el diseño interno del Laboratorio de Informática Forense se ha considerado varios aspectos, como la seguridad física, condiciones ambientales, infraestructura y otros aspectos necesarios para la creación adecuada de un LIF, a fin de garantizar la integridad de las evidencias y buen manejo de las mismas.

4.10.1 Seguridad Física

La seguridad Física es de vital importancia, debido a que, en el laboratorio existe todo tipo de evidencias que son fundamentales para demostrar la inocencia o culpabilidad en un delito informático. En una investigación realizada en la cuidad de Pereira donde se determinaba la viabilidad de la implementación de un laboratorio de informática forense, el autor establecido una serie de medidas de seguridad físicas para tomar en cuenta a fin

que solo ingrese personal autorizado, evitando así algún daño, alteración o perdidas de las evidencias [63], estas medidas de seguridad son:

- **Acceso por medio de un Sistema Biométrico y cerradura automática:** Un sistema de seguridad fiable, con el que se puede registrar y autorizar la entrada y salida del personal al laboratorio.
- **Sistema de Videograbación:** Las cámaras deben funcionar las 24/7 y solo el director del laboratorio podrá acceder a las grabaciones para consultar los eventos ocurridos dentro las diferentes áreas del LIF.
- **Sistema de alarmas:** Un sistema de seguridad que este intercomunicado con la policía.
- **Identificación:** El personal deberá portar una credencial que acredite que es personal del LIF.
- **Otras consideraciones:** Las personas que se quieran comunicar con el personal del laboratorio lo deberán hacer en áreas anexas, se llevará un registro con nombre, motivo, fecha y firma de la persona y el personal que fue solicitado. (ver Anexo F). Además de contar con un servicio de emergencias en casos de incidentes.

4.10.2 Infraestructura interna

Por otro lado, el laboratorio debe de contar con los siguientes elementos:

- **Una propia conexión a red:** Una conexión robusta y propia para cualquier tipo de investigación, comunicación de información que tenga que llevar a cabo el personal [63].
- **Generador eléctrico o UPS para el bloque central:** Si por alguna razón, se queda sin energía eléctrica, el generador suministrará electricidad [63].

- **Cableado Telefónico**: Para las comunicaciones externas/internas mediante códigos de seguridad [63].
- **Habitación**: En lo posible que la habitación no tenga ventanas, esto con el objetivo de asegurar la privacidad de las evidencias y asegurarse que el techo no tenga la posibilidad de caer algún tipo de elemento contaminante [63].

4.10.3 Condiciones ambientales

El laboratorio de informática forense debe contar iluminación adecuada; humedad y temperatura apropiada; ventilación y energía eléctrica óptima, debido a que se está manejando con dispositivos eléctricos y electrónicos sensibles a cambios ambientales. Por ello se debe tomar en cuenta las siguientes consideraciones:

- Asegurarse que la temperatura dentro del laboratorio sea entre 18 ºC y 30 ºC, idóneos para el buen funcionamiento de los equipos de cómputo y el bienestar de los operarios, en lo posible mantener una temperatura ambiental de 22 ºC para mantener los niveles de humedad en un 60% [63], esto con el objetivo de proteger a los aparatos electrónicos de la corrosión por altos niveles de humedad y las descargas estáticas que pueden causar los bajos niveles de la misma.
- Para la iluminación general del laboratorio debe de contar con techos de color blanco para activar la reflexión, a la vez que las paredes deben de contener colores tenues, para que exista una iluminación uniforme en los espacios de trabajo. También combinar con una iluminación focal en las distintas áreas, esta es una luz un poco más intensa y directa que permite trabajar de mejor manera. Elegir lámparas LED de luces blancas de entre 3,000 y 4 000 º K, con una intensidad lumínica entre 500 y 750 Lux [64].
- Evitar interferencia de radiofrecuencia y electromagnética en las evidencias.

- Instalar material aislante que eviten la propagación de las vibraciones y ruidos dentro del laboratorio.
- Esterilizar los puestos de trabajo.
- Utilizar extintores de polvo químico (mismos que ya cuenta la Universidad).

4.10.4 Áreas del LIF

Luego de mencionar todos estos aspectos y de determinar cuál laboratorio es el más idóneo, se ha procedido a realizar un diseño del Laboratorio de Informática Forense, el cual está dividido en diferentes áreas, con el fin que cada lugar que se detalla en la ilustración está diseñado para realizar una actividad importante, mismas que se describirán después de la figura. Ver Figura 11.

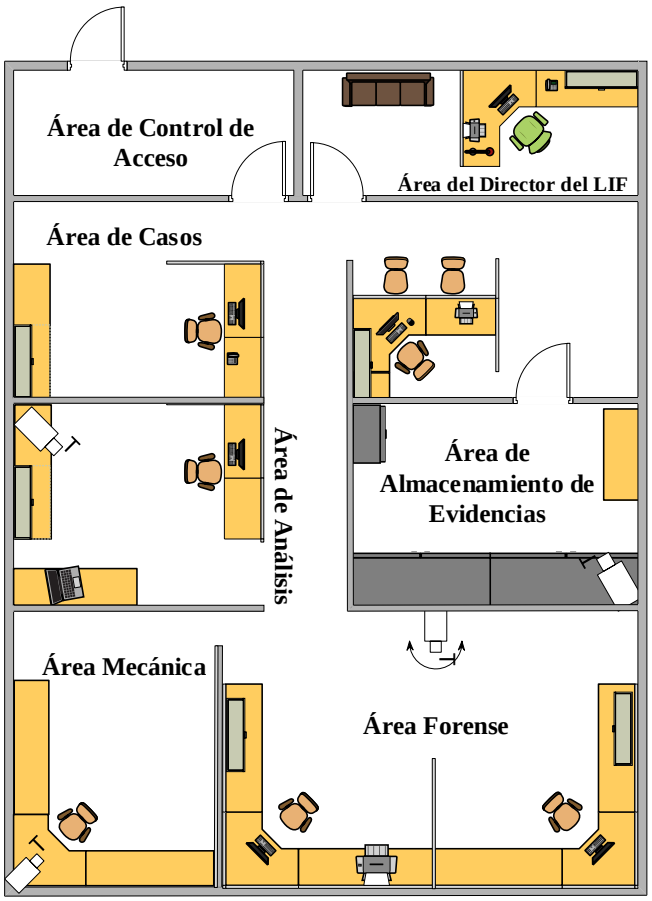


Figura 11. Diseño interno del LIF

Fuente: Autor.

- **Área de Control de Acceso.**

En esta área se controla el acceso a solo el personal autorizado, además, es donde se contará con el sistema biométrico para registrar la entrada y salida de los mismos.

- **Área del director del LIF.**

Es el sitio del director de Laboratorio de Informática Forense, en este lugar se tendrá el acceso a las grabaciones de las videocámaras, de la misma forma, es donde se supervisará el funcionamiento de las demás áreas.

- **Área de Casos.**

Está destinado para el oficial de casos y en este se tendrá los registros de los casos que se estén investigando dentro del laboratorio, como también, la priorización de las actividades de las otras áreas.

- **Área de Análisis.**

Lugar donde el oficial de primer contacto e imagen se encuentra, este cuenta con software pertinente para realizar imágenes forenses de las evidencias para posteriormente guardarlas en el área de almacenamiento, también en este sitio posee hardware preparado y listo para cuando el oficial tenga que salir a la escena.

- **Área de Almacenamiento de Evidencias.**

En esta área es donde encontrarán bajo custodia todo tipo de evidencia que haya llegado al LIF, aquí se guardarán en casilleros metálicos y estarán bajo grabación 24/7. Para acceder a ellos se debe primero llenar un registro con fecha/hora, la evidencia solicitada y el nombre de la persona de quien solicita, (ver Anexo G). En este lugar se encuentra la persona responsable de las evidencias, mismo que realizara la supervisión, registros y protección de las pruebas.

- **Área Mecánica.**

Este sitio está destinado al desmontaje, ensamble y el manejo físico de equipos de cómputo o dispositivos móviles que lo requieran.

- **Área Forense.**

Esta área se encuentran los peritos informáticos / investigadores, donde contarán con equipos de cómputo con software que permita desarrollar la investigación, como también herramientas de hardware si así lo requiere.

Aspectos del Laboratorio: La habitación cuenta con ventanas altas que imposibilita la visualización del interior del laboratorio, esto sumado a que se encuentra en el primer piso del Bloque Central, lo que asegura que las actividades que se realicen dentro de las áreas sean totalmente confidenciales. También, cuenta con cielo raso por lo que es necesario asegurarse que no exista aberturas donde puedan caer elementos contaminantes que puedan dañar las evidencias.

4.10.5 Requisitos legales

La norma ISO/IEC 17025, es una guía de referencia para todo tipo de laboratorio que necesite demostrar que operan de manera competente y tienen la capacidad de obtener resultados válidos. Donde se describe una gran cantidad de requisitos como el personal, instalaciones, condiciones ambientales, equipamiento etc. Además, es aplicable sin estimar la cantidad del personal en cualquier tipo de sector como: Construcción, Telecomunicación, Energía, Transporte, Ciencias forenses, entre otras más [65].

Por otra parte, la Sociedad Estadounidense de Directores de Laboratorios Criminalísticos (ASCLD) trata de una sociedad de profesionales sin fines de lucro que buscan fomentar el interés, desarrollo, técnicas de gestión para los laboratorios, cual cuenta con un

programa de acreditación de laboratorios de criminalística tanto para sectores públicos y privados [66]. (ver Anexo H)

Por lo que el laboratorio debe adherirse a los estándares de ISO/IEC 17025:2017 y ASCLD/LAB, en lo posible conseguir las certificaciones correspondientes por medio de la prestación de servicios de calidad que cumplan con requerimientos de nivel nacional e internacional.

4.11 Propuesta de adquisición

En la actualidad existe una gran variedad de hardware y software que son de gran utilidad en un análisis digital, estas mismas hacen que el trabajo realizado sea más preciso debido a que, apoyan a la recolección de evidencias, como también la extracción y el análisis del mismo. Por lo que, para consolidar el diseño del Laboratorio de Informática Forense anteriormente presentado, se propone la adquisición de herramientas tanto de hardware como de software de uso libre o con licencia para esta área, a fin de lograr encontrar pruebas de que los autores cometieron algún delito informático y estos mismos sean penados por la ley ecuatoriana.

4.11.1 Herramientas de Hardware para el LIF

- **Black hole Faraday bag kit**

  Bolsas aislantes ante señales de radiofrecuencias para computadoras portátiles, tabletas, dispositivos móviles, etc. Son utilizadas para la incautación, transporte y conservación de las evidencias. Duraderas y livianas para su uso tanto en el laboratorio como en el lugar de la investigación [67]. Ver Figura 12.

Figura 12. Black hole Faraday bag

Fuente: Forensic Store.

- **Clonador Discos duros**

Este dispositivo puede clonar discos duros o SSD de 2,5” y de 3.5” con alta capacidad a gran velocidad, necesario para no manipular la evidencia original. Puede operar de manera autónoma e independientemente de los sistemas operativo. Se debe tener en cuenta que las unidades de almacenamiento de destino deben ser mayor o igual a las de origen [68]. Ver Figura 13.

Figura 13. Duplicador y Sanitizador Autónomo de Discos Duros de 2,5/3,5" de 2 Bahías HDD/SSD

Fuente: StarTech.com.

- **Wiebetech USB Writer Blocker**

Hace posible examinar, ver y generar imágenes de todo tipo de unidades Flash USB de forma sencilla y rápida, además que protege y no altera los datos. También permite a los investigadores revisar el contenido de las unidades que no puedan ser eliminadas de los

puertos USB, por medio del SO Windows, impidiendo que se dañe o interrumpa los datos de origen [69]. Ver Figura 14.

Figura 14. USB 3.1 WriteBlocker

Fuente: WiebeTech.

- **Adaptador y lector para recuperación de datos móviles.**

Se trata de una herramienta para lectura de datos para chip de memoria Android: eMMC153/169, eMCP162/186, eMCP221, eMCP529, sirve para restaurar datos móviles como: mensajes, fotos, SMS, videos, datos de aplicaciones, registros de llamadas, etc., de aquellos celulares que no enciendan, dañados, mojados, rotos o tengan algún otro daño físico [70].Ver Figura 15.

Figura 15. Adaptador de chip de memoria eMMC153/169

Fuente: ALLSOCKET.

Esta herramienta es compatible con softwares de recuperación de datos como: WinHex, Superdatarecovery, r-studio, 7-Datarecovery, etc.

- **Portátil forense FRED L**

Es una computadora portátil de recuperación de evidencias con gran rendimiento, está diseñada para el trabajo forense, posibilita la clasificación, adquisición y análisis de las evidencias digitales [71]. Ver Figura 16.

Figura 16. Portátil forense FRED L

Fuente: Digital Intelligence.

Esta portátil cuenta con:

- **CPU:** Intel i7-11800h 8 núcleos 2,3 GHz (4,6 Turbo), Cache de 24 MB.
- **Sistema Operativo:** Windows 10 Pro de 64 bits.
- **Mainboard:** Conjunto de chips Intel HM570 Express.
- **RAM:** 64 GB PC4-25600 DDR4.
- **Tarjeta Gráfica:** NVIDIA GeForce RTX 3060 6GB GDDR6
- **Almacenamiento:** SSD 500GB

Será de mucha utilidad para cuando el personal tenga que salir a alguna área designada según el caso que se presente.

4.11.2 Herramientas de Software para el LIF

Existe una gran variedad de softwares para la realizar investigaciones forenses, incluso sistemas operativos que ya contienen aplicaciones de uso libre, mismos que nos serán

útiles para el diseño del Laboratorio de Informática Forense. A continuación, se describirán un par de estos.

- **CAINE**

Este es un sistema operativo Open Source, basado en Linux y está completamente orientado a la informática forense, este mismo contienen una gran variedad de software para realizar análisis forenses completos. Proporciona una interfaz amigable para el usuario y sencilla de utilizar. Las herramientas que podemos encontrar en esta tenemos: Autopsy, The Sleuth, Wireshark, RegRipper, AutoMacTc, Binlocker, Fsstat, PhotoRec entre otras más [72]. Ver Figura 17.

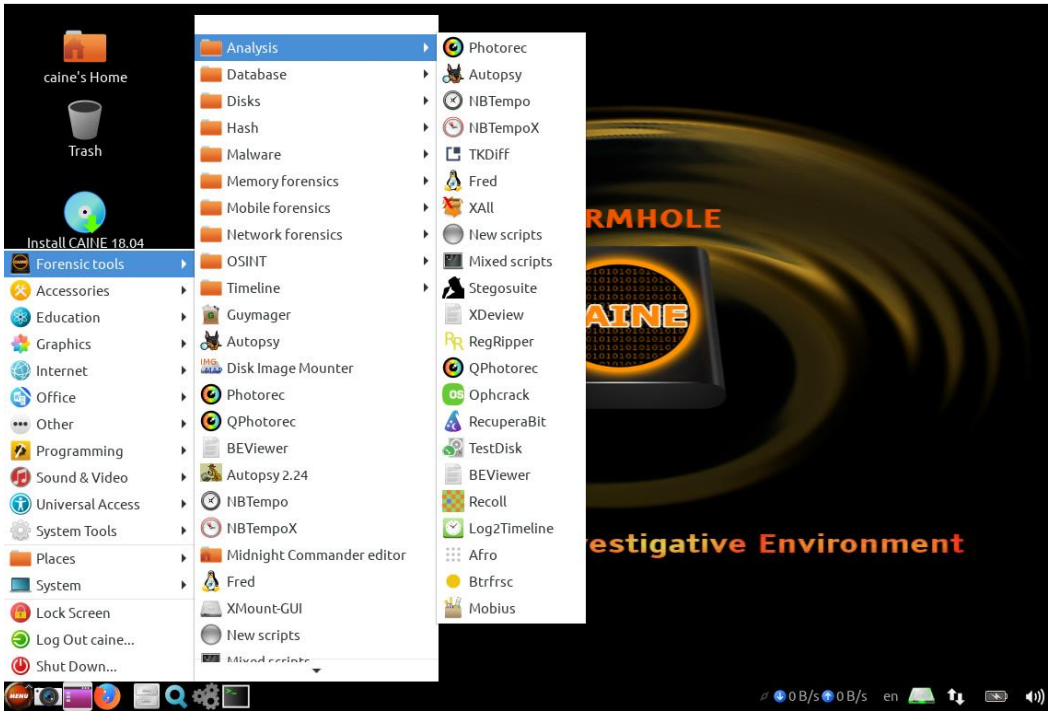


Figura 17. Softwares que contiene CAINE

Fuente: Computer Forensics Linux Live Distro, CAINE.

Además, CAINE también posee herramientas que pueden ser ejecutadas directamente en Windows, como: FTK Imager, Windows File Analyzer, Photorec & TestDisk y muchas más.

- **KALI LINUX**

Es un sistema operativo Open Source, utilizado tanto para pentesting como para la informática forense. Una de las grandes propiedades que tiene Kali Linux es la de disponer de un modo Live para realizar análisis forenses, también evita la escritura en nuestros discos duros internos, de la misma forma evita que los almacenamientos extraíbles se monten de manera automática, permitiéndonos hacerlo de manera manual. Al igual que el anterior, contiene una gran variedad de herramientas forenses que nos ayudaran en nuestra investigación [73]. Ver Figura 18.

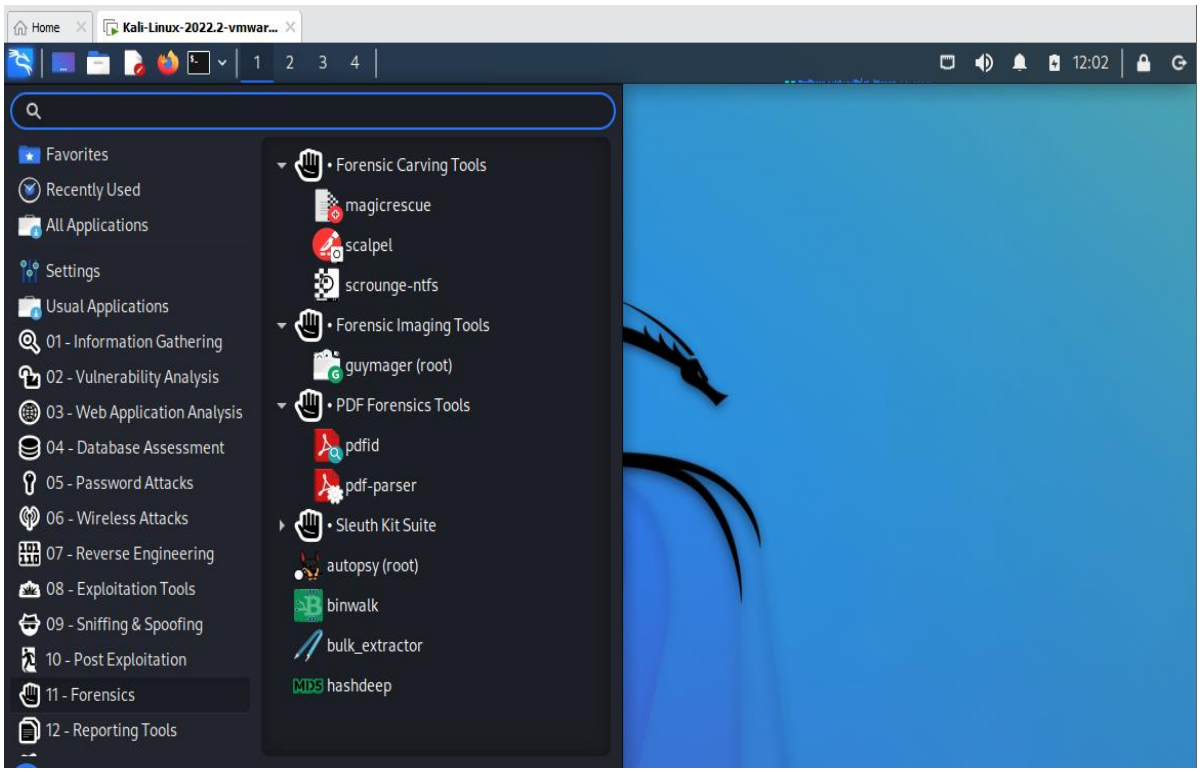


Figura 18. Softwares que contiene Kali Linux

Fuente: Autor.

Podemos utilizar ambos sistemas operativos por medio de máquinas virtuales a fin de aprovechar todas las herramientas que ya contienen estas mismas, a fin de cumplir con las investigaciones.

Herramientas de Software para el análisis forense.

Por otro lado, también se propondrán herramientas tanto de uso libre como de pago, con el objetivo de fortalecer el diseño del LIF y que nos ayudarán en las tareas forenses que requerimos.

- **Oxygen Forensics Detective**

Es un software forense que fue creado para la extracción, decodificación y el análisis de datos de una gran variedad de smartphones, dispositivos IoT, tarjetas de medios, servicios en la nube, drones, entre otras más. También, este software puede eludir bloqueos de pantalla, desvelar datos eliminados, descubrir contraseñas, extraer y analizar información de las aplicaciones más populares, puede hallar conexiones sociales, categorizar imágenes y generar líneas de tiempo [74]. Ver Figura 19.

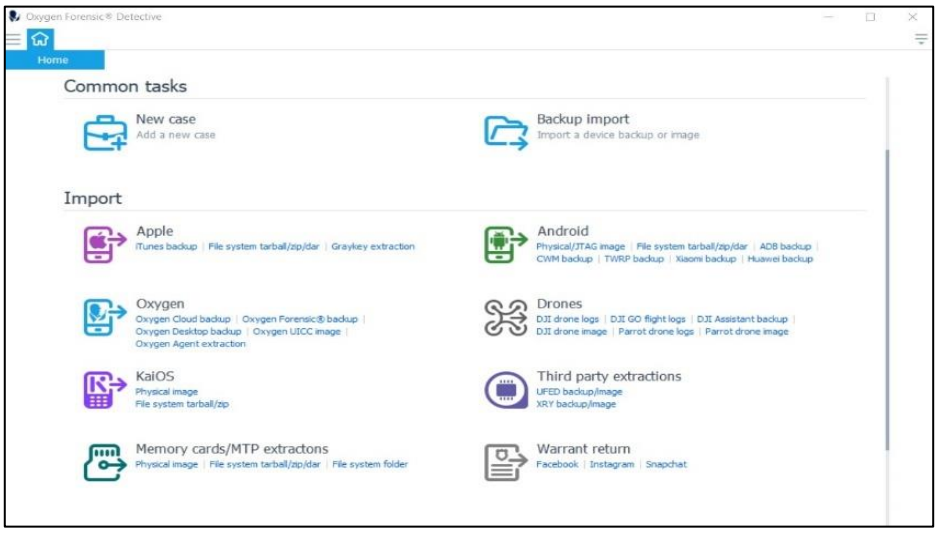


Figura 19. Backups e imágenes de importación

Fuente: Oxygen Forensics.

- **FTK Imager**

Es una herramienta de Access Data, cuyo propósito la visualización previa de datos recuperados de cualquier tipo de disco duro, CD, DVD, memorias USB, etc., con el fin de poder crear replicas (Imágenes forenses) de estas unidades sin generar cambios en la evidencia original, para su posterior análisis [75].

- **Autopsy**

Es una plataforma digital forense con múltiples aplicaciones que nos serán de ayuda para el análisis forense de imágenes de discos duros, funciona en los distintos sistemas operativos como: Windows, Linux, Mac OS, etc. También nos permite añadir módulos a fin de cubrir necesidades. Esta herramienta es utilizada por militares, policías e incluso empresas para la investigación en un equipo [76]. Ver Figura 20.

Figura 20. Logo de Autopsy

Fuente: Autopsy.

- **EnCase Forensic**

EnCase Forensic es una potente plataforma para la investigación y análisis profundo de los archivos del usuario para recolectar evidencias como imágenes, documentos, información sobre los registros de Windows e incluso historiales de búsqueda manteniendo la integridad de la evidencia intacta, además con la posibilidad de generar informes sobre los hallazgos realizados, mismos que son válidos para ser presentados ante un tribunal [77].

- **Guasap Forensic**

Trata de una aplicación de código abierto para la realización de peritajes informáticos y autentificación de conversaciones en la red social WhatsApp, donde puede extraer bases de datos, archivos multimedia y la realización de clonado bit a bit con su respectivo hash. Asimismo, puede encontrar indicios de dispositivos rooteados, aplicaciones instaladas, mensajes borrados, líneas de tiempo con los distintos wifis conectados/desconectados e

incluso la aplicación puede generar informes en HTML [78]. Es compatible con sistemas operativos Windows y Linux.

- **Wireshark**

Wireshark es un software que permite analizar el tráfico de red, permitiendo ver la jerarquía de protocolos, estadísticas de los paquetes capturados, grafica de flujos, conversaciones entre otras más. También se caracteriza por el análisis fuera de línea y captura en vivo [79]. Además, posee una interfaz gráfica, es gratuito y se encuentra disponible para Windows, Linux, Solaris, MacOS, etc. Ver Figura 21.

Figura 21. Logo de WireShark

Fuente. WireShark

- **Elcomsoft iOS Forensic ToolKit**

Es un software que permite la obtención lógica o física de datos de dispositivos Apple IOS como: iPod Touch, iPhone, iPad, Apple Watch, etc. Esta aplicación nos permite crear imágenes bit a bit de los archivos de los dispositivos, la recolección de datos en tiempo real, extracción de datos multimedia protegidas con pin y adquisición de información como claves de cifrado, contraseñas, códigos de accesos y datos protegidos [80]. Compatibles con sistemas Windows y MacOS.

- **OSForensics**

OSForensics nos da la posibilidad de hacer un escaneo del sistema operativo completo para una investigación digital, permitiéndonos extraer todo tipo de datos forenses de computadoras de manera sencilla y rápida, además, con esta herramienta podemos

localizar pistas, visualizar archivos, organizar y analizar datos, a fin de poder generar una presentación de los hallazgos más significativos [81].

- **Event Log Explorer**

Este software permite monitorear, visualizar y analizar todo tipo de evento registrado en los Logs del sistema Windows. Este aplicativo funciona tanto con registros locales como remotos, de la misma forma facilita la lectura de los eventos directamente, lo que hace posible el acceso a incluso registros dañados. Además, nos da la posibilidad de filtrarlos por tipo de evento, parámetro, descripción e incluso exportar los registros para su presentación [82].

- **Volatility Framework**

Volatility es un framework forense que contiene una serie de herramientas de código abierto para realizar análisis de memoria Volátil (RAM). Esta nos permite enlistar conexiones de red cerradas y activas, visualizar historiales de Internet, enumerar procesos ejecutados, identificar archivos del sistema y recuperación de volcados de memoria. También ofrece la posibilidad de recuperar comandos ingresados en el CMD, capturas de pantalla, contraseñas hash, claves, entre otras más [83]. Ver Figura 22.

Figura 22. Logo de Volatility

Fuente: InfoSec Write-ups.

- **WinHex**

Es un editor hexadecimal, una herramienta muy útil en el área de la informática forense, debido a que permite recuperar archivos borrados, datos perdidos u ocultos. Este software posee varias características como: buscar, reemplazar, analizar, concatenar, unificar, comparar y dividir archivos, de la misma forma facilita la clonación de disco, imágenes y copias de seguridad [84].

- **Exiftool**

Se trata de un software Open Source con la que podemos leer, escribir y editar los metadatos que se encuentran en todo tipo de archivo digital: Videos, audios, imágenes hasta PDFs, a fin de obtener información valiosa para la investigación como: ubicación, fecha de creación/ modificación, autores, permisos, etc. Esta herramienta es ejecutable en sistemas operativos Windows, Linux, MacOS e incluso cuenta con una versión para Android, está versión siendo la única que dispone de una interfaz gráfica [85].

4.11.3 Presupuesto para la adquisición

El presupuesto necesario para la adquisición de hardware para el laboratorio de informática forense, sería el siguiente. Ver Tabla 15.

Presupuesto para la adquisición del Hardware			
Nombre	**Precio**	**Cantidad**	**Subtotal**
Black hole Faraday bag kit	$ 330	3	$ 990
Duplicador y Sanitizador Autónomo de Discos Duros de 2,5/3,5" de 2 Bahías HDD/SSD	$ 116.99	3	$ 350.97
USB 3.1 WriteBlocker	$ 399	3	$ 1,197

Lector múltiple de chips de memoria Android (4 Unidades)	$ 512	1	$ 512
Portátil forense FRED L	$ 4,999	1	$ 4,999
		Total	**$ 8,048,97**

Nota: Todos los precios están sujetos a la página oficial y/o distribuidoras.

Tabla 15. Presupuesto para la adquisición del hardware

Fuente: Autor.

- El presupuesto necesario para la adquisición de software para el laboratorio de informática forense, sería el siguiente. Ver Tabla 16.

Presupuesto para la adquisición del Software				
Nombre	**Versión Gratuita**	**Versión de Pago**	**Cantidad**	**Subtotal**
CAINE	Open Source	N/A	3	$ 0
Kali Linux	Open Source	N/A	3	$ 0
Oxygen Forensics Detective	N/A	$ 452 - $1,699 (Según la versión)	1	$ 1,699
FTK Imager	Version limitada	Version para empresas $1,200	1	$ 1,200
Autopsy	Open Source	N/A	3	$ 0
EnCase Forensic	N/A	$ 3,683.85 por equipo de trabajo	3	$ 11,051.55

Guasap Forensic	Open Source	N/A	3	$ 0
Wireshark	Versión Gratuita	N/A	3	$ 0
Elcomsoft iOS Forensic ToolKit	N/A	$ 1,495 por equipo de trabajo	2	$ 2,990
OSForensics	Versión Gratuita por 30 días	$ 1,499 por equipo de trabajo	2	$ 2,998
Event Log Explorer	Version limitada por 24 horas	$ 199 por equipo de trabajo	3	$ 597
Volatility Framework	Open Source	N/A	3	$ 0
WinHex	Version de prueba	$ 130.13 por equipo de trabajo	2	$ 260.26
Exiftool	Open Source	N/A	3	$ 0
			Total	**$ 20,795.81**

Nota: Todos los precios están sujetos a la página oficial y/o distribuidoras.

Tabla 16. Presupuesto para la adquisición del software

Fuente: Autor.

- **Presupuesto inicial**

El presupuesto inicial necesario para poder poner en marcha el laboratorio de informática forense, contando solo el presupuesto para la adquisición de hardware y software da un total de **$ 28,844.78**.

- **Presupuesto para renovación de licencias**

El presupuesto para la renovación de las licencias para un estimado de 5 años es el siguiente. Ver tabla 17.

Presupuesto para la renovación de licencias durante 5 años					
Software	**Duración de licencia**	**Cantidad de equipos en uso**	**Precio**	**Subtotal**	**+ 4 años de licencias**
Oxygen Forensics Detective	1 año	1	$ 1,699	$ 1,699	$ 6,796
FTK Imager	1 año	1	$ 1,200	$ 1,200	$ 4,800
EnCase Forensic	Perpetuo	3	$ 3,683.85	$ 11,051.55	
Elcomsoft iOS Forensic ToolKit	1 año	2	$ 1,495	$ 2,990	$ 11, 960
OSForensics	Perpetuo	2	$ 1,499	$ 2,998	
Event Log Explorer	1 año	3	$ 199	$ 597	$ 2,388
WinHex	1 año	2	$ 130.13	$ 260.26	$ 1,041.04
Total 1 año (Adquisición inicial)				$ 20,795.81	
Total 4 años (Renovación de licencias)					$ 26,985.04
			Total 5 años	**$ 47,780.85**	

Tabla 17. Presupuesto para la renovación de licencias durante 5 años

Fuente: Autor.

4.12 Mantenimiento

El laboratorio de informática forense requiere de mantenimiento para un buen funcionamiento de los equipos de cómputo como de las instalaciones, a fin de asegurar que, lo resultados de las investigaciones forenses que se realizan dentro de esta área sean confiables a la par de asegurar su confidencialidad y seguridad.

A continuación, en la siguiente tabla se describirán el tipo de mantenimiento que se deben cumplir y la frecuencia que se lo deben realizar. Ver Tabla 18.

Mantenimiento del Laboratorio de Informática Forense		
Instalaciones	**Preventivos**	**Frecuencia**
	- Mantenimiento de la mobiliaria de las áreas	Anual
	- Limpieza interior del laboratorio	Semanal
	Correctivos	**Frecuencia**
	- Cambio de la mobiliaria de las áreas	Cuando se requiera
	- Reubicación de las áreas	Cuando se requiera
Equipos	**Preventivos**	**Frecuencia**
	- Limpieza del equipo, ajustes, calibraciones.	Bimensual
	- Actualizar softwares, parches del sistema operativo, etc.	Mensualmente
	- Actualización de Seguridad (Antivirus)	Bimensual
	- Verificación de Licencias	Anualmente
	Correctivos	**Frecuencia**
	- Reparación o cambio de los componentes del equipo	Cuando se requiera
	- Remplazo del equipo de cómputo	Cuando se requiera

Tabla 18. Mantenimiento del Laboratorio de Informática Forense

Fuente: Autor.

CAPITULO 5

5.1 Conclusiones y Recomendaciones

5.1.1 Conclusiones

La investigación bibliográfica evidencio la existencia de una gran cantidad de artículos descritos en la COIP destinados a sancionar acciones delictivas con relación a la informática, sin embargo, a pesar de ello es claro la necesidad que tiene el país por aumentar lugares donde existan laboratorios de informática forense, donde se puede realizar investigaciones, puesto que se ve cada vez más reflejada en el incremento de denuncias de delitos informáticos.

La Universidad Católica de Cuenca, campus Azogues, cuenta con la infraestructura idónea para implementar un laboratorio de informática forense, logrando ofrecer la seguridad e integridad de las evidencias, además de contar con equipos de cómputo propicias para la adquisición de software y hardware, igualmente se requiere personal cualificado que haga uso de dichas herramientas a fin de lograr desarrollar investigaciones forenses pertinentes.

Se deben tener en cuenta los lineamientos presentados para el fortalecimiento del laboratorio, debido a que, es necesario contar con un modelo de trabajo, una metodología para realizar los procedimientos correspondientes en las investigaciones, como también de las guías de buenas prácticas, normas relacionadas a la informática forense para un mejor desempeño y en lo posible evitar el cuestionamiento del manejo de las evidencias.

La metodología propuesta en este proyecto no es un modelo definitivo, el mismo puede ir cambiando a lo largo del tiempo con el objetivo de mejorar los tiempos

de respuesta del personal y aumentar la eficiencia en la manipulación de la evidencia digital para obtener mejores resultados.

El personal del laboratorio competente es precisamente necesario, debido a que, a pesar de invertir en tener las mejores herramientas de hardware y software no servirán de nada si los miembros no están precisamente capacitados en manejar las distintas herramientas y desconoce la forma de emplear la metodología implicando que las pruebas presentadas ante los tribunales no sean admitidas.

El diseño del laboratorio está elaborado acorde al espacio y a la propuesta de modelo de investigación forense, motivo que cada área tiene un objetivo específico a cumplir con el personal correspondiente, sin embargo, el diseño se puede mejorar si se posee de un espacio más amplio. Por otro lado, se deben tener en cuenta las condiciones ambientales y de seguridad necesarias antes de realizar el boceto del LIF.

El mantenimiento es importante para mantener en condiciones óptimas tanto la instalación física como los equipos de cómputo, en especial cuando se trata de un laboratorio de este tipo, dado que es necesario que las evidencias que ingresan al lugar no se vean afectadas por algún contaminante del ambiente o un mal funcionamiento de los equipos.

5.1.2 Recomendaciones

Es importante estudiar a fondo los artículos tipificados en el Código Orgánico Integral Penal Ecuatoriano relacionado con los delitos informáticos para determinar el alcance que tendrá el laboratorio de informática forense.

La constante evolución tecnológica ocasiona que sea necesario adquirir equipos con altas especificaciones para mantener actualizado software y hardware puesto

que estos eventualmente llegarían a ocupar más requerimientos debido al gran manejo de datos que procesan. Esto con el objetivo de lograr confrontar las nuevas técnicas de los delitos informáticos que vayan surgiendo por el mismo motivo.

Capacitar al personal dentro de laboratorio es vital para mejorar las habilidades de los miembros, a fin de asegurar la calidad de los procedimientos realizados dentro del laboratorio.

La gran cantidad de software gratuitos da la posibilidad de enseñar tanto a estudiantes como a docentes sobre los delitos informáticos, como actúan y las investigaciones que se realizan para llegar con el ciberdelincuente, a fin de incentivar a interesarse por esta área forense.

Establecer políticas de protección, confidencialidad, manejo y seguridad de la información, como también políticas de calidad y atención al cliente para el laboratorio de informática forense.

REFERENCIAS BIBLIOGRÁFICAS

[1] V. Pons Gamón, “Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad,” *URVIO*, vol. 20, pp. 80–93, Jun. 2017.

[2] F. Sánchez Gálvez, “La importancia de la informática forense.,” *CyberSecurity Información & Privacidad*, Apr. 30, 2021. https://csecmagazine.com/2021/04/30/la-importancia-de-la-informatica-forense/.

[3] Y. I. Toala Indio, “Delitos Informáticos Frecuentes en el Ecuador: Casos de Estudio,” Universidad Politécnica Salesiana Sede Guayaquil, Guayaquil, 2021.

[4] A. Rosero, “Ciberdelincuentes operan de cuatro formas en el Ecuador,” *El Comercio*, Jan. 11, 2022.

[5] L. Reyes-Ruiz and F. Carmona Alvarado, “La investigación documental para la comprensión ontológica del objeto de estudio,” *Ediciones Universidad Simón Bolívar*, Barranquilla, Oct. 2020.

[6] J. Costa, “Ciencia e Ingeniería Forenses: Una Necesidad Social y Una Salida Profesional,” *ciènciaprop®*, vol. 1, no. 5, Aug. 2018.

[7] F. G. González-Robayo, J. S. González-Sanabria, and L. Téllez-Hernández, “Laboratorios de informática para mejorar el proceso de cumplimiento fiscal de Colombia,” *Rev. Científica*, vol. 36, no. 3, pp. 325–340, Aug. 2019, doi: 10.14483/23448350.14958.

[8] S. C. Ortega Ruiz and S. Paez Diaz, “Propuesta de guías de laboratorio para la asignatura de Informática Forense del programa de Ingeniería de Sistemas de la Universidad ECCI,” Universidad ECCI, Bogotá , 2020.

[9] R. S. Velasquez Pampañaupa and F. Davalos Soto, “Informática Forense y su influencia en la calidad de servicio en el Centro de Cómputo de la Universidad Tecnológica de los Andes,” Universidad Tecnológica de los Andes, Abancay – Apurímac, 2021.

[10] J. S. Larrea Ronquillo, “Estudio e implementación de metodologías de análisis forense digital aplicables en un laboratorio de informática forense en la carrera de ingeniería en networking y telecomunicaciones,” Universidad de Guayaquil, 2016.

[11] D. J. Carrillo Vinueza and D. K. Cortez Oviedo, “Desarrollo de una propuesta para la implementación de un laboratorio de informática forense dentro del centro de procesamientos de datos (CDP) de la carrera de Ingeniería de Ciencias de la Computación de la Universidad Politécnica Salesiana campus Sur,” Universidad Politécnica Salesiana sede Quito, 2019.

[12] M. Espinoza Mina, “Informática forense: una revisión sistemática de la literatura,” *Rehuso*, vol. 4, no. 2, pp. 112–128, May 2019, [Online]. Available: https://revistas.utm.edu.ec/index.php/Rehuso/article/view/1641/2094.

[13] O. L. Garcés Pérez, “Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática,” *Ediciones Futuro*, Boyeros, Oct. 2021.

[14] B. Lutkevich, “What is Computer Forensics (Cyber Forensics)?,” *TechTarget Security*, May 2021. https://www.techtarget.com/searchsecurity/definition/computer-forensics.

[15] K. Afifi-Sabet, “What is network forensics?,” *IT PRO*, Dec. 07, 2021. https://www.itpro.co.uk/cyber-attacks/31660/what-is-network-forensics.

[16] J. Moreno, I. Leguias, and M. Vargas-Lombardo, “Revisión sobre la forensía digital en dispositivos móvil con sistemas operativos Android,” *IDT*, vol. 14, no. 2, pp. 74–83, Dec. 2018, [Online]. Available: https://revistas.utp.ac.pa/index.php/id-tecnologico/article/view/2076/3031.

[17] J. M. García Góngora, “Introducción a las ciencias forenses,” *Universitat Oberta de Catalunya*, Barcelona, pp. 1–34, Feb. 2018.

[18] J. González, J. Bermeo, E. Villacreses, and J. Guerrero, “Vista de Delitos informáticos: una revisión en Latinoamérica,” *UTMACH*, Machala, Jul. 19, 2018.

[19] V. Pons Gamón, “Vista de Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad,” *URVIO - Rev. Latinoam. Estud. Segur.*, vol. 20, pp. 80–93, Jun. 2017, [Online]. Available: http://dx.doi.org/10.17141/urvio.20.2017.2563.

[20] J. D. Desayes Herrera, “Ciberseguridad: Importancia de una estratégica centroamericana homologada para contrarrestar la ciberdelincuencia como una amenaza emergente,” Universidad Nacional Autónoma de Nicaragua, Managua, 2022.

[21] C. A. Flores Quispe, “Tipos De Hackers,” *Universidad Mayor de San Andrés*, La Paz, pp. 16–18, 2018.

[22] J. Chen, “Carding,” *Investopedia*, Mar. 14, 2022. https://www.investopedia.com/terms/c/carding.asp.

[23] D. E. Ojeda Pereira and M. M. Muñoz, “Análisis de las vulnerabilidades en el manejo de la información bajo la norma iso/iec 27001:2013, en la empresa gestión & negocios administrativos sas del distrito de riohacha – la guajira,” Universidad Nacional Abierta y a Distancia UNAD, 2018.

[24] L. J. Bermúdez, “Phishing y Pharming. La problemática de la determinación de competencias en casos extraterritoriales,” Universidad Siglo 21, 2019.

[25] CSIRTUTPL, “¿Qué es la piratería online y cuáles son sus peligros?,” *UTLP, Universidad Técnica Particular de Loja*, Mar. 12, 2022. https://csirt.utpl.edu.ec/node/489.

[26] “Guía de Ciberataques,” *Instituto Nacional de Ciberseguridad de España*, Oct. 28, 2020. https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf.

[27] D. Cunha Barbosa, “Qué es un ataque de Man-in-the-Middle y cómo funciona,” *WeLiveSecurity*, Dec. 28, 2021. https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/.

[28] R. A. García Monje, “Seguridad informática y el Malware,” *Universidad Piloto de Colombia*, Oct. 10, 2017.

[29] J. F. Palmer Padilla, “Seguridad y Riesgos: Cyberbullying, Grooming y Sexting,” Universidad Oberta de Catalunya, 2017.

[30] C. Vélez Martínez, “Robo de identidad,” *Gac. Inst. Ing. UNAM*, vol. 1, no. 102, pp. 20–21, Feb. 2017, [Online]. Available: http://gacetaii.iingen.unam.mx/GacetaII/index.php/gii/article/view/1822.

[31] “Ransomware: una guía de aproximación para el empresario,” *Instituto Nacional de Ciberseguridad de España*, Apr. 20, 2021. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf.

[32] S. Guacaneme Medina, “Fugas de información en el ciberespacio, una nueva amenaza para los Estados.,” Universidad Militar Nueva Granada, 2021.

[33] M. Alonso González, “Fake News: desinformación en la era de la sociedad de la información,” *Ámbitos. Rev. Int. Comun.*, vol. 45, pp. 29–59, 2019, doi: 10.12795/Ambitos.

[34] “Online illicit trade is more than just the dark web,” *PMI - Philip Morris International*, Jul. 24, 2019. https://www.pmi.com/illicit-trade-prevention/blog/online-illicit-trade-is-more-than-just-the-dark-web.

[35] S. Figueiras, “¿Qué es el derecho informático?,” *CEUPE*, Apr. 09, 2021. https://www.ceupe.mx/blog/que-es-el-derecho-informatico.html.

[36] M. E. Poma-Alejandro, “Análisis de derecho comparado del perito informático,” Universidad Internacional de La Rioja, Quito, 2019.

[37] F. Martín, “Evidencias digitales: significado, objetivo y tratamiento,” *Legaltech*, Aug. 11, 2021. https://blog.lemontech.com/evidencias-digitales/#¿Que_son_las_evidencias_digitales.

[38] M. Zambrano Quiroz, J. Zambrano Quiroz, D. Zambrano Quiroz, and C. Tubay, “Informática forense - El caos de la manipulación de la información digital,” *Supl. CICA*, vol. 5, no. 11, pp. 185–212, Jun. 2021, [Online]. Available: https://suplementocica.uleam.edu.ec/index.php/SuplementoCICA/article/view/71.

[39] P. A. Ochoa Arévalo, “El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación,” *Rev. Econ. y Política*, vol. XIV, no. 28, pp. 35–46, 2018, doi: 10.25097/rep.n28.2018.03.

[40] L. Obbayi, “Computer forensics: Chain of custody,” *INFOSEC*, Jul. 06, 2019. https://resources.infosecinstitute.com/topic/computer-forensics-chain-custody/.

[41] EL UNIVERSO, “Ecuador ha recibido 40 millones de ataques cibernéticos, revela viceministro de Telecomunicaciones,” Apr. 15, 2019.

[42] EL UNIVERSO, “El aumento de la ciberdelincuencia a escala de economía mundial,” Apr. 19, 2022.

[43] Asamblea Nacional del Ecuador, *Código Orgánico Integral Penal*. Quito: COIP, 2021, p. 144.

[44] ISO, “ISO/IEC 27037:2012,” *International Organization for Standardization*, 2018. https://www.iso.org/standard/44381.html.

[45] L. N. Medina Velandia, “Criptografía y mecanismos de seguridad,” *Fund. Univ. del Área Andin.*, p. Tema 2, 2017, [Online]. Available: https://digitk.areandina.edu.co/handle/areandina/1423.

[46] G. Semprini, “Lineamientos para la creación de laboratorios informáticos forenses,” *Soc. Argentina Informática e Investig. Oper.*, pp. 7–19, 2016.

[47] C. E. López Grande and R. S. Guadron Gutiérrez, “Informática forense: cuando el delito hace uso de la tecnología,” *Esc. Espec. en Ing.*, Nov. 2017, [Online]. Available: http://hdl.handle.net/10972/3019.

[48] ISO, “ISO/IEC 27041:2015 - Tecnología de la información. Técnicas de seguridad. Orientación para garantizar la idoneidad y adecuación del método de investigación de

incidentes," *International Organization for Standardization*, 2021. https://www.iso.org/standard/44405.html.

[49] ISO, "ISO/IEC 27042:2015 - Tecnología de la información. Técnicas de seguridad. Directrices para el análisis e interpretación de evidencia digital," *International Organization for Standardization*, 2021. https://www.iso.org/standard/44406.html.

[50] ISO, "ISO/IEC 27043:2015 - Tecnología de la información. Técnicas de seguridad. Principios y procesos de investigación de incidentes," *International Organization for Standardization*, 2020. https://www.iso.org/standard/44407.html.

[51] E. Rivetti, Á. Gamarra, and H. B. Parra de Gallo, "Proyecto de creación de un laboratorio de forensia de IoT," *ReDDi Rev. Digit. del Dep. Ing. e Investig. Tecnológicas la Univ. Nac. La Matanza*, vol. 5, no. 1, pp. 1–10, Aug. 2020, [Online]. Available: http://repositoriocyt.unlam.edu.ar/handle/123456789/1205.

[52] SWGDE, "SWGDE Best Practices for Computer Forensic Acquisitions," *Scientific Working Group on Digital Evidence*, Apr. 25, 2018. https://www.swgde.org/documents/published-by-committee/forensics.

[53] SWGDE, "SWGDE Best Practices for Digital Evidence Collection," *Scientific Working Group on Digital Evidence*, Jul. 11, 2018. https://www.swgde.org/documents/published-by-committee/forensics.

[54] M. S. Jafri, S. Raharjo, and M. R. Arief, "Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones," *CCIT (Creative Commun. Innov. Technol. J.*, vol. 15, no. 1, pp. 82–105, Feb. 2022.

[55] Ciberforensic, "Directrices RFC 3227," *Ciberforensic*, Jun. 16, 2020. https://www.ciberforensic.com/directrices-rfc-3227.

[56] U.S Departament of Justice, "Electronic Crime Scene Investigation: A Guide for First Responders," *Natl. Inst. Justice*, 2001.

[57] C. González Henao and J. Cañón Franco, "Monografía informática forense," Universidad Tecnológica de Pereira, 2017.

[58] J. Arquillo Cruz, "Herramienta de apoyo para el análisis forense de computadoras," Universidad de Jaén, 2007.

[59] P. C. Ayazo Villadiego, "Uso de la informática forense aplicada a delitos informáticos en la industria colombiana," Universidad Nacional Abierta y a Distancia "UNAD," Cordoba, 2019.

[60] H. W. Morocho Morocho and D. F. Segarra Fajardo, "Análisis de recuperación de información usando la metodología 'SANS' para dispositivos de almacenamiento," Instituto de Tecnologías Sudamericano , Cuenca, 2020.

[61] L. D. Lobo Parra, D. Rico Bautista, Y. Medica Cárdenas, and A. Sanchez Ortiz, "Definición de una metodología práctica para la adquisición y análisis de evidencia digital en el contexto de una investigación post mortem," *Revista Ibérica de Sistemas e Tecnologias de Informação*, Lousada, pp. 369–384, 2019.

[62] J. M. Guerrero Rodriguez and L. A. Sanchez Cruz, "Requerimientos para el diseño de un Laboratorio de Análisis Forense Digital enfocado a Pequeñas y Medianas empresas en Colombia," Universidad Piloto de Colombia, Bogota, 2013.

[63] H. M. Buitrago López, "Viabilidad de implementación de un laboratorio de informática

forense en la Ciudad de Pereira," Universidad Católica de Pereira, 2016.

[64] Departamento Técnico Faro Barcelona, "Mejor iluminación de oficinas: Consejos, tipos y normativa," *Faro Barcelona*, Sep. 05, 2022. https://faro.es/es/blog/una-correcta-iluminacion-en-la-oficina/.

[65] ISO, "ISO/IEC 17025:2017 - Requisitos generales para la competencia de los laboratorios de ensayo y calibración," *International Organization for Standardization*, 2017. https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v2:es.

[66] ASCLD, "American Society of Crime Laboratory Directors," 2022. https://www.ascld.org/.

[67] Forensic Store, "Black Hole Faraday Bag Kit," 2022. https://www.forensicstore.com/product/black-hole-faraday-bag-kit/.

[68] StarTech.com, "Clonación de disco duro," 2022. https://www.startech.com/en-us/hdd/satdock2reu3.

[69] WiebeTech, "USB 3.1 WriteBlocker," 2022. https://wiebetech.com/products/usb-3-1-writeblocker/.

[70] ALLSOCKET, "Herramienta de recuperación de datos de Android," 2022. http://www.allsocket.com/en/Product.asp?SortID=5.

[71] Digital Intelligence, "Portátil Foresne FRED L," 2022. https://digitalintelligence.com/store/products/fred-l-forensic-laptop-f4130?taxon_id=18#contents.

[72] Computer Forensic Linux Live Distro, "CAINE (Computer Aided Investigative Environment)," *Computer forensics - Digital forensics*, 2019. https://www.caine-live.net/index.html.

[73] Kali, "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," 2022. https://www.kali.org/.

[74] Oxygen Forensics, "Oxygen Forensics Detective - Mobile forensic solutions: software and hardware," 2022. https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective.

[75] Exterro, "FTK Imager," 2022. https://www.exterro.com/ftk-imager.

[76] Basis Technology, "Autopsy - Digital Forensics," 2022. https://www.autopsy.com/.

[77] ONDATA International, "EnCase Forensic Software: Características y Funciones," 2022. https://www.ondata.es/recuperar/encase_forensic.htm#.

[78] QuantiKa14, "Guasap Forensic," 2022. https://quantika14.com/guasap-forensic/#page-content.

[79] Wireshark, "Go Deep," 2022. https://www.wireshark.org.

[80] Elcomsoft Co.Ltd, "Elcomsoft iOS Forensic Toolkit," 2022. https://www.elcomsoft.es/eift.html.

[81] PassMark, "OSForensics - Digital investigation," 2022. https://www.osforensics.com/.

[82] FSPro Labs, "Windows event log analysis software," 2022. https://eventlogxp.com/.

[83] Hacktivities, "Forensics — Memory Analysis with Volatility," *InfoSec Write-ups*, Dec. 28,

2021. https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765?gi=c335a431d0d1.

[84] X-Ways, “WinHex: Hex Editor & Disk Editor, Computer Forensics & Data Recovery Software,” 2022. https://www.x-ways.net/winhex/index-m.html.

[85] L. Sacco, “Mi Arsenal De Software: ExifTool,” *PERITOS INFORMATICOS*, Jul. 12, 2022. https://peritosinformaticos.ar/exiftool/.

[86] “ASCLD - Iniciativa de Acreditación,” 2022. https://www.ascld.org/accreditation-initiative/.

ANEXOS

ANEXO A. Documento para el Aseguramiento del área

Informe de la escena			
ID de Caso:			*000*
Nombre del responsable			
Cargo			
Fecha	*(dd/mm/aaaa)*	**Hora de llegada**	*(hh:mm)*
Dirección			
Detalles del lugar			
Nombres de los involucrados en la escena			
Fotografías del lugar			
Firma del responsable			

Fuente: Autor

ANEXO B. Documento para la Identificación y Recolección de la Evidencia

Identificación y recolección de evidencia				
ID de caso				*000*
Nombre del responsable				
Cargo				
Fecha:	*(dd/mm/aaaa)*	**Hora**	*(hh:mm)*	
Número de evidencia	Tipo de dispositivo	Tipo de evidencia	Nombre del propietario	Herramienta utilizada
Firma del responsable				

Fuente: Autor

ANEXO C. Documento para el trasporte de la evidencia

Transporte de evidencia					
ID de caso				***000***	
Nombre del responsable					
Cargo					
Fecha	*(dd/mm/aaaa)*	**Hora de salida**		*(hh:mm)*	
Número de evidencia		**Tipo de dispositivo**	**Observaciones**		
Firma del responsable					

Fuente: Autor

ANEXO D. Documento de Inventario de evidencias

Inventario de evidencias			
ID de Caso			*000*
Nombre del responsable			
Cargo			
Fecha	*(dd/mm/aaaa)*	**Hora de llegada**	*(hh:mm)*
Número de evidencia			
ID de la evidencia			
Tipo de dispositivo			
Tipo de evidencia			
Estado de la evidencia			
Observaciones			
Fotografía			
Firma del responsable			

Fuente: Autor

ANEXO E. Documento de Análisis y Examen de la evidencia

Análisis y Examen de la evidencia			
ID de Caso			*000*
Nombre del responsable			
Cargo			
Fecha	*(dd/mm/aaaa)*	**Hora de inicio**	*(hh:mm)*
ID de la evidencia			
Tipo de análisis			
Herramienta Utilizada			
Detalles del análisis			
Fecha	*(dd/mm/aaaa)*	**Hora de finalización**	*(hh:mm)*
Resultados obtenidos			
Firma del responsable			

Fuente: Autor

ANEXO F. Control de visitas

Control de visitas				
Fecha	**Hora de Solicitud**	**Hora de finalización**	**Nro. De visita**	*001*
(dd/mm/aaaa)	*(hh:mm)*	*(hh:mm)*		
Nombre			**Cédula**	
Motivo				
Firma				
Nombre del miembro del personal			**Cargo**	
Firma				
Control de visitas				
Fecha	**Hora de Solicitud**	**Hora de finalización**	**Nro. De visita**	*002*
(dd/mm/aaaa)	*(hh:mm)*	*(hh:mm)*		
Nombre			**Cédula**	
Motivo				
Firma				
Nombre del miembro del personal			**Cargo**	
Firma				

Fuente: Autor

ANEXO G. Solicitud de entrega de evidencia

Solicitud de entrega de evidencia				
Fecha	**Hora de Entrega**		**Nro de Solicitud**	*001*
(dd/mm/aaaa)	*(hh:mm)*			
Nombre del responsable				
ID de caso				
ID de Evidencia				
Detalles				
Entregado por		**Recibido por**		
Firma		**Firma**		

Fuente: Autor

ANEXO H. Hoja de ruta de Acreditación de ASCLD

Fuente: The American Society of Crime Laboratory Directors [86].

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

Universidad Católica de Cuenca	AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL	CÓDIGO: F – DB – 30 VERSION: 01 FECHA: 2021-04-15 Página **1** de **1**

Diego Eduardo León Pacheco portador de la cédula de ciudadanía Nº **0301961819**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"Propuesta de un Laboratorio de Informática Forense en la Universidad Católica de Cuenca, Campus Azogues"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Azogues, **18 de enero de 2023**

F: .....

Diego Eduardo León Pacheco

C.I. **0301961819**

www.ucacue.edu.ec